

«Эта книга — живое и бодрящее изложение великолепного подхода авторов к квантовым процессам. Рекомендую ее всем — без ограничения возраста!» — Луис Кауфман, Иллинойский университет

«В книге с нуля разрабатывается диаграммный язык для квантовой теории, а особенно для квантовых процессов. Книга, безусловно, удалась — яркая, полная, абсолютно понятная — читать сплошное наслаждение». — Джереми Баттерфилд, Кембриджский университет

Не имеющие аналогов особенности квантового мира в этой книге объясняются на языке диаграмм — новаторском наглядном методе изложения сложных теорий. Применяемый формализм позволяет выработать интуитивное понимание квантовых особенностей без сложных вычислений — для чтения достаточно базовой математической подготовки. Это чисто диаграммное изложение квантовой теории — плод 10-летних исследований, объединяющий классические методы линейной алгебры и гильбертовых пространств с передовыми достижениями в области квантовых вычислений и основанной квантовой теории.

Написанная простым языком, с юмором и включающая свыше 100 упражнений, эта книга идеальна в качестве начального курса по основам квантовой теории и квантовым вычислениям для студентов, начиная с младших курсов и до уровня аспирантов, а для ученых из разных областей — физики, биологии, лингвистики и когнитивистики — станет прекрасной возможностью открыть для себя новый набор инструментов исследования процессов и их взаимодействий.

Боб Коке (Bob Coecke) — профессор кафедры основанной квантовой теории, логики и структур Оксфордского университета, где также возглавляет междисциплинарную «квантовую группу». Его основополагающие исследования простираются от квантовой механики до композиционной структуры смысла в естественных языках, а недавно он также заинтересовался причинностью и когнитивной архитектурой.

Алекс Киссинджер (Aleks Kissinger) — доцент кафедры квантовых структур и логики в университете Рэг-бауд. Занимается диаграммными языками, теорией переписывания, теорией категорий и приложениями к квантовым вычислениям и основам физики.

ISBN 978-5-97060-727-5



9 785970 607275 >

 CAMBRIDGE
UNIVERSITY PRESS

 ДМК
ИЗДАТЕЛЬСТВО
www.dmk.rf

Интернет-магазин:
www.dmkpress.com

Оптовая продажа:
КТК "Галактика"
books@aliens-kniga.ru

ИЗОБРАЖЕНИЕ КВАНТОВЫХ ПРОЦЕССОВ

Боб Коке и Алекс Киссинджер

ИЗОБРАЖЕНИЕ КВАНТОВЫХ ПРОЦЕССОВ

Начальный курс квантовой теории
и рассуждений на диаграммах



 ДМК
ИЗДАТЕЛЬСТВО

Боб Коке
Оксфордский университет

Алекс Киссинджер
Университет Радбауд

Изображение квантовых процессов

*Начальный курс квантовой теории
и рассуждений на диаграммах*

Bob Coecke
University of Oxford

Aleks Kissinger
Radboud University

Picturing quantum processes

*A first course in quantum theory
and diagrammatic reasoning*



CAMBRIDGE
UNIVERSITY PRESS

Боб Коке
Оксфордский университет

Алекс Киссинджер
Университет Радбауд

Изображение квантовых процессов

*Начальный курс квантовой теории
и рассуждений на диаграммах*



ИЗДАТЕЛЬСТВО

Москва, 2019

УДК 517.982.224
ББК 22.12
К55

Коке Б., Киссинджер А.

К55 Изображение квантовых процессов / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2019. – 880 с.: ил.

ISBN 978-5-97060-727-5

Эта книга – живое изложение великолепного подхода авторов к квантовым процессам.

Не имеющие аналогов особенности квантового мира в этой книге объясняются на языке диаграмм – новаторском наглядном методе изложения сложных теорий.

Применяемый формализм позволяет выработать интуитивное понимание квантовых особенностей без сложных вычислений – для чтения достаточно базовой математической подготовки. Это чисто диаграммное изложение квантовой теории – плод 10-летних исследований, объединяющий классические методы линейной алгебры и гильбертовых пространств с передовыми достижениями в области квантовых вычислений и оснований квантовой теории.

Книга написана простым языком, с юмором и включает свыше 100 упражнений.

Издание будет полезно в качестве начального курса по основаниям квантовой теории и квантовым вычислениям для студентов, а также для ученых из разных областей – физики, биологии, лингвистики и когнитивистики.

УДК 517.982.224
ББК 22.12

Printed in the United Kingdom by TJ International Ltd. Padstow Cornwall. Copyright © 2017 Bob Coecke and Aleks Kissinger. Russian-language edition copyright © 2019 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-107-10422-8 (анг.)
ISBN 978-5-97060-727-5 (рус.)

Copyright © 2017 Bob Coecke and Aleks Kissinger
© Оформление, издание, перевод, ДМК Пресс, 2019

Содержание

| | |
|--|----|
| Предисловие | 12 |
| Глава 1. Введение | 17 |
| 1.1. Пингвины и белый медведь | 17 |
| 1.2. Так что же тут нового? | 21 |
| 1.2.1. Новое отношение к квантовой теории: особенности | 22 |
| 1.2.2. Новый вид математики: диаграммы | 25 |
| 1.2.3. Новое основание физики: процессные теории | 27 |
| 1.2.4. Новая парадигма: квантовый пикторализм | 29 |
| 1.3. Исторические замечания и ссылки..... | 31 |
| Глава 2. Как читать эту книгу | 35 |
| 2.1. Кто вы и чего вы хотите? | 35 |
| 2.2. Меню | 36 |
| 2.2.1. Как эволюционируют диаграммы в этой книге | 36 |
| 2.2.2. Голливудский трейлер | 39 |
| 2.2.3. Промежуточное синтаксическое загрязнение | 40 |
| 2.2.4. Итоги, исторические замечания, ссылки, эпитафьи | 41 |
| 2.2.5. Заголовки со звездочкой и материал повышенной сложности | 41 |
| 2.3. Часто задаваемые вопросы | 42 |
| Глава 3. Процессы как диаграммы | 45 |
| 3.1. От процессов к диаграммам..... | 46 |
| 3.1.1. Процессы – блоки, системы – провода..... | 46 |
| 3.1.2. Процессные теории | 49 |
| 3.1.3. Диаграммы – это математика..... | 52 |
| 3.1.4. Процессные равенства | 55 |
| 3.1.5. Подстановка диаграмм..... | 59 |
| 3.2. Схемные диаграммы..... | 61 |
| 3.2.1. Параллельная композиция | 61 |
| 3.2.2. Последовательная композиция | 62 |
| 3.2.3. Два эквивалентных определения схем | 64 |
| 3.2.4. Диаграммы лучше алгебры..... | 67 |
| 3.3. Функции и отношения как процессы | 70 |
| 3.3.1. Множества | 70 |
| 3.3.2. Функции | 72 |
| 3.3.3. Отношения..... | 74 |
| 3.3.4. Сравнение функций с отношениями | 77 |
| 3.4. Специальные процессы | 77 |
| 3.4.1. Состояния, эффекты и числа..... | 77 |
| 3.4.2. Как выразить невозможное: нулевые диаграммы | 85 |
| 3.4.3. Процессы, равные «с точностью до числа» | 86 |
| 3.4.4. Нотация Дирака | 88 |
| 3.5. Итоги: что следует запомнить | 90 |

| | |
|---|------------|
| 3.6. Дополнительный материал* | 93 |
| 3.6.1. Абстрактные тензорные системы* | 94 |
| 3.6.2. Симметричные моноидальные категории* | 96 |
| 3.6.3. Диаграммы общего вида и схемы* | 98 |
| 3.7. Исторические замечания и ссылки | 99 |
| Глава 4. Струнные диаграммы | 102 |
| 4.1. Чашки, крышки и струнные диаграммы | 103 |
| 4.1.1. Разделимость | 104 |
| 4.1.2. Двойственность процессов и состояний | 107 |
| 4.1.3. Уравнения разгибания | 110 |
| 4.1.4. Струнные диаграммы | 112 |
| 4.2. Транспонирование и след | 114 |
| 4.2.1. Транспонирование | 115 |
| 4.2.2. Транспонирование составных систем | 120 |
| 4.2.3. След и частичный след | 122 |
| 4.3. Отражение диаграмм | 124 |
| 4.3.1. Адъюнкция | 124 |
| 4.3.2. Сопряжение | 129 |
| 4.3.3. Внутреннее произведение | 134 |
| 4.3.4. Унитарность | 138 |
| 4.3.5. Положительность | 139 |
| 4.3.6. \otimes -положительность | 141 |
| 4.3.7. Проекторы | 143 |
| 4.4. Квантовые особенности, выводимые из струнных диаграмм | 146 |
| 4.4.1. Теорема о невозможности универсальной разделимости | 147 |
| 4.4.2. Две теоремы о невозможности клонирования | 151 |
| 4.4.3. Как будто время вспять течет | 156 |
| 4.4.4. Телепортация | 159 |
| 4.5. Итоги: что следует запомнить | 164 |
| 4.6. Дополнительный материал* | 169 |
| 4.6.1. Струнные диаграммы в абстрактных тензорных системах* | 169 |
| 4.6.2. Двойственные типы и самодвойственность* | 170 |
| 4.6.3. Инволютивные компактные замкнутые категории* | 174 |
| 4.7. Исторические замечания и ссылки | 175 |
| Глава 5. От диаграмм к гильбертову пространству | 178 |
| 5.1. Базисы и матрицы | 180 |
| 5.1.1. Базис для типа | 180 |
| 5.1.2. Матрица процесса | 187 |
| 5.1.3. Суммы процессов | 192 |
| 5.1.4. От матриц к процессам | 197 |
| 5.1.5. Матрицы изометрических и унитарных процессов | 203 |
| 5.1.6. Матрицы самоадьюнктных и положительных процессов | 207 |
| 5.1.7. Следы матриц | 211 |
| 5.2. Матричное исчисление | 213 |
| 5.2.1. Последовательная композиция матриц | 213 |
| 5.2.2. Параллельная композиция матриц | 214 |
| 5.2.3. Матричная форма чашек и крышек | 221 |
| 5.2.5. Матрицы как процессные теории | 224 |
| 5.3. Гильбертовы пространства | 227 |

| | |
|---|------------|
| 5.3.1. От диаграмм к линейным отображениям и гильбертовым пространствам | 227 |
| 5.3.2. От сопряжения к положительности..... | 229 |
| 5.3.3. Почему математики любят комплексные числа | 231 |
| 5.3.4. Классические логические вентили как линейные отображения..... | 237 |
| 5.3.5. X-базис и линейное отображение Адамара | 240 |
| 5.3.6. Базис Белла и отображения Белла | 245 |
| 5.4. Гильбертовы пространства и диаграммы | 250 |
| 5.4.1. Струнные диаграммы полны относительно линейных отображений..... | 251 |
| 5.4.2. Теоретико-множественное определение гильбертовых пространств..... | 253 |
| 5.5. Итоги: что следует запомнить | 261 |
| 5.6. Дополнительный материал* | 266 |
| 5.6.1. За пределами конечного числа измерений*..... | 267 |
| 5.6.2. Категории с суммами и базисами* | 269 |
| 5.6.3. Суммы в теории узлов* | 271 |
| 5.6.4. Эквивалентность симметричных моноидальных категорий* | 272 |
| 5.7. Исторические замечания и ссылки | 278 |
| Глава 6. Квантовые процессы..... | 281 |
| 6.1. Переход к чистым квантовым отображениям путем дублирования..... | 283 |
| 6.1.1. Дублирование порождает вероятности..... | 284 |
| 6.1.2. Дублирование устраняет глобальные фазы | 287 |
| 6.1.3. Процессная теория чистых квантовых отображений | 291 |
| 6.1.4. Что сохраняется при дублировании | 296 |
| 6.1.5. Что не сохраняется при дублировании | 301 |
| 6.2. От отбрасывания к квантовым отображениям | 305 |
| 6.2.1. Отбрасывание | 305 |
| 6.2.2. Нечистота | 310 |
| 6.2.3. Вес и причинность для квантовых состояний | 313 |
| 6.2.4. Процессная теория квантовых отображений | 319 |
| 6.2.5. Каузальность квантовых отображений | 324 |
| 6.2.6. От каузальности к изометричности и унитарности | 326 |
| 6.2.7. Разложение Крауса и смешивание | 330 |
| 6.2.8. Теорема о нераспространении | 337 |
| 6.3. Относительность в процессных теориях..... | 341 |
| 6.3.1. Причинная структура | 342 |
| 6.3.2. Из причинности следует несигнальность | 347 |
| 6.3.3. Причинность и ковариантность | 348 |
| 6.4. Квантовые процессы..... | 350 |
| 6.4.1. Недетерминированные квантовые процессы | 352 |
| 6.4.2. Недетерминированная реализация всех квантовых отображений | 355 |
| 6.4.3. Очищение квантовых процессов..... | 358 |
| 6.4.4. Для телепортации необходимо классическое взаимодействие | 361 |
| 6.4.5. Управляемые процессы..... | 363 |
| 6.4.6. Квантовая телепортация в деталях | 365 |
| 6.5. Итоги: что следует запомнить | 368 |
| 6.6. Дополнительный материал* | 372 |
| 6.6.1. Дублирование общих процессных теорий* | 372 |
| 6.6.2. Аксиоматизация дублирования* | 374 |
| 6.6.3. А теперь кое-что из другой области* | 376 |
| 6.7. Исторические замечания и ссылки | 377 |

| | |
|---|-----|
| Глава 7. Квантовые измерения | 380 |
| 7.1. Измерения ОНБ | 382 |
| 7.1.1. Введение в измерительные приборы от додо..... | 382 |
| 7.1.2. Возмущающие измерения ОНБ | 385 |
| 7.1.3. Невозмущающие измерения ОНБ | 390 |
| 7.1.4. Суперпозиция и интерференция | 391 |
| 7.1.5. Наилучшая из имеющихся альтернатив наблюдению | 395 |
| 7.2. Динамика измерений и квантовые протоколы | 396 |
| 7.2.1. Индуцированная измерением динамика I: обратное действие..... | 397 |
| 7.2.2. Пример: вентильная телепортация | 400 |
| 7.2.3. Индуцированная измерением динамика II: коллапс..... | 402 |
| 7.2.4. Пример: перекоммутация запутывания | 404 |
| 7.3. Более общие виды измерения | 406 |
| 7.3.1. Измерения фон Неймана | 406 |
| 7.3.2. Квантовый формализм фон Неймана | 412 |
| 7.3.3. Измерения POVM..... | 416 |
| 7.3.4. Теоремы Наймарка и Озавы о дилатации..... | 418 |
| 7.4. Томография..... | 421 |
| 7.4.1. Томография состояния | 421 |
| 7.4.2. Информационно полные измерения | 424 |
| 7.4.3. Локальная томография = процессная томография..... | 426 |
| 7.5. Итоги: что следует запомнить | 428 |
| 7.6. Дополнительный материал*..... | 432 |
| 7.6.1. А существуют ли вообще квантовые измерения?* | 432 |
| 7.6.2. Проекторы и квантовая логика* | 435 |
| 7.6.3. Невозможность локальной томографии* | 437 |
| 7.7. Исторические замечания и ссылки | 439 |
| | |
| Глава 8. Изображение классически-квантовых процессов | 441 |
| 8.1. Классические системы как провода..... | 445 |
| 8.1.1. Двойные и одиночные провода..... | 446 |
| 8.1.2. Пример: плотное кодирование..... | 449 |
| 8.1.3. Измеритель и кодировщик | 451 |
| 8.1.4. Классически-квантовые отображения | 453 |
| 8.1.5. Удаление и причинность..... | 457 |
| 8.2. От пауков к классическим отображениям..... | 460 |
| 8.2.1. Классические отображения..... | 461 |
| 8.2.2. Копирование и удаление..... | 464 |
| 8.2.3. Пауки | 474 |
| 8.2.4. Если нечто ведет себя как паук, то это и есть паук..... | 481 |
| 8.2.5. Все линейные отображения как пауки + изометрии..... | 484 |
| 8.2.6. Паучьи диаграммы и полнота | 489 |
| 8.3. От пауков к квантовым отображениям | 491 |
| 8.3.1. Измеритель и кодировщик как пауки | 492 |
| 8.3.2. Декогеренция..... | 497 |
| 8.3.3. Классические, квантовые и гибридные пауки..... | 502 |
| 8.3.4. Смешивание с пауками | 507 |
| 8.3.5. Запутывание для нечистых состояний..... | 511 |
| 8.4. Измерения и протоколы с участием пауков | 514 |
| 8.4.1. Измерения ОНБ | 515 |
| 8.4.2. Управляемые унитарные процессы | 518 |

| | |
|--|-----|
| 8.4.3. Телепортация | 521 |
| 8.4.4. Плотное кодирование..... | 524 |
| 8.4.5. Перекоммутация запутывания..... | 525 |
| 8.4.6. Измерения фон Неймана | 526 |
| 8.4.7. Измерения POVM и теорема Наймарка о дилатации | 529 |
| 8.5. Итоги: что следует запомнить | 530 |
| 8.6. Дополнительный материал* | 537 |
| 8.6.1. Пауки как алгебры Фробениуса* | 538 |
| 8.6.2. Некоммутативные пауки* | 541 |
| 8.6.3. Волосатые пауки* | 544 |
| 8.6.4. Пауки как слова* | 547 |
| 8.7. Исторические замечания и ссылки | 547 |

Глава 9. Изображение фаз и дополненности..... 550

| | |
|--|-----|
| 9.1. Украшенные пауки..... | 552 |
| 9.1.1. Несмещенность и фазовые состояния | 552 |
| 9.1.2. Фазовые пауки | 558 |
| 9.1.3. Слияние фазовых пауков | 560 |
| 9.1.4. Фазовая группа | 563 |
| 9.1.5. Фазовые вентили | 566 |
| 9.2. Многоцветные пауки | 570 |
| 9.2.1. Дополнительные пауки | 570 |
| 9.2.2. Дополненность и несмещенность | 576 |
| 9.2.3. От дополненности к вентилю CNOT | 582 |
| 9.2.4. «Цвета» классических данных | 585 |
| 9.2.5. Дополнительные измерения..... | 587 |
| 9.2.6. Квантовое распределение ключей | 591 |
| 9.2.7. Телепортация с дополнительными измерениями..... | 594 |
| 9.3. Сильная дополненность | 600 |
| 9.3.1. Недостающие правила | 601 |
| 9.3.2. Моногамия сильной дополненности | 604 |
| 9.3.3. Лики сильной дополненности..... | 605 |
| 9.3.4. Классическая подгруппа | 610 |
| 9.3.5. От пауков к отображениям четности | 617 |
| 9.3.6. Классификация сильной дополненности | 621 |
| 9.4. ZX-исчисление..... | 624 |
| 9.4.1. ZX-диаграммы универсальны..... | 626 |
| 9.4.2. ZX-исчисление для диаграмм Клиффорда..... | 629 |
| 9.4.3. ZX-исчисление для додо: только диаграммы и ничего более | 634 |
| 9.4.4. ZX для профессионалов: строим собственное исчисление | 640 |
| 9.4.5. ZX для богов: полнота | 645 |
| 9.4.6. Что нам дало полное ZX-исчисление | 653 |
| 9.5. Итоги: что следует запомнить | 655 |
| 9.6. Дополнительный материал* | 661 |
| 9.6.1. Сильно дополнительные пауки как алгебра Хопфа* | 661 |
| 9.6.2. Сильная дополненность и нормальные формы* | 664 |
| 9.7. Исторические замечания и ссылки | 667 |

Глава 10. Квантовая теория: полная картина..... 670

| | |
|---------------------------------|-----|
| 10.1. Диаграммы | 671 |
| 10.1.1. Схемные диаграммы | 671 |

| | |
|---|------------|
| 10.1.2. Струнные диаграммы..... | 673 |
| 10.1.3. Дублированные диаграммы..... | 675 |
| 10.1.4. Паучьи диаграммы..... | 677 |
| 10.1.5. ZX-диаграммы..... | 680 |
| 10.2. Процессы..... | 682 |
| 10.2.1. Причинность..... | 683 |
| 10.2.2. Разложение процессов и невозможность распространения..... | 683 |
| 10.2.3. Примеры..... | 685 |
| 10.3. Законы..... | 691 |
| 10.3.1. Дополнительность..... | 691 |
| 10.3.2. Сильная дополнительность..... | 694 |
| 10.3.3. ZX-исчисление..... | 696 |
| 10.4. Исторические замечания и ссылки..... | 699 |
| Глава 11. Основания квантовой теории..... | 701 |
| 11.1. Квантовая нелокальность..... | 701 |
| 11.1.1. Уточнения квантовой теории..... | 702 |
| 11.1.2. Сценарии ГХЦ–Мермина..... | 704 |
| 11.1.3. Получение противоречия..... | 706 |
| 11.2. Квантовоподобные процессные теории..... | 708 |
| 11.2.1. Дополнительность в теории отношений..... | 708 |
| 11.2.2. Модельная квантовая теория Спеккенса..... | 710 |
| 11.2.3. Фазы в спек-теории..... | 714 |
| 11.2.4. ZX-исчисление для спек-теории..... | 718 |
| 11.2.5. Нелокальность в спек-теории?..... | 721 |
| 11.3. Итоги: что следует запомнить..... | 723 |
| 11.4. Исторические замечания и ссылки..... | 724 |
| Глава 12. Квантовые вычисления..... | 726 |
| 12.1. Схемная модель..... | 727 |
| 12.1.1. Квантовые вычисления как ZX-диаграммы..... | 728 |
| 12.1.2. Построение квантовых вентилях в виде ZX-диаграмм..... | 731 |
| 12.1.3. Универсальность схем..... | 738 |
| 12.2. Квантовые алгоритмы..... | 745 |
| 12.2.1. (Ложная?) магия квантового оракула..... | 746 |
| 12.2.2. Алгоритм Дойча–Йожи..... | 750 |
| 12.2.3. Квантовый поиск..... | 755 |
| 12.2.4. Задача о скрытой подгруппе..... | 760 |
| 12.3. Основанные на измерении квантовые вычисления..... | 767 |
| 12.3.1. Графовые и кластерные состояния..... | 769 |
| 12.3.2. Измерение графовых состояний..... | 770 |
| 12.3.3. Прямое распространение..... | 772 |
| 12.3.4. Прямое распространение с помощью классических проводов..... | 775 |
| 12.3.5. Универсальность..... | 779 |
| 12.4. Итоги: что следует запомнить..... | 784 |
| 12.5. Исторические замечания и ссылки..... | 786 |
| Глава 13. Квантовые ресурсы..... | 787 |
| 13.1. Ресурсные теории..... | 788 |
| 13.1.1. Бесплатные процессы..... | 789 |
| 13.1.2. Сравнение ресурсов..... | 791 |

| | |
|---|------------|
| 13.1.3. Измерение ресурсов | 794 |
| 13.2. Теория чистоты | 796 |
| 13.2.1. Сравнение чистоты..... | 797 |
| 13.2.2. Измерение (не)чистоты..... | 806 |
| 13.3. Теория запутывания | 807 |
| 13.3.1. LOCC-запутывание | 808 |
| 13.3.2. SLOCC-запутывание | 821 |
| 13.3.3. Взрывающиеся пауки | 827 |
| 13.3.4. Назад к основам: арифметика | 832 |
| 13.4. Итоги: что следует запомнить..... | 836 |
| 13.5. Исторические замечания и ссылки..... | 840 |
| Глава 14. Программа Quantomatic..... | 842 |
| 14.1. Проверка Quantomatic в деле | 843 |
| 14.2. !-блоки: замена многоточию..... | 849 |
| 14.3. Синтез физических теорий | 852 |
| 14.4. Исторические замечания и ссылки..... | 855 |
| Некоторые обозначения | 857 |
| Библиография..... | 858 |
| Предметный указатель | 874 |

Предисловие

Рады видеть вас здесь! Эта книга о том, как рассказывать о квантовой теории в картинках. Но прежде чем переходить к самой истории, стоит сказать пару слов о том, как она появилась. С одной стороны, история совсем новая – в том смысле, что тесно связана с исследованиями последних 10 лет, которыми мы занимались совместно с коллегами. С другой стороны, можно сказать, что ей уже 80 лет, и восходит она к тем временам, когда фон Нейман на удивление всему миру развенчал свой собственный квантовый формализм и стал искать что-то получше. Можно также сказать, что началась она, когда Эрвин Шрёдингер нашел ответ на сомнения Альберта Эйнштейна по поводу «жуткого дальнего действия», установив структуру составных систем (и, в частности, их неразделимость), ставшую сердцем квантовой теории.

К истории можно подойти и с другой стороны, вспомнив, что 40 лет назад тогда еще студент Роджер Пенроуз заметил, что о тензорном исчислении гораздо удобнее рассуждать в терминах картинок, а не символов.

Но 80 лет назад авторов еще не было на свете, по крайней мере в человеческой ипостаси, а 40 лет назад мы еще были слишком малы, так что это предисловие предлагает эгоцентрический взгляд на рождение книги, которую вы держите в руках. А заодно дает нам возможность от всего сердца признать заслуги всех тех, без кого эта книга не состоялась бы (равно как и тех, кто чуть было не похоронил ее).

Все началось довольно плохо для Боба, который в 1990-х годах работал над докторской диссертацией, посвященной никому тогда не интересной теме контекстных «представлений скрытых параметров» в квантовой теории – недавно ей было дипломатично найдено другое название – *онтологические модели* (Harrigan and Spekkens, 2010; Pusey et al., 2012). Помаявшись некоторое время без работы и предприняв неудачную попытку стать рок-звездой, Боб занялся еще менее перспективной темой квантовой логики фон Неймана (Birkhoff and von Neumann, 1936), примыкающей к работам эксцентричного борца с традициями Константина Пирона (Constantin Piron, 1976).

Именно тогда на сцене появилась теория категорий, а также серьезные идеи о фундаментальной роли композиции в квантовых системах – а это уже естественно привело к выходу квантовых процессов (а не квантовых состояний) на передний план...



Если вас мутит от теории категорий, не бросайте книгу! Хотя эта теория оказала влияние на многие изложенные в книге идеи, эта книга вовсе не о ней!

...И в конечном итоге эти идеи должны были заложить формальную и концептуальную основу наглядного подхода к квантовой теории. Категориальный взгляд на основания квантовой теории был впервые предложен в работе Дэвида Мура (David Moore, 1995), очень талантливого ученого, академическая карьера которого печально закончилась в конце 1990-х годов – периоде, когда на концептуально ориентированную физику повсеместно был наложен запрет. Совместно с Муром и Изаром Штуббе (Isar Stubbe) Боб предпринял первые попытки переформули-

ровать квантовую теорию в терминах теории категорий (Coecke et al., 2001), но, к несчастью, эта попытка унаследовала многочисленные недостатки прежней квантовой логики. Основная проблема квантовой логики заключалась в неявном предположении о том, что рассматриваемые физические системы всегда являются «частью представляющегося внешним мира явлений, который предполагается отделенным от своего окружения в том смысле, что его взаимодействиями с окружающей средой можно либо вообще пренебречь, либо смоделировать их каким-то простым способом» (Moore, 1999). Однако взаимодействия со средой – это нечто такое, что обязательно нужно принимать во внимание!

После исключения из университета (чему виной бюрократия, местные дразги и бесконечное лицемерие) Боб безуспешно пытался найти себя в искусстве, и когда на горизонте уже маячила перспектива стать безработным, случилось чудо: два совершенно незнакомых ему человека, Пракаш Панангаден и Самсон Абрамски, выбрали «испытательную» ставку «постдока» в Компьютерной лаборатории в Оксфорде (тогда ее ласково называли Комлаб). И хотя Боб абсолютно не разбирался в информатике, а компьютерщиков считал нездешними чудиками, которые днями напролет плятятся в экраны, он нашел в этом подразделении родной дом и очень скоро обнаружил, что компьютерщики, в отличие от специалистов по квантовой логике, уже давно изучают структуру взаимодействующих систем и умеют элегантно описывать такие системы на языке теории категорий. Более того, на этом конкретном факультете информатики по теории категорий даже читался отдельный курс для соискателей степени бакалавра.

И тут на сцену выходит второй соавтор. В то время Алекс приехал в Оксфорд по двухмесячной программе студенческого обмена из своего родного Университета Талса, штат Оклахома (рис. 0.1), и как раз слушал тот самый курс по теории категорий, который читал Самсон. Психоделическая природа этого курса (включая гостевую лекцию о странных на вид моноидных категориях, прочитанную не менее странным типом) заинтересовала Алекса настолько, что он погрузился в предмет с головой. По совету Самсона он начал посещать групповой семинар «Квантовый ланч» (Quantum Lunch). Формат семинара был такой: грандиозный совместный обед в пабе, а затем занятие, на котором пьяный и сонный докладчик вещал столь же пьяной и сонной аудитории на темы из только зарождающейся дисциплины категориальной квантовой механики. Здорово было.

Два месяца обернулись девятью годами, комлаб превратилась в «факультет информатики», и хотя, похоже, никто уже не мог припомнить, когда Алекс тут появился, дело кончилось диссертациями – сначала магистерской, потом докторской – и постдоком.



Рис. 0.1 ❖ Типичные виды Талсы, штат Оклахома

Без удивительного сочетания концептуального мышления и владения математическим аппаратом в этом уникальном анклав информатики книга, которую вы держите в руках, не состоялась бы. В разительном противоречии с запретом на слова «фундаментальный» и «концептуальный» в физике 1990-х годов, в этой новой среде «фундаментальность» и «концептуальность» считались великими достоинствами! В результате родилось новое исследовательское сообщество специалистов по информатике, чистых математиков, философов и исследователей в возродившейся области оснований квантовой механики. Пожалуй, не будет преувеличением сказать, что эта уникальная атмосфера внесла весомый вклад в возрождение сообщества оснований квантовой механики в целом, в ходе которого некоторые из его высокоуважаемых членов, и в особенности Chiribella et al. (2010) и Hardy (2013a), приняли диаграммную парадигму.

Конференции по квантовой физике и логике (Quantum Physics and Logic – QPL), основанные Питером Селинджером (Peter Selinger) в 2003 году под другим названием (но с такой же аббревиатурой!), стали форумом, сыгравшим особую роль в разработке основных результатов, легших в основу этой книги. На самом деле самая первая работа по диаграммным рассуждениям о новых квантовых теориях (Coecke, 2003) была представлена на первой конференции QPL. Формализация этого результата в терминах теории категорий (Abramsky and Coecke, 2004), которая теперь называется категориальной квантовой механикой, стала настоящим хитом в сообществе семантики компьютерных наук, и в итоге несколько молодых людей выстроили научную карьеру в этой области. Самые авторитетные конференции по информатике (например, LiCS и ICALP) регулярно принимают работы по категориальной квантовой механике, а недавно то же самое начали делать ведущие физические журналы (например, Physical Review Letters и New Journal of Physics).

Мы очень благодарны за полноводный поток средств на исследования (см. рис. 0.2) от Совета по исследованиям в области инженерных и физических наук Великобритании (EPSRC), Европейской комиссии (FP6 FET Open), Управления НИР ВМС США (ONR), Управления НИР ВВС США (AFOSR), Института фундаментальных вопросов (Foundational Questions Institute – FQXi) и фонда Джона Темплтона (JTF). Последний предоставил особенно щедрое финансирование обоим авторам в процессе работы над книгой. В результате квантовая группа в Оксфорде за 10 лет

с 2004 по 2013 год увеличилась с 5 до 50 человек, а некоторые из тех, кто составлял ее первоначальный костяк, уже создают группы в других местах, разнося по миру благую весть картинок и процессов. Постоянное взаимодействие с квантовой группой (и ее многочисленной диаспорой) было абсолютно необходимым условием для рождения данной книги.

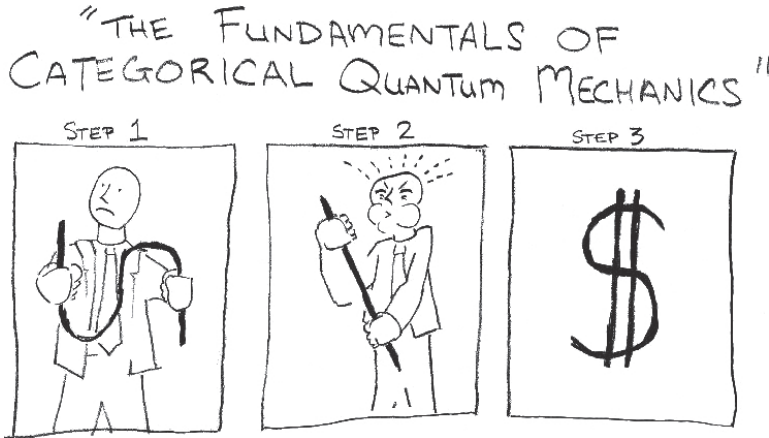


Рис. 0.2 ❖ Тянем-потянем – денежку вытянем

Но как же все-таки возникла идея написать эту книгу? Здесь, в Оксфорде, вообще-то не приветствуется упоминание «того места»¹. Но летом 2012 года издательство Cambridge University Press обратилось к нам с вопросом, не пора ли написать книгу о языке диаграмм. В результате появилась мысль прочесть курс по квантовой информатике, целиком построенный на диаграммах. Заметки к лекциям и составили бы основу для книги, которая, по задумке, должна была быть готова к весне 2013 года. Беглого взгляда на первые две страницы книги достаточно, чтобы понять, что этот план провалился. Заметки к лекциям отправились в мусорную корзину, и осенью 2013 года мы начали все с чистого листа. Получилось то, что вы сейчас читаете.

Пока мы писали книгу, произошло немало всего: один из авторов возобновил музыкальную карьеру, встретил девушку, женился, стал отцом и отправился с ребенком в Пекин, чтобы тот посмотрел, как папа участвует в Metal Show. Тем временем другой автор тоже женился, попробовал себя в разговорном жанре, получил место в Университете Радбауд (у смертельных врагов Боба – голландцев) и отрасли огромную бороду (рис. 0.3). Оба автора приобрели известность у завсегда-таев местного паба как пьянчуги, которых как-то вышибли за порог (ходят слухи, что из-за спора об интерпретации квантовой теории, но ни один из авторов не помнит точно). Они также создали группу не то южной кантри-фолк-музыки, не то индустриального шума под названием Quantum Dagger Orchestra.

¹ Имеется в виду вечный соперник – Кэмбридж. – Прим. перев.

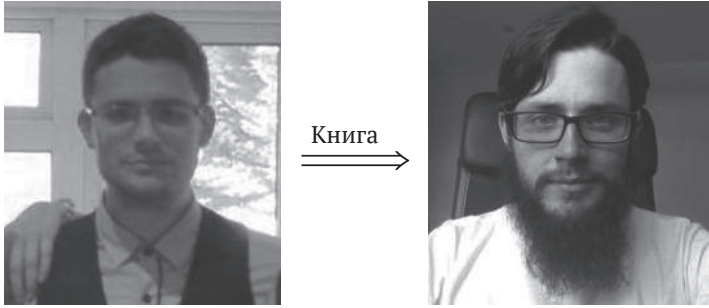


Рис. 0.3 ❖ Корреляция между ростом Алексовой бороды и завершением работы над книгой

Студенты, посещавшие этот курс на протяжении нескольких лет, стали бесценным источником идей и практической информации о том, что годится для преподавания этого новаторского подхода к квантовой теории, а что – нет. Особенно мы хотим поблагодарить студентов Цзянь Нань Чжана (Jiannan Zhang), Уильяма Даттона (William Dutton), Джейкоба Коула (Jacob Cole), Пака Чоя (Pak Choy) и Крэйга Халла (Craig Hull), прослушавших курс в 2013 году, Томаса Хэлгаса (Tomas Halgas) – 2014 год и Эрнеста Окампо (Ernesto Ocampo), Мэтью Пикеринга (Matthew Pickering), Каллума Оукли (Callum Oakley), Эшока Менона (Ashok Menon), Игнасио Функе Прието (Ignacio Funke Prieto) и Бенджамина Доуса (Benjamin Dawes) – 2015 год. Все они внесли вклад в конечный продукт, указав на опечатки в первоначальной и исправленных редакциях заметок к лекциям.

Отдельное спасибо Яареду Аль-Мехайри (Yaared Al-Mehairi), Даниэлю Марсдену (Daniel Marsden), Кэти Кэйси (Katie Casey), Джону-Марку Аллену (John-Mark Allen), Фабрициону Дженовезе (Fabrizio Genovese), Маайке Цварту (Maaike Zwart), Гектору Миллер-Бэйкуэллу (Hector Miller-Bakewell), Джо Болту (Joe Bolt), Джону ван де Ветерингу (John van de Wetering) и Адрия Гаррига Алонсо (Adrià Garriga Alonso), которые внесли значительные по качеству и (или) количеству исправления, а также классным наставникам Мириам Бэкенс (Miriam Backens), Владимиру Замдхиеву (Vladimir Zamdhiev), Уиллу Зенгу (Will Zeng), Джону-Марку Аллену и Чиаран Ли (Ciaran Lee) за ценный общий вклад, модельные решения и за то, что они приняли на себя всю тяжесть разочарования студентов, у которых не получались некоторые «экспериментальные» упражнения.

Подробные исправления окончательной рукописи подготовили неразлучные приятели Джон Хардинг (John Harding) и Франк Фалькенборг (Frank Valckenborgh), а рассерженного Боба фотографировал еще один их собутыльник Росс Данкан (Ross Duncan). Постоянные напоминания Алексу кушать и избегать травм головы были предоставлены его женой Клэр. Боб не обращал внимания на аналогичные напоминания своей жены Сельмы.

Все диаграммы в этой книге созданы с помощью пакета PGF/TikZ для LaTeX и программы TikZiT. Последнюю версию можно скачать с сайта tikzit.github.io.

И напоследок: почему Cambridge University Press, а не Oxford University Press? Потому что своим волшебством книга обязана CUP, тогда как OUP... нечего сказать.

Глава 1

Введение

При нормальных условиях ученый-исследователь занимается не инновациями, а решением задач, и интересуется такими задачами, которые, по его мнению, могут быть поставлены и решены в рамках существующей научной традиции.

– *Thomas Kuhn, The Essential Tension, 1977*

Квантовая теория ставила перед физиками и философами задачи с момента своего рождения в начале XX века. Но с начала 1980-х годов многие ученые перестали спрашивать, почему квантовая теория такая странная, а задалась вопросом:

Что можно сделать со странностью квантового мира?

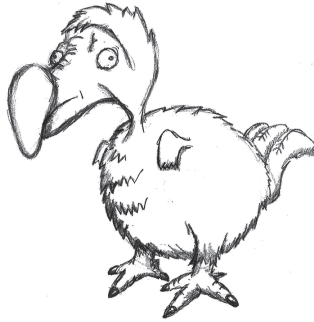
В этой книге мы не только восприняли эту смену точки зрения, но и низвергли других идолов квантовой теории. Мы утверждаем, что следует не только изменить характер вопросов, предъявляемых к квантовой теории, но и

сменить язык, на котором она обсуждается!

Прежде чем принять этот вызов лицом к лицу, мы расскажем коротенькую историю, демонстрирующую, как квантовый мир опровергает то, что принято считать интуитивно очевидным...

1.1. ПИНГВИНЫ И БЕЛЫЙ МЕДВЕДЬ

В квантовой теории рассматриваются весьма специфические физические системы – зачастую очень маленькие – и отличия их поведения от того, к чему мы привыкли в повседневной жизни. К типичным физическим системам, подчиняющимся квантовым законам, можно отнести такие микрочастицы, как фотоны и электроны. Но пока отвлечемся от этого и начнем рассмотрение с более «оперной» квантовой системы. Вот Дэйв:



Это птица додо. Не простой, ничем не примечательный додо, а *квантовый додо*. Будем предполагать, что Дэйв ведет себя так же, как мельчайшая нетривиальная квантовая система, двухуровневая, которую в наши дни принято называть квантовым битом, или *кубитом*. Сравним состояние Дэйва и его классического аналога, *бита*. Биты – это строительные блоки классических компьютеров (мы еще поговорим об этом), а кубиты – строительные блоки квантовых компьютеров. Вот свойства бита:

- 1) допускает два состояния, которые мы привычно называем 0 и 1;
- 2) может быть подвергнут действию любой функции;
- 3) может быть беспрепятственно прочитан.

Слова «может быть подвергнут действию любой функции» означают, что мы можем применить к биту любую функцию, изменяющую его состояние. Например, функция НЕ изменяет состояние на противоположное (0 на 1, 1 на 0), а функция «константа 0» переводит любое состояние в 0. Слова «может быть беспрепятственно прочитан» означают, что мы можем прочитать состояние любого бита в памяти компьютера, ничего не повредив и не изменив это состояние.

Это настолько очевидно, что даже странно писать... но лишь до тех пор, пока мы не сравним с квантовым аналогом. Вот свойства кубита:

- 1) допускает целую сферу состояний;
- 2) может быть подвергнут вращениям этой сферы и никаким другим операциям;
- 3) доступ к нему возможен только со стороны специальных процессов, называемых *квантовыми измерениями*, этот доступ ограничен и отнюдь не безобиден.

Множество состояний, занимаемых системой, называется ее *пространством состояний*. Для классического бита это пространство состоит всего из двух состояний, тогда как у кубита может быть бесконечно много состояний, которые можно наглядно представить в виде сферы. В квантовой теории это пространство состояний называется *сферой Блоха*. Для объяснений подойдет любая сфера, поэтому возьмем просто Землю. На Земле достаточно места для двух состояний бита, так что поместим 0 на Северный полюс, а 1 – на Южный:



Как именно выбрать полюса, не важно, но важно, чтобы они были *диаметрально противоположными* точками сферы – антиподами.

Поскольку к сфере состояний кубита можно применять только вращения, то нельзя одновременно отобразить 0 и 1 в 0 (как в случае классического бита), поскольку такого вращения не существует. С другой стороны, есть масса способов поменять местами 0 и 1, поскольку существует много (различных!) вращений, переворачивающих сферу.

А что такое квантовые измерения? Как и при чтении обычного бита, измерение кубита дает один из двух ответов (например, 0 или 1, отсюда и название кубит). Однако этот акт «измерения» вовсе не так безобиден, как простое чтение бита для получения его значения. Чтобы прочувствовать это, вернемся к Дэйву. Поскольку кубиты могут обитать в любой точке мира, Дэйв – как и одна особенно знаменитая (классическая) птица додо – живет в Оксфорде:



Предположим теперь, что мы хотим установить, где живут определенные животные, при следующих предположениях:

- 1) разрешено только спрашивать, живет ли животное в определенном месте на Земле или в диаметрально противоположном ему;
- 2) все животные могут разговаривать и всегда отвечают «правильно»;
- 3) хищные животные не едят спрашивающего.

Если спросить белого медведя, живет ли он на Северном полюсе или на Южном, тот ответит «на Северном полюсе». Если снова задать тот же вопрос, он опять ответит «на Северном полюсе», потому что именно там живут белые медведи. Аналогично, если спросить пингвина, он будет отвечать «на Южном полюсе» столько раз, сколько мы задаем вопрос.

С другой стороны, что скажет Дэйв, если спросить его, живет ли он на Северном или на Южном полюсе? Дэйв просто не поймет вопроса, но поскольку додо немного туповаты, все равно ответит. Однако, согласно предположению 2, все животные отвечают правильно. Следовательно, раз Дэйв сказал «на Северном полюсе», значит, так оно и есть: он действительно находится на Северном полюсе!



Если повторить вопрос, он снова ответит «на Северном полюсе» и будет твердить это, пока его не съест белый медведь (рис. 1.1). Но если бы он в самом начале сказал «на Южном полюсе», то немедленно там и оказался бы.





Рис. 1.1 ❖ Белый медведь, пытающийся произвести «возмущающее измерение» Дэйва

Так что вне зависимости от ответа Дэйва его состояние изменилось. Информация о том, что первоначально он находился в Оксфорде, утрачена навсегда. Это явление, известное как *коллапс* квантового состояния, имеет место почти для всех вопросов (т. е. измерений), которые мы можем задать. Важно, что коллапс почти всегда *недетерминирован*. Не измерив Дэйва, мы почти никогда не узнаем, окажется ли он на Северном полюсе или на Южном. «Почти», за одним исключением: если спросить Дэйва, находится ли он в Оксфорде или на островах Антиподов, он ответит «в Оксфорде» и останется на месте.

Квантовая теория не может уверенно предсказать судьбу Дэйва, но может вычислить *вероятности* того, куда коллапсирует Дэйв: на Северный полюс или на Южный. В данном случае квантовая теория говорит, что Дэйв с большей вероятностью окажется на Северном полюсе и будет съеден белым медведем, а не на Южном полюсе, где замерзнет в компании пингвинов.

Птицы додо вымерли не без причины...

1.2. Так что же тут нового?

Прошло уже почти сто лет с момента несчастливого путешествия Дэйва на Северный полюс. А в последние двадцать лет мы стали свидетелями резкого подъема интереса к новым исследованиям в квантовой теории, от пересмотра базовых концепций (рис. 1.2) до появления принципиально новых технологий. Хрестоматийный пример – *квантовая телепортация*, когда нелокальные аспекты квантовой теории применяются для передачи квантового состояния на большие (иногда) расстояния, и при этом из классической коммуникации используется малая крошечка (точнее, две малые крошечки – бита...). Квантовая телепортация демонстрирует тонкую связь между квантовой теорией и структурой пространства-времени на самом глубоком уровне. В то же время она является шаблоном важной квантовой вычислительной модели (основанные на измерениях квантовые вычисления) и составной частью многих квантовых коммуникационных протоколов.

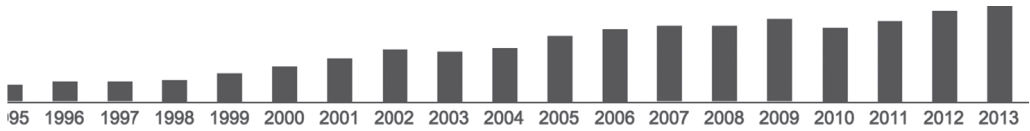


Рис. 1.2 ❖ Согласно Google Scholar, цитируемость статьи Эйнштейна, Подольского и Розена, в которой впервые была описана квантовая нелокальность, за последние двадцать лет многократно возросла, и теперь она стала самой цитируемой статьей Альберта Эйнштейна. А учитывая конкуренцию, это говорит о многом

Квантовая теория в том виде, в котором мы ее теперь знаем – т. е. ее формулировка в терминах *гильбертовых пространств*, – увидела свет в 1932 году в книге фон Неймана «Математические основы квантовой механики». С другой стороны, квантовая телепортация была открыта только в 1992 году. Отсюда вопрос:

Почему для открытия квантовой телепортации понадобилось 60 лет?

Первое объяснение состоит в том, что в рамках традиций физических исследований за эти 60 лет вопрос о том, возможно ли нечто, подобное квантовой телепортации, попросту никогда не задавался. Он стал очевиден, лишь когда исследователи вышли за рамки существующей научной традиции и задали на первый взгляд странный вопрос:

Каковы особенности квантовой теории с точки зрения обработки информации?

Однако можно сделать еще один шаг и спросить, почему для открытия телепортации оказалось необходимо сначала задать этот вопрос. Почему тот факт, что квантовая теория допускает квантовую телепортацию, не был так же очевиден, как то, что молотком можно забивать гвозди? Наш ответ на этот вопрос заключается в том, что традиционный язык гильбертовых пространств не слишком хорош для выражения многих аспектов квантовой теории и, в частности, таких, которые, подобно телепортации, включают взаимодействие нескольких систем во времени и в пространстве. Поэтому мы задаем новый вопрос:

Какой язык больше подходит для рассуждений о квантовой теории?

Именно ответу на этот вопрос и посвящена наша книга. Читатель узнает о многих квантовых особенностях, важность которых возросла в связи с появлением таких новых дисциплин, как квантовые вычисления, квантовая информация и квантовые технологии, и о том, как эти разработки идут рука об руку с возрождением интереса к изучению оснований квантовой теории. Все это будет сделано с помощью новаторского представления квантовой теории с помощью диаграмм. Мы не только создадим двумерную нотацию для описания квантовых процессов и рассуждений о них, но и опишем уникальную методику, позволяющую обращаться с квантовыми процессами и, что особенно важно, с *композициями* квантовых процессов, как с полноправными гражданами.

1.2.1. Новое отношение к квантовой теории: особенности

С момента возникновения квантовой теории многие выдающиеся мыслители испытывали от нее глубокое неудовлетворение. В начале XX века были приложены колоссальные усилия и привлечена изощренная математика, чтобы преде-

монстрировать наличие *парадоксов* в квантовой теории. Все началось со ставшей знаменитой работы Эйнштейна, Подольского и Розена (ЭПР), написанной в 1935 году, в которой утверждалось, что квантовое состояние дает «неполное описание» физической реальности. Грубо говоря, по их мнению, чего-то не хватает, чтобы придать квантовой теории смысл, не противоречащий нашим традиционным интуитивным представлениям. Однако в 1964 году Джон Белл показал, что любая попытка «пополнить» квантовую теорию согласно стандартам ЭПР обречена на неудачу, и тем самым похоронил традиционные интуитивные представления о квантовой теории. Белл показал, что в самих основаниях квантовой теории таится фундаментальная неустранимая нелокальность (рис. 1.3).

Если теория относительности привела Эйнштейна к красивому и элегантно-му описанию Вселенной в макроскопическом масштабе, то квантовая теория, казалось, только замутила воду. И эта фраза более-менее точно характеризует восприятие квантовой теории большинством ученых. Есть два основных способа преодолеть неудовлетворенность «квантовой странностью». Первый – просто игнорировать концептуальные сложности. Такое отношение превалировало в сообществе физики элементарных частиц, провозгласившем лозунг «заткнись и считай». Альтернатива – с головой погрузиться в концептуальные проблемы, окружающие квантовую теорию, пожертвовав большую часть жизни (не говоря уже о рассудке) на их «исправление».

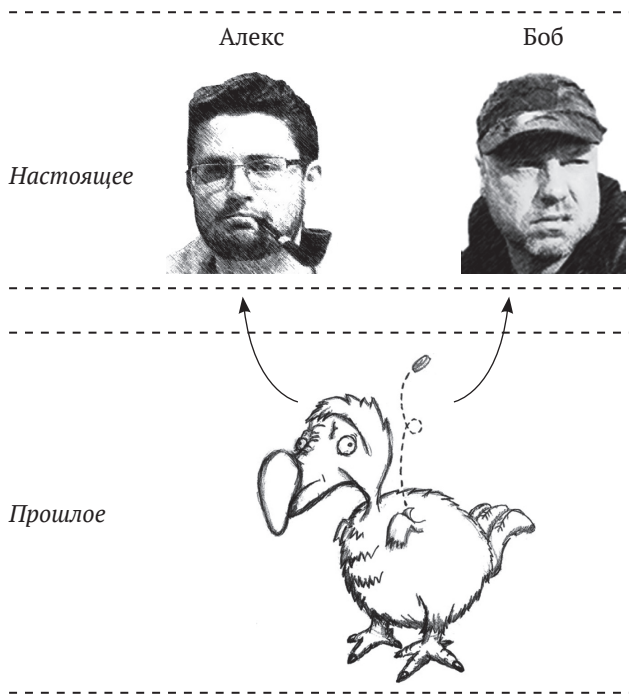


Рис. 1.3 ❖ Нелокальность квантовой теории означает, что квантовые особенности невозможно объяснить средствами классической вероятностной модели. Иными словами, существуют ситуации (не та, что описана выше), когда удаленные наблюдатели, производящие квантовые измерения, видят статистические корреляции, которые нельзя объяснить общей причиной



Рис. 1.4 ❖ Алиса спрашивает Дэйва об отношениях Алекса и Боба

Затем в начале 1980-х годов произошел важный перелом в отношении, который можно свести к простому вопросу:

А что, если так называемые дефекты квантовой теории на самом деле особенности?

Иными словами, пришло понимание того, как много можно выиграть, если принимать квантовую теорию такой, как она есть, и попытаться уяснить, как использовать «квантовую странность» во благо. Можно даже надеяться, что это позволит нам лучше познакомиться с квантовостью, привыкнуть к ее странностям, и, быть может, вновь обретенная не столь традиционная интуиция даже начнет наполняться смыслом.

И действительно, квантовая нелокальность, которую Эйнштейн когда-то воспринимал как некое нежелательное «жуткое дальное действие», внезапно оказалась ключевым ресурсом. Фактически за много лет до того, как программисты стали использовать приведенную выше фразеологию для оправдания собственной лени при отладке («Это не дефект, а особенность!»), Ричард Фейнман уже указал, что есть, по крайней мере, одна вещь, в которой квантовые системы по-настоящему хороши: моделирование квантовых систем! Оказывается, что эту задачу весьма трудно решить с помощью обычного классического компьютера. На протяжении последующих десятилетий ученые открыли множество странных и удивительных вещей, на которые способны квантовые системы: отправлять защищенные сообщения, телепортировать физические системы, эффективно разлагать большие числа на простые множители.

Вновь вспыхнувший интерес к квантовым особенностям породил несколько новых дисциплин: квантовые вычисления – как можно использовать квантовые системы для вычислений; квантовая теория информации – каковы последствия включения квантовых явлений в сбор и передачу информации; квантовые технологии – как практически создавать устройства, в которых квантовые особенности применяются для того, чтобы сделать нашу жизнь лучше.

```

0 0 1 1 0 1 0 0 1 1 1 0 1 0
0 1 0 1 0 1 0 0 1 0 0 1 0 0
1 0 1 0 0 1 0 1 0 0 0 1 0 0
0 1 1 1 0 0 1 1 1 0 0 0 1 1
1 0 0 0 1 0 0 0 0 1 1 0 1 0
0 1 1 0 0 1 1 1 1 0 1 0 0 1 0
0 1 1 1 0 1 0 0 0 1 0 1 0 1 0
1 1 0 1 0 0 0 0 1 0 1 0 1 0
0 1 0 1 0 1 0 0 0 1 0 1 0 1 0
0 1 0 0 1 1 0 1 0 0 0 1 1 0 1
1 0 0 1 1 0 1 0 1 0 0 0 1 1 0
0 1 0 0 1 0 0 1 1 0 0 0 0 1 1
1 1 0 0 0 1 1 0 1 0 1 1 1 0
0 1 0 1 1 1 0 1 1 0 1 0 0 0

```

против

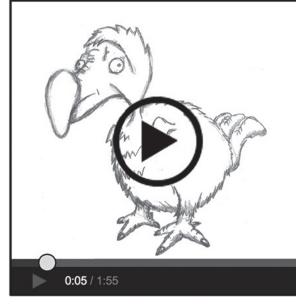


Рис. 1.5 ❖ Сравнение низкоуровневого и высокоуровневого представлений цифровых данных, присутствующих в вычислительном устройстве

1.2.2. Новый вид математики: диаграммы

Подчеркнем, что открытие новых квантовых явлений было делом нетривиальным, и в нем участвовали весьма одаренные люди. Рискнем сделать смелое заявление: если принять язык, подходящий для квантовой теории, то эти явления бросаются в глаза. Напротив, традиционный язык квантовой теории, гильбертово пространство, является серьезным препятствием на пути к открытию таких явлений. Чтобы понять, почему это так, воспользуемся простой метафорой.

Представьте, что вы пытаетесь определить, что снято на видео, глядя лишь на его цифровую кодировку (рис. 1.5). Очевидно, что это практически невыполнимая задача. Хотя цифровые данные, т. е. последовательности нулей и единиц, действительно являются рабочей лошадкой технологии и хотя «в принципе» можно понять, как с их помощью закодированы мультимедийные файлы на вашем жестком диске, поручение декодировать конкретную двоичную последовательность больше напоминает наказание для корыстолюбивых банкиров и коррумпированных политиков, чем решение интересной задачи.

Разумеется, даже от опытного программиста не ждут прямой работы с двоичными данными. Где-то по пути к современному программированию был придуман язык ассемблера, который позволяет переводить понятное человеку (не всякому) представление в команды процессора. И хотя при этом писать программы, управляющие компьютером, стало проще, все равно, чтобы понять, что делает кусок кода на ассемблере, придется не раз почесать затылок. Использование *низкоуровневых языков* типа языка ассемблера создает искусственный барьер между программой и выражаемой ей концепцией и ставит практические пределы сложности задач, решаемых программами. Поэтому сегодня практически все программисты пишут на *высокоуровневых языках* (рис. 1.6).

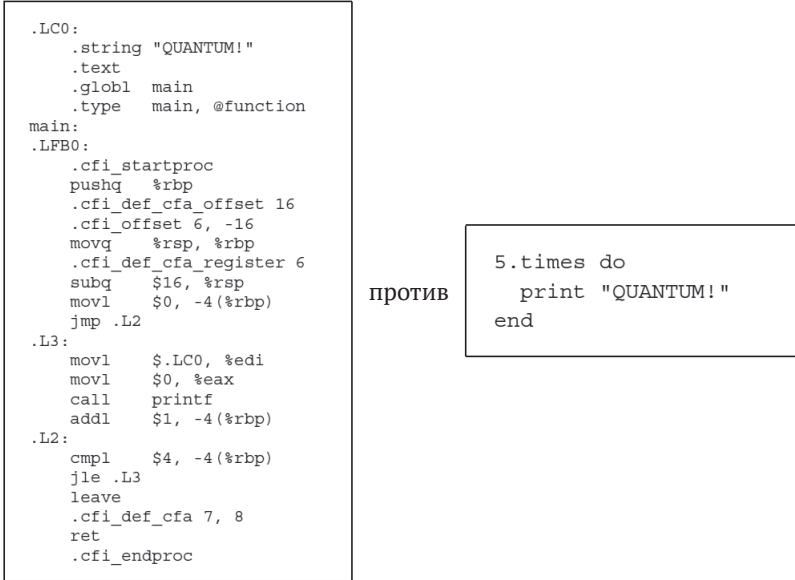


Рис. 1.6 ❖ Сравнение низкоуровневого и высокоуровневого языков программирования. Обе программы, слева и справа, решают одну и ту же задачу, но первая написана на низкоуровневом языке ассемблера x86, а вторая на высокоуровневом языке Ruby

А «открытие новых квантовых явлений» в терминах традиционного (т. е. низкоуровневого) языка квантовой теории, а именно «последовательностей комплексных чисел» (вместо «последовательностей нулей и единиц»), ничуть не легче. Этим и объясняется тот факт, что для открытия квантовой телепортации потребовались усилия шести авторитетнейших ученых, и произошло это спустя 60 лет после создания формализма квантовой теории. С другой стороны, язык диаграмм, который мы используем в этой книге, является *высокоуровневым* языком для исследования квантовых явлений (рис. 1.7). Вскоре мы увидим, что стоит принять его в качестве языка квантовой теории, как явления наподобие квантовой телепортации станут очевидны!

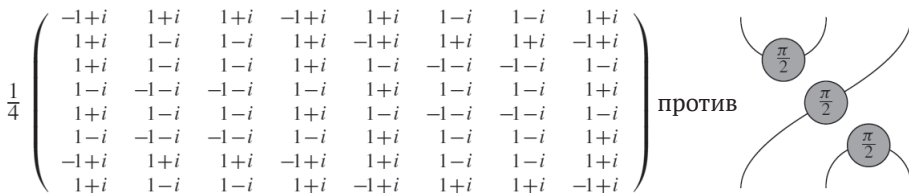


Рис. 1.7 ❖ Сравнение низкоуровневого и высокоуровневого языков квантовых процессов аналогично сравнению низкоуровневого и высокоуровневого представлений данных на рис. 1.5 и сравнению низкоуровневого и высокоуровневого языков программирования на рис. 1.6

Хотя это и выходит за рамки книги, стоит отметить, что используемый нами язык диаграмм нашел применения и в других областях, например моделирование

смысла в естественном языке (рис. 1.8), проведение доказательств в формальной логике, теория управления и моделирование электрических схем.

Диаграммы становятся все более важным инструментом исследования в таких экзотических разделах чистой математики, как теория узлов, теория представлений и алгебраическая топология. С помощью диаграмм мы устраняем из представлений математических объектов огромный объем избыточного синтаксического мусора (рис. 1.9), что позволяет сосредоточиться на важных свойствах самих объектов.

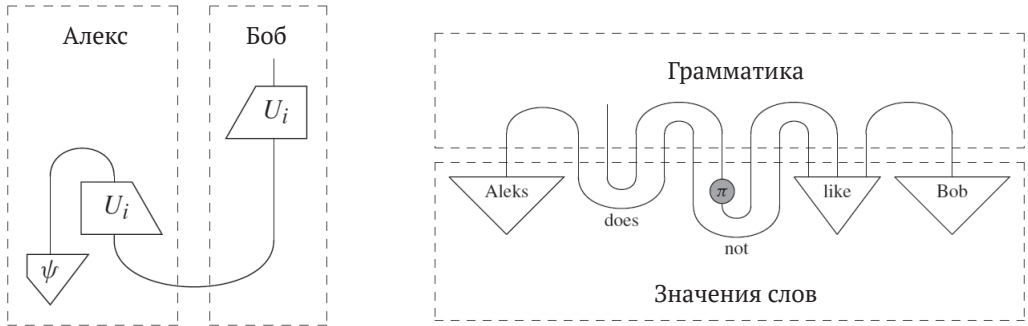


Рис. 1.8 ❖ Сравнение диаграммных представлений квантовых процессов с диаграммами «потока смысла» в естественном языке. Хотя контексты сильно различаются, Алекс и Боб отлично чувствуют себя в обоих благодаря схожести диаграмм. В диаграмме, относящейся к естественному языку, верхняя часть представляет грамматическую структуру, нижняя – значения отдельных слов, а связи показывают, как значения слов взаимодействуют, порождая смысл всего предложения

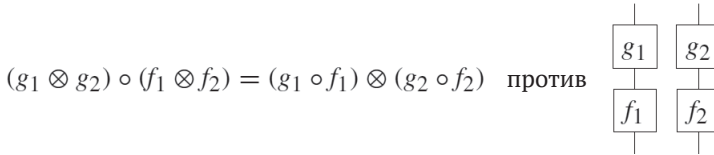


Рис. 1.9 ❖ Два разных синтаксических описания одной и той же диаграммы. На символическом языке слева два синтаксически неодинаковых выражения, возможно, означают одно и то же. С другой стороны, на графическом языке справа существует только одно представление. Этот пример подробно обсуждается в разделе 3.2.4

Имеются ясные признаки того, что роль диаграммных рассуждений в науке в целом неуклонно возрастает, и эта книга – первая попытка дать полное изложение такого большого предмета, как квантовая теория, исключительно на этом новом языке. Прочитав эту книгу – а еще лучше прослушав курс на ее основе, – вы, подобно обезьянам, запущенным в космос в 1960-х годах, станете «первыми покупателями» (или «подопытными экземплярами») в этом совершенно новом магазине.

1.2.3. Новое основание физики: процессные теории

Приняв диаграммный язык в качестве формальной основы для описания квантовой теории (или любой другой физической теории), мы соглашаемся по-новому взглянуть на физические теории.

Прежде всего в традиционных физических системах во главу угла ставится понятие «состояния системы», тогда как в диаграммных теориях естественно трактовать произвольные процессы наравне с состояниями. Состояние в этом случае рассматривается как частный случай процесса – процесс «подготовки». Иными словами, происходит сдвиг от вопроса «чем является» к вопросу «что происходит», что, очевидно, сулит больше интересного. Здесь можно провести аналогию с информатикой, в которой время и силы тратятся в основном на рассуждения о процессах (т. е. программах), а состояния (данные) нужны лишь для того, чтобы программы их использовали и обменивались ими. Также становится ясно, что акцентировать внимание следует не на отдельных программах, а на совокупностях *взаимодействующих* программ – только так можно понять комплексные распределенные компьютерные системы, которые играют все более важную роль в современном мире.

Еще один пример, когда изучение взаимодействий критически важно для понимания системы, возникает в биологии. Хотя в принципе информацию об оперении птицы можно вывести из ее генетического кода, это не объясняет, почему у нее именно такое оперение. С другой стороны, если посмотреть, где обитает животное и как оно привлекает партнера, то ответ на этот вопрос сразу становится очевиден. Так и наш подход к физике основан на изучении не отдельных систем, а общей структуры и композиции многих систем и процессов. Таковую структуру, состоящую из всех «допустимых процессов» и их взаимодействий, мы называем *процессной теорией*.

Шрёдингер довольно рано осознал, что самые поразительные неклассические особенности квантовой теории проявляются при рассмотрении не одной системы, а совместного поведения нескольких систем. Квантовые системы не ведут себя как совокупность индивидуумов, а устанавливают сложные взаимосвязи, благодаря которым становятся возможны удивительные вещи:

Если две системы, о состоянии которых нам известно по их представителям, вступают во временное физическое взаимодействие, обусловленное известными действующими на них силами, и если по прошествии некоторого периода взаимовлияния системы снова разделяются, то их уже нельзя описать так же, как прежде, а именно наделив каждую собственным представителем. Я бы назвал это не одной из, а самой характерной чертой квантовой механики – той, что вынуждает отказаться от классических способов рассуждения.

Шрёдингер говорит, что самая важная характеристика квантовой механики становится видна только при изучении взаимодействия двух систем. Поэтому можно было бы ожидать, что любой подход к квантовой теории должен начинаться с повышенного внимания к композиции. Но странно – ни в одном выбранном наугад учебнике по квантовой механике такая точка зрения не встречается. И лишь в конце 1990-х годов – в немалой степени благодаря открытиям, о которых мы сказали в разделе 1.2.1, – эта идея вновь стала приоритетной.

Разумеется, концепция процессной теории выдвигает композицию на первый план и предлагает естественный способ рассуждения о процессах. Следует уделять меньше внимания низкоуровневым аспектам математического определения процессов, а сосредоточиться на поиске высокоуровневых принципов, управляющих их взаимодействием. В совокупности эти принципы составляют то, что можно назвать *логикой взаимодействия* в процессной теории. Фон Нейман также

полагал, что квантовую теорию следует интерпретировать в терминах логических принципов. Спустя три года после публикации «Математических основ» фон Нейман писал:

Я хочу сделать признание, которое может показаться аморальным: «Я больше абсолютно не верю в гильбертово пространство».

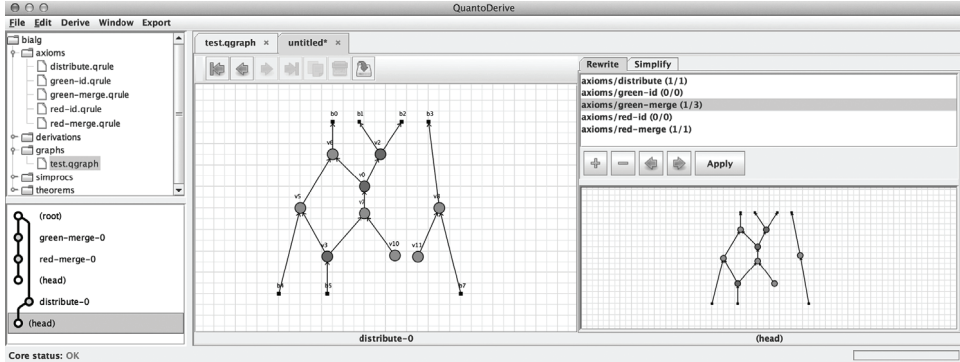


Рис. 1.10 ❖ Quantomatic: средство доказательства теорем с помощью диаграмм

Далее он пишет, что физический смысл в квантовой теории имеет не структура гильбертова пространства, а квантовый аналог «логических суждений» (пропозиций), т. е. свойства, которые можно проверить с помощью квантовых измерений. Однако этому новому виду логики, названному *квантовой логикой*, не удалось заменить гильбертово пространство в качестве концептуальной основы квантовой теории. И основным препятствием стала концентрация на отдельных системах и неспособность включить в концепцию композицию систем. С прагматической точки зрения, переход от гильбертова пространства к квантовой логике затруднил установление новых фактов и открытие новых квантовых особенностей, даже для установления базовых фактов от его адептов требовалась незаурядная изобретательность.

Напротив, новый вид логики взаимодействия, основанный на процессных теориях, быстро стал практическим инструментом высокоуровневых рассуждений о квантовых системах, и не только – не в последнюю очередь благодаря интуитивно понятному языку диаграмм. Он даже лег в основу диаграммного *доказывателя теорем* – интерактивной программы Quantomatic, которая автоматически или полуавтоматически строит доказательства (рис. 1.10).

Так как же мы назовем этот новый способ рассуждения о квантовой теории, опирающийся исключительно на диаграммы и делающий акцент на процессах и логике их взаимодействия? Поскольку термин «квантовая логика» уже занят, придется использовать чуть более образное название...

1.2.4. Новая парадигма: квантовый пикторализм

В разделе 1.2.1 мы говорили, что неудовлетворенность квантовой теорией мешала осознать, что на самом деле является квантовыми особенностями и как их можно применить во благо. Впоследствии, задавая правильный «позитивный» вопрос, удалось открыть много новых особенностей. Далее мы высказали утверждение,

что при наличии адекватного математического языка квантовые особенности стали бы очевидны. Можно сделать еще один шаг и спросить себя: «А быть может, такой математический язык не просто удобнее для работы, но и ближе к тем элементам, из которых состоит мир?»

Святым Граалем теоретической физики является построение теории квантовой гравитации. Очень может быть, что для разработки непротиворечивой теории квантовой гравитации придется ослабить некоторые ключевые предположения квантовой теории. Стандартная формулировка теории на основе гильбертова пространства предстает в виде неразрывного целого, поэтому необходимо найти альтернативное представление, которое позволило бы отделить существенные свойства от случайных. Следовательно, представление, соответствующее истинному миру, имело бы чрезвычайную важность.

До недавнего времени едва ли не все попытки найти такое представление страдали уже упомянутыми выше навязчивыми идеями, т. е. в качестве отправной точки брали какой-то дефект квантовой теории:

- *C**-алгебры: некоммутативность «квантовых наблюдаемых»;
- квантовая логика: недистрибутивность «квантовых пропозиций»;
- квантовая теория меры: неаддитивность «квантовых мер».

(Просим прощения за математический жаргон.) Точный смысл всего вышеперечисленного неважен, важно лишь, что во всех этих подходах на первое место выдвигается свойство, которым квантовая теория не обладает. И что с этим делать? Насколько полезно знать, что рыба не является птицей додо? Не очень полезно, поскольку отвертка – тоже не додо.

Вместо того чтобы ставить во главу угла свойства, которых у квантовой теории нет, следует поискать новые уникальные возможности, предлагаемые квантовой теорией. Мы утверждаем, что самые интересные свойства квантовой теории – диаграммные, что подводит нас к первому «определению» в этой книге.

Определение 1.1. Под *квантовым пикторализмом* понимается использование диаграмм для описания и рассуждения обо всех существенных особенностях взаимодействующих квантовых процессов таким образом, что диаграммные равенства становятся фундаментальной основой квантовой теории.

Теперь взглянем на квантовый пикторализм в действии. Рассмотрим следующий дефект квантовой теории: «Состояние двух квантовых систем в общем случае невозможно разделить на независимые состояния систем *A* и *B*». По-другому то же самое можно выразить так: мы можем «засвидетельствовать» неразделимость, заметив, что существуют *максимально запутанные состояния* двух систем, что можно лаконично охарактеризировать одним (очень полезным!) графическим равенством (рис. 1.11).

Второй «позитивный» эффект, изучаемый в этой книге, – *существование дополнительных измерений*. Соответствующее «негативное» утверждение состоит в том, что многие квантовые измерения не являются *совместимыми* (т. е. не могут быть произведены одновременно). На самом деле упомянутые выше некоммутативность и недистрибутивность как раз и призваны уловить эту несовместимость измерений. Напротив, *максимальная несовместимость*, выраженная вторым равенством на рис. 1.11, представляет реальное квантовое поведение, которое можно наблюдать экспериментально и использовать, например, при проектировании квантовых протоколов безопасности.



Рис. 1.11 ❖ Две квантовые особенности, «существование максимально запутанных состояний» и «существование дополнительных измерений», в терминах графических примитивов. Этим особенностям посвящены соответственно главы 4 и 9

Теперь можно даже спросить, достаточно ли таких особенностей, чтобы полностью охарактеризовать квантовую теорию. Можно ли построить новый формализм квантовой теории, в котором аксиомы, представляющие существенные физические свойства, определяются с помощью элегантных диаграмм? Хотя эта история еще далеко не закончена, ответ, похоже, утвердительный. Мы надеемся, что в процессе чтения данной книги вы испытаете такое же удовольствие от установления этого факта, какое когда-то испытали мы.

1.3. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

В конце каждой главы, в том числе и этой, мы приводим краткую историческую справку по изложенному в ней материалу. В этой вводной главе мы затронули много вещей, которые будут подробнее рассмотрены в последующих главах, поэтому раздел получился довольно объемным.

Прежде всего несколько слов о птицах додо. Они вымерли в 1680 году. Останки единственного сохранившегося экземпляра додо ныне покоятся в Музее естественной истории Оксфордского университета. Поэтому появление додо Дэйва – дань уважения как к «оксфордскому додо», так и к другому знаменитому додо, выведенному в психоделическом путешествии Алисы в Страну чудес нашим собратом по Оксфорду и специалистом по математической логике Льюисом Кэрроллом (Carroll, 1942). Так вышло, что наш герой погребен меньше чем в 100 метрах от места, где впервые был экспериментально продемонстрирован квантовый алгоритм (Jones et al., 1998), а также от помещения, в котором была написана эта книга.

Настоящие квантовые системы, в отличие от воображаемых квантовых додо, впервые были идентифицированы как таковые Максом Планком (Max Planck, 1900), работа которого дала толчок растянувшимся на 30 лет попыткам построить формализм квантовой теории в том виде, в котором мы его сейчас знаем, и в конечном итоге привела к квантовой теории в формулировке фон Неймана, основанной на гильбертовом пространстве и линейных отображениях (von Neumann, 1932). Вышедшие с тех пор стандартные учебники квантовой теории по-прежнему очень напоминают оригинал – конечно, за исключением этого!

Статья ЭПР (Einstein et al., 1935) чаще всего трактуется как неудовлетворенность Эйнштейна квантовой теорией. Сам Эйнштейн никогда не подтверждал своего авторства формулировок в статье ЭПР и позже опубликовал статью только от своего имени (Einstein, 1936). Как было отмечено выше, статья ЭПР ныне считается первой работой, указывающей на квантовую нелокальность, поскольку в ней явно подчеркнута противоречие между квантовой теорией и предположе-

нием о «локальном реализме». Джон Белл (1964) усилил это утверждение, доказав общую теорему о локально реалистичных моделях и показав, что если квантовая теория корректна, то она обязана нарушать предположение о локальном реализме. Современная концепция локального реализма заключается в том, что вероятностные корреляции между событиями, наблюдаемыми в разных местах, можно объяснить классической причинно-следственной вероятностной моделью (см., например, Pearl, 2000). Даже в наши дни поиск уточнений и обобщений теоремы Белла является областью активных исследований (см., например, Wood and Spekkens, 2012).

Важно, что версия Белла допускает экспериментальную проверку, и нарушение локального реализма было много раз подтверждено экспериментально, начиная с работ Aspect et al. (1981, 1982). Таким образом, экспериментально установлено, что мир действительно «нелокален», как и предсказывала квантовая теория. Отметим, что против первоначального эксперимента выдвигался ряд возражений, указывающих на логические изъяны этой конкретной демонстрации нелокальности. Но с тех пор на все возражения дали ответы другие эксперименты (Weihs et al., 1998; Rowe et al., 2001; Hensen et al., 2015). Вообще, число различных экспериментов, подтверждающих ту или иную форму квантовой нелокальности, мягко говоря, впечатляет (см., например, Rauch et al., 1975; Zeilinger, 1999; Pan et al., 2000; Gröblacher et al., 2007).

Статья ЭПР способствовала также поиску интерпретаций квантовой теории. Поскольку ЭПР заявляла о неполноте квантовой теории, одно семейство интерпретаций ставило задачей пополнение теории, хотя, согласно теореме Белла, любая такая попытка по необходимости должна быть нелокальной. Наиболее известна интерпретация Дэвида Бома (David Bohm, 1952a, b) со скрытыми параметрами. Другая, излюбленная Голливудом, интерпретация со множественными мирами принадлежит Хью Эверетту III (Hugh Everett III, 1957). По умолчанию официальной считается Копенгагенская интерпретация Нильса Бора и Вернера Гейзенберга, хотя в глазах многих это и не интерпретация вовсе, поскольку, на первый взгляд, она не содержит ничего, кроме рецепта вычисления вероятностей. Подробный обзор и развернутое обсуждение интерпретаций квантовой теории можно найти в работе Bub (1999).

Лозунг «заткнись и считай» часто приписывается Ричарду Фейнману, который действительно воплощал его в своей работе, но на самом деле его провозгласил в мае 2004 года Дэвид Мермин (David Mermin), который вообще-то вовсе не прятался от фундаментальных вопросов квантовой теории. Он употребил этот термин, имея в виду не общую практику, принятую в физике элементарных частиц, а для того чтобы выразить свое отношение к Копенгагенской интерпретации (Mermin, апрель 1989).

Раз уж мы заговорили о Фейнмане, отметим, что он первым понял, что есть нечто такое, в чем квантовые системы действительно хороши: моделирование их самих (Feynman, 1982). Таким образом, его концепция квантового эмулятора сохранила первые ростки идеи квантовых вычислений. Открытие не столь самореперентных применений квантовых особенностей в обработке информации началось через несколько лет с появлением квантового распределения ключей (Bennett and Brassard, 1984). Год спустя в Оксфордском университете Дэвид Дойч (David Deutsch, 1985) сформулировал понятие универсального квантового компьютера –

квантового аналога универсальной машины Тьюринга (Turing, 1937). Это повлекло за собой открытие квантовых алгоритмов, значительно превосходящих все классические по производительности (Deutsch and Jozsa, 1992; Shor, 1994; Grover, 1996; Simon, 1997). Термин «кубит» ввел в обиход Шумахер (Schumacher, 1995).

Квантовая телепортация предложена в работе Bennett et al. (1993), а ее первая экспериментальная реализация описана в работе Bouwmeester et al. (1997). Вопрос о том, почему для открытия квантовой телепортации понадобилось 60 лет, был задан одним из авторов этой книги на семинаре в Институте теоретической физики Периметр, и на него сразу же дал ответ оказавшийся в аудитории Жиль Брассар (Gilles Brassard), один из авторов квантовой телепортации и первопроходец в области квантовой информации вообще. Он сказал, что прежде никто не занимался квантовыми особенностями в применении к обработке информации, поэтому и вопрос такой не возникал. Этот обмен мнениями документирован в работе Coecke (2005).

Используемые в этой книге диаграммы являются обобщением диаграмм Роджера Пенроуза (Roger Penrose, 1971), который ввел их в качестве альтернативы обычной тензорной нотации (см. раздел 3.6.1). Однако и до, и после этого было изобретено много подобных диаграммных языков.

Блок-схемы в теории языков программирования были одним из первых абстрактных представлений программ и алгоритмов. Эти блок-схемы, появившиеся в работе Gilbreth and Gilbreth (1922) под названием «диаграммы процессов», широко используются и во многих других дисциплинах. В квантовой информации применение диаграммных представлений началось с квантовых схем – нотации, заимствованной у схем, состоящих из логических вентилях, и дополненной рядом новых чисто квантовых вентилях (см., например, Nielsen and Chuang, 2010).

Диаграммная нотация, специально ориентированная на процессы, отвечающие за квантовую странность, впервые была введена в работах Coecke (2003, 2014a) и независимо в работе Kauffman (2005). Под эти диаграммы был подведен аксиоматический фундамент в работе Abramsky and Coecke (2004) и независимо в работе Baez (2006). Это проложило путь диаграммному подходу к квантовой теории в целом. Основными столпами, поддерживающими возведенное в этой книге здание, являются диаграммное представление смешанных состояний и вполне положительных отображений Селинджера (Selinger, 2007), диаграммное представление классических данных в виде «пауков» в работах (Coecke and Pavlovic, 2007; Coecke et al., 2010a), диаграммное представление фаз, дополнительной и введение сильной дополнительной, опять же в терминах пауков, в работе Coecke and Duncan (2008, 2011) и постулат о причинности, сформулированный в работе Chiribella et al. (2010). Термин «квантовый пикторализм» впервые предложен в работе Coecke (2009).

Перечислим важные темы в области квантовых вычислений и примыкающих к ней, которые были исследованы с помощью диаграмм: квантовые схемы (Coecke and Duncan, 2008), квантовые вычисления на основе (топологических) измерений (Coecke and Duncan, 2008; Duncan and Perdrix, 2010; Horsman, 2011), квантовое исправление ошибок (Duncan and Lucas, 2013), квантовый обмен ключами (Coecke and Perdrix, 2010; Coecke et al., 2011a), нелокальность (Coecke et al., 2011b, 2012) и квантовые алгоритмы (Vicary, 2013; Zeng and Vicary, 2014).

К структурным теоремам квантовой теории, вытекающим из диаграммного подхода, относятся теоремы о полноте (Selinger, 2011a; Duncan and Perdrix, 2013; Backens, 2014a; Kissinger, 2014b) и некоторые теоремы о представлении (Kissinger, 2012a; Coecke et al., 2013c).

Из рассматриваемых нами применений такого рода диаграмм к другим научным дисциплинам упомянем работы Coecke et al. (2010c) и Sadrzadeh et al. (2013) – естественные языки, Mellies (2012) – логика в информатике, Pavlovic (2013) – вычислимость, Hinze and Marsden (2016) – программирование, Baez and Fong (2015) – электрические схемы, Bonchi et al. (2014a) и Baez and Erbele (без даты) – теория управления, Hedges et al. (2016) – приложения теории игр в экономике, Baez and Lauda (2011) – протоистория, Baez and Stay (2011) – розеттский камень, Coecke (2013) – альтернативное Евангелие.

Обсуждение неудовлетворенности фон Неймана гильбертовым пространством приведено в работе Redei (1996), из которой мы заимствовали вторую из двух цитат в разделе 1.2.3. Попытки модификации, обобщения и аксиоматизации квантовой теории, в значительной степени вдохновленные квантовой логикой (Birkhoff and von Neumann, 1936), начались с работ Mackey (1963), Jauch (1968), Foulis and Randall (1972), Piron (1976) и Ludwig (1985). В работе Coecke et al. (2000) приведен их обзор. В работе Stubbe and van Steirteghem (2007) доходчиво описано, как решетки свойств приводят к гильбертову пространству. Обзор формализма «тестового пространства» (или «формализма мануалов») Фоулиса и Рэндалла приведен в работе (2000). Подход Людвиг в последнее время вновь стал популярен под названием «обобщенные вероятностные теории» (Barrett, 2007). Кроме того, несколько исследователей предприняло попытки объединить прежние аксиоматические подходы с диаграммами и (или) композиционной структурой (Harding, 2009; Heunen and Jacobs, 2010; Jacobs, 2010; Vicary, 2011; Abramsky and Heunen, 2012; Coecke et al., 2013a, b; Tull, 2016).

Идея о придании процессам привилегированной роли в квантовой теории уже встречалась в работах Whitehead (1957) (см. цитату в начале главы 6) и Bohr (1961), а в работе Bohm (1986) вышла на первый план. Онтологии процессов восходят еще к досократовым временам и прежде всего к Гераклиту Эфесскому, жившему в VI в. до н. э. (см. цитату в начале главы 2). Диаграммы, а следовательно, привилегированная роль процессов и их композиций, служат холстом для построения физических теорий в работах Chiribella et al. (2010), Coecke (2011) и Hardy (2011, 2013b).

Первая цитата в разделе 1.2.3 – о роли композиции в квантовой теории – взята из работы Schrödinger (1935). Первой настоящей «логикой взаимодействия» была *геометрия взаимодействия* из работы Jean-Yves Girard (1989), которая была переформулирована в виде, больше напоминающем язык, используемый в этой книге, в работе Abramsky and Jagadeesan (1994) и затем в работе Duncan (2006). Тот факт, что квантовый пикторализм можно рассматривать как логику взаимодействия, обосновывается в работе Coecke (2016), исходя из того, что корнями логики является язык, а использование логики – это искусственное рассуждение. Диаграммный доказыватель теорем Quantomatic описан в работе (Kissinger and Zamdzhiev, 2015) и во время написания этой книги еще активно разрабатывался. Его можно скачать с сайта проекта quantomatic.github.io.

Глава 2

Как читать эту книгу

Все течет, все меняется.

– Гераклит Эфесский, 535–475 гг. до н. э.

2.1. Кто вы и чего вы хотите?

Существует множество книг по квантовой теории и квантовым особенностям, но эта уникальна, т. к. основана на квантовом пикторализме.

Предварительные условия. Да их почти и нет. Мы не ожидаем, что читатель хорошо знаком с физикой или информатикой либо имеет основательную подготовку по математике. В принципе, знаний математики в объеме средней школы будет достаточно.

Так, основы линейной алгебры (и, конечно, квантовой теории) излагаются с нуля в форме диаграмм. Но это не значит, что первая половина книги будет скучной для специалиста, поскольку это изложение радикально отличается от привычного.

Целевая аудитория. Благодаря низким требованиям к начальному уровню читателя, а также уникальной форме и содержанию этот учебник рассчитан на широкую аудиторию – от студентов до специалистов в самых разных областях: физике, информатике, математике, логике, философии науки, а также на исследователей, работающих на стыке наук, в т. ч. биологов, инженеров, когнитивистов и педагогов.

В особенности книга адресована студентам и исследователям в области квантовых вычислений и квантовой информации, поскольку мы применяем инструменты квантового пикторализма непосредственно к этим дисциплинам. Исследователь, практически занимающийся квантовыми вычислениями, может открыть для себя новый арсенал средств для решения задач, которые не поддавались традиционным методам, а студент, возможно, обнаружит, что некоторые предметы объясняются гораздо понятнее.

Еще одна целевая аудитория состоит из студентов и специалистов, интересующихся основаниями и (или) философией физики. Из этой книги они узнают о процессо-ориентированном подходе к физике, когда композиция систем считается полноправным субъектом, а не производным понятием. В частности, это первая книга, в которой язык диаграмм используется, чтобы отразить идею процессной теории и поставить такие теории на место нового основания квантовой теории, позволяющего выразить все ее стандартные понятия.

Книга также будет интересна специалистам по логике и информатике, для которых диаграммы могут стать новым видом логической парадигмы, подчеркивающей примат «композиции» над «пропозицией» (суждением). Для них изучение квантовой теории может стать дополнительным бонусом к знакомству с этой новой парадигмой разработки теорий.

Но поскольку этот учебник включает все, что должно быть представлено в стандартном учебнике по квантовым вычислениям и основаниям квантовой теории, его можно использовать и как введение в эти дисциплины. И хотя наша нотация отличается от употребляемой в других учебниках, книга все же охватывает учебную программу первого курса по квантовым вычислениям, и мы прилагаем усилия, чтобы связать новые концепции и обозначения с теми, что традиционно используются в литературе.

Кроме того, эту книгу можно рассматривать как введение в диаграммные рассуждения, и, пожалуй, это первая книга, где данная тема затрагивается.

2.2. МЕНЮ

Пока мы еще не можем предложить стейк из додо, но благодаря недавним научным достижениям, быть может, недалек тот день, когда голуби дадут жизнь новым Дэйвам и Дэйветтам.

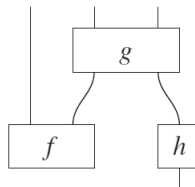
2.2.1. Как эволюционируют диаграммы в этой книге

В этой книге более-менее параллельно развиваются две истории:

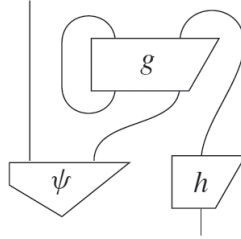
- разработка диаграммного языка и
- изложение квантовой теории как процессной теории.

Весь смысл квантового пикторализма в том и состоит, чтобы показать, как тесно переплетаются эти две темы. Мы начнем с очень общего диаграммного языка и постепенно будем добавлять средства, увеличивающие его выразительность. То есть исходный язык будет достаточно общим для описания самых разнообразных процессов, и потихоньку мы доберемся до квантовых процессов. По ходу дела мы будем представлять квантовые особенности, но не раньше, чем язык станет достаточно богатым для их обсуждения. В результате квантовая телепортация встретится гораздо раньше таких конкретных понятий, как кубиты. Всего на пути к полноценной квантовой теории будет пять крупных скачков в выразительной способности диаграмм.

1. В главе 3 мы представим очень простой диаграммный язык, в котором не будет ничего, кроме *блоков* и *проводов*. Это позволит нам естественно выразить композиции процессов в любой процессной теории:

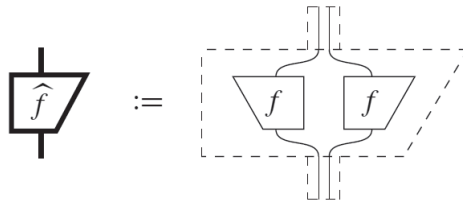


2. В главе 4 определены *струнные диаграммы* (string diagram), которые выделяют специальные классы процессных теорий, где провода могут быть чашеобразными и крышкообразными, а каждый блок можно отражать относительно горизонтальной или вертикальной оси:

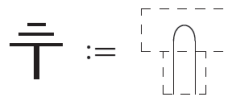


С их помощью уже можно продемонстрировать такие квантовоподобные особенности, как неразделимость, унитарность и невозможность клонировать произвольные состояния. Продолжая приведенное в начале раздела 1.2 обсуждение того, почему для открытия квантовой телепортации понадобилось 60 лет, отметим, что язык струнных диаграмм с очевидностью показывает, что нечто подобное квантовой телепортации возможно.

3. Далее мы вводим два вида блоков и проводов: тонкие и толстые. Это позволит нам различать квантовые и классические системы. Толстые блоки и провода, определенные в главе 6, получаются путем *удвоения* тонких:

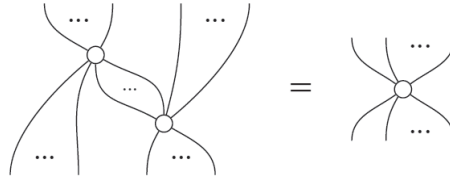


Удвоение гарантирует, что все порождаемые теорией числа положительны и, стало быть, их можно интерпретировать как вероятности. Заодно это позволяет определить *отбрасывание*:



– специальный процесс, который играет ключевую роль в нашем изложении квантовой теории и принципа причинности, необходимого для совместимости с теорией относительности.

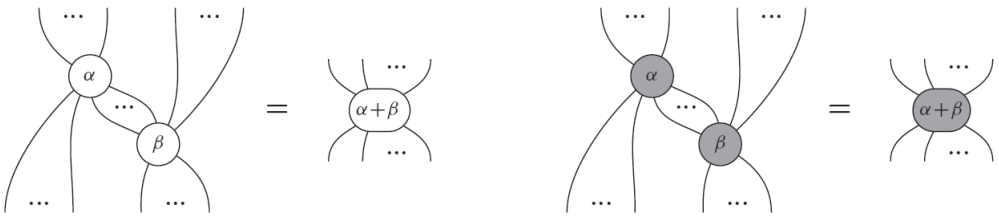
4. Определенные в главе 8 пауки – это причудливое обобщение проводов. Если у провода имеется только один вход и один выход, то паук представляет соединение с произвольным числом входов и выходов. Поведение пауков подчиняется правилу «слияния пауков», утверждающему, что при соединении двух пауков они сливаются в один.



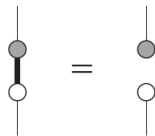
Среди прочего пауки используются для того, чтобы отразить уникальную особенность поведения классических данных: возможность копирования и удаления. Они также позволяют представить взаимодействие классических и квантовых систем прямо на диаграммах, посредством операций измерения и кодирования:



5. И последний скачок – в главе 9 мы допускаем диверсификацию пауков. Теперь у пауков могут быть *разные цвета и фазы*:



Эти дополнительные данные дают возможность определять все необходимые нам процессы с помощью одних лишь диаграмм (т. е. не привлекая, например, матрицы) и элегантно выражать такие чрезвычайно важные особенности, как дополнительность:



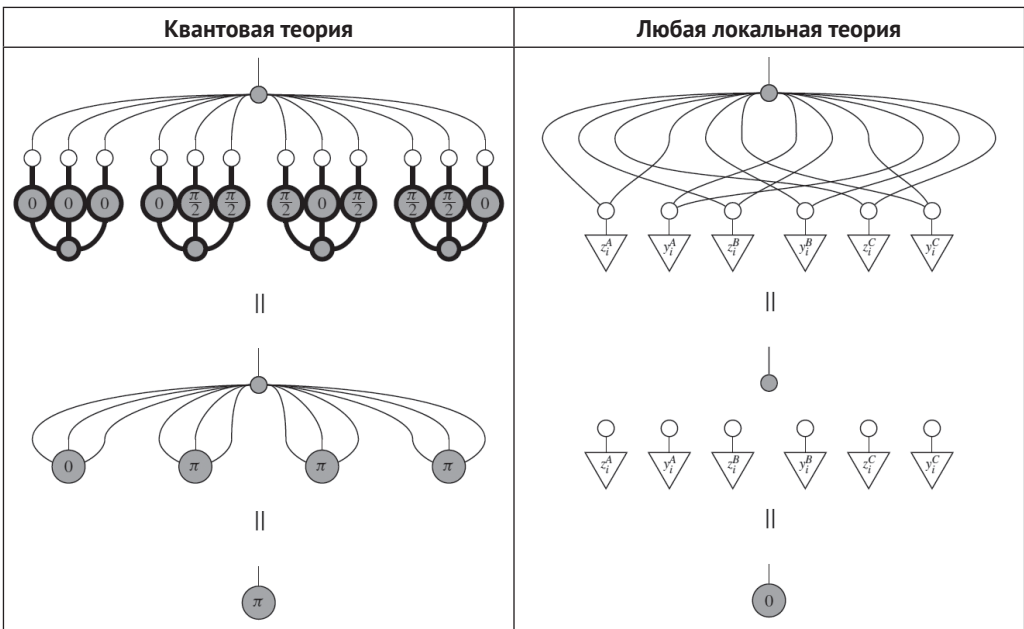
Теперь диаграммный язык становится достаточно богатым, чтобы недвусмысленно записать любой процесс из m кубитов в n кубитов, т. е. он становится *универсальным* для кубитов. Правила манипулирования такими диаграммами называются *ZX-исчислением*. На самом деле это исчисление не просто универсальное, но еще и полное для важных фрагментов квантовой теории кубитов. Это означает, что все равенства, которые можно вывести с помощью матриц, можно вывести и с помощью диаграмм.

Имея в своем распоряжении полный диаграммный язык, мы в главе 10 дадим лаконичную и элегантную картину квантовой теории. Приведем предварительный анонс того, как это выглядит, в форме, напоминающей...

2.2.2. Голливудский трейлер

Самой яркой и в то же время наименее понятной квантовой особенностью, вне всяких сомнений, является квантовая нелокальность. В конце книги мы подробно расскажем о существовании нелокальностей (и докажем это). А сейчас позволим читателю мельком взглянуть на тайны, которые будут раскрыты.

В стандартных учебниках рассказ о нелокальности занимает несколько страниц текста, испещренного формулами, а у нас он сведется к двум диаграммным вычислениям, одно в контексте квантовой теории, а другое в контексте локальных теорий. Эти вычисления дают противоречивые результаты.



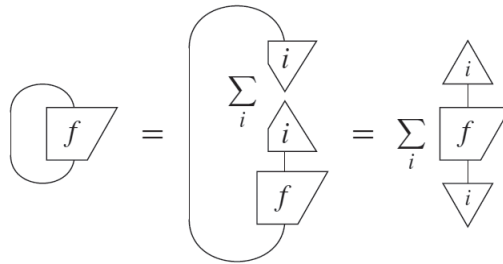
Мы узнаем, что левая диаграмма моделирует четыре измерения ГХЦ-состояния, за которыми следует вычисление *четности* результатов измерений. Иными словами, теория говорит нам, следует ли ожидать четного или нечетного количества щелчков (или пиканий, вспышек и т. д.) от измерительного устройства. Мы увидим, что сведение к π на левой диаграмме означает, что, согласно квантовой теории, количество будет нечетным. Сравните это с правым выводом, в котором предполагается, что существуют некоторые заранее установленные корреляции, определяющие результаты измерений. Так всегда обстоит дело с локальной теорией, поскольку все корреляции отдаленных событий можно проследить до некоторой общей причины. Сведение к 0 на правой диаграмме означает, что любая локальная теория предсказывает четное количество щелчков, и, стало быть, имеет место противоречие между квантовой теорией и локальностью.

Этот пример взят из главы 11 «Основания квантовой теории», в которой мы также представим модельную теорию, которая очень похожа на квантовую теорию кубитов, но не является нелокальной. Две главы посвящены более узким темам. В главе 12 «Квантовые вычисления» мы рассматриваем такие стандартные темы,

как схемная модель квантовых вычислений и квантовые алгоритмы, а также менее стандартные (но приобретающие все большую важность), в том числе основанные на измерениях квантовые вычисления. В главе 6 «Квантовые ресурсы» мы представим общую инфраструктуру для изучения ресурсов в квантовой теории, а в качестве особенно важного примера возьмем квантовую запутанность. Мы также покажем, что качественно различные типы квантовой запутанности можно рассматривать как пауков с сильно различающимся поведением.

2.2.3. Промежуточное синтаксическое загрязнение

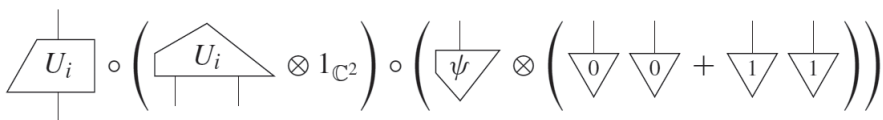
Мы еще не упомянули главу 5. Она ничего не вносит в разработку квантового пикторализма, но наводит мосты с обычным квантово-механическим формализмом. Основной обсуждаемый в ней вопрос ставится так. Пусть дана процессная теория со струнными диаграммами, при каких условиях провода представляют гильбертовы пространства, а блоки – линейные отображения? Отвечая на этот вопрос, мы присоединим к струнным диаграммам некоторые символы, так что получится гибридный диаграммно-символьный формализм, в котором возможны такие вычисления:



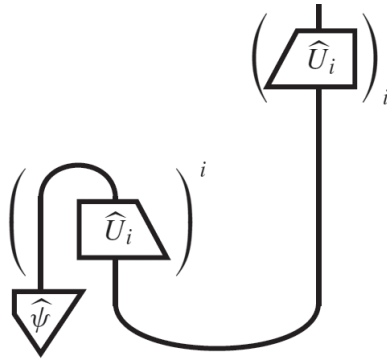
Такой гибридный формализм полезен сам по себе и широко используется в других областях математики, например в теории узлов. Но важнее, что он является введением в обычный формализм для тех, кто еще с ним незнаком, а для тех, кто знаком, проясняет, как с ним связаны диаграммы. Наконец, и это, наверное, самое главное, он позволяет точно сформулировать, какие вычисления возможны с помощью струнных диаграмм.

В частности, он позволяет сделать нечто, чего не найдешь в стандартных учебниках, – осуществить плавный переход от линейных отображений к квантовым процессам и в конечном итоге к процессам, моделирующим квантовую недетерминированность и взаимодействие классической и квантовой теорий исключительно графическими средствами.

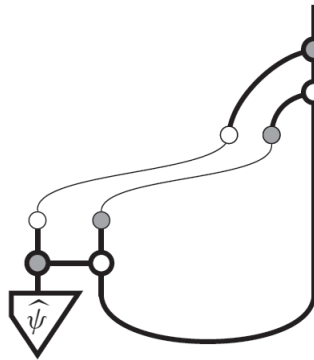
Попутно мы, подобно Данте, перейдем из линейно-алгебраического ада:



через чистилище



прямоком в чисто диаграммный рай:



2.2.4. Итоги, исторические замечания, ссылки, эпиграфы

Каждая глава (за исключением главы 10, которая сама является подведением итогов) содержит короткий раздел «Итоги: что следует запомнить», в котором перечисляются наиболее существенные уроки.

Кроме того, в конце каждой главы имеется раздел «Исторические замечания и ссылки», где дается историческая справка, относящаяся к рассмотренному материалу, приводятся важнейшие библиографические ссылки и предлагается литература для дальнейшего чтения.

Эпиграфы в начале каждой главы всегда связаны с ее содержанием. В некоторых случаях это очевидно из текста, а установление релевантности прочих мы оставляем в качестве упражнения для читателя.

2.2.5. Заголовки со звездочкой и материал повышенной сложности

Разделы, теоремы, замечания, примеры и упражнения, помеченные звездочкой (*), например «Замечание* х.у.з», факультативны. Обычно для их понимания необходимы знания, имеющиеся не у всех читателей, да и не всем интересные, а потому они адресованы только определенной части читателей. Например, за-

мечание со звездочкой может предполагать наличие дополнительных знаний из области линейной алгебры, квантовой теории или программирования. Заметим кстати, что в каждой главе имеется раздел «Дополнительный материал», который может представлять интерес для особо продвинутых студентов и специалистов. В частности, в таких разделах описывается связь между диаграммами и моноидальными категориями. Некоторое внимание уделяется также современным исследованиям квантового пикторализма, его связям с недавними успехами в области чистой математики и удивительным параллелям с семантикой естественного языка.

2.3. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

С годами мы обратили внимание, что нам часто задают одни и те же вопросы. Мы также предвидим два новых вопроса, относящихся конкретно к данной книге. Попробуем ответить на те и другие.

В1. *Зачем нужно X страниц для изложения тривиальной темы Y ?*

О. По нескольким причинам:

- как следует из названия книги, это первый курс не только по квантовой теории, но и по диаграммным рассуждениям. Поэтому мы вводим в рассмотрение новые понятия только тогда, когда располагаем достаточно богатым языком для их обсуждения. Не всегда это происходит в том порядке, которого вы ожидаете;
- мы не предполагаем никаких предварительных знаний и выводим все, что можно, из первых принципов, рассчитывая на очень широкий круг потенциальных читателей. Это означает, что многие вещи, хорошо знакомые многим читателям, например линейную алгебру, мы излагаем с нуля. Однако мы строим изложение этих базовых понятий диаграммным способом, настолько отличающимся от привычного, что, как нам кажется, любой читатель найдет для себя кое-что интересное в каждой главе.
- Увы, диаграммы потребляют много места. Извините, деревьев.

В2. *А где главное (т. е. числа)?*

О. Традиционно сложилось убеждение, что предсказательная способность физической теории неотделима от ее способности порождать числа, например вероятности. Многим с трудом удастся примирить эту идею с диаграммой, которая выглядит как дискретный логический объект. Однако в главе 3.4.1 мы увидим, что числа естественно возникают как частный случай диаграмм. Но все равно наиболее интересные особенности, рассматриваемые в этой книге, качественные, а не количественные. Как было анонсировано в голливудском трейлере, диаграммы будут все время использоваться для демонстрации того, что в квантовой теории возможны типы поведения, немыслимые в классической физике.

В3. *А как насчет бесконечномерных гильбертовых пространств?*

О. Урок, который можно вынести из квантовых вычислений и обработки квантовой информации, состоит в том, что для доступа ко многим новым революционным особенностям квантовой теории достаточно ограничиться конечным чис-

лом измерений (зачастую всего двумя!). На самом деле долго державшуюся веру в то, что «настоящая физика» имеет место только в бесконечномерной области, со всеми приводящими осложнениями, можно приписать незнанию новых квантовых особенностей, которые были открыты в последние 20 лет. Конечно, мы не утверждаем, что о бесконечномерных пространствах следует забыть, но квантовому пикторализму они несут трудности особого рода. И самая заметная из них – что основные элементы диаграмм (чашки, крышки и пауки) просто непредставимы в виде ограниченных операторов между бесконечномерными гильбертовыми пространствами. Поэтому в течение многих лет мы считали, что нужно выбирать между мощностью (и сложностью) бесконечномерных пространств и элегантностью диаграммных рассуждений с использованием крышек, чашек и пауков. Однако некоторые встречающиеся в этой книге построения, которые вроде бы опираются на крышки и чашки, можно выполнить, полностью избежав их (Coecke and Neunen, 2011), а недавние результаты Gogioso and Genovese (2016) наводят на мысль, что наши крышки позволяют совместить приятное с полезным! Точнее, применив технику нестандартного анализа, они показали, что хотя чашки, крышки и пауки не существуют в бесконечномерном пространстве, рассуждать о них все-таки можно, при условии что они не фигурируют в конечном ответе.

Пока этот новый способ работы с бесконечномерными системами находится в младенчестве, но обещает пришествие настоящего бесконечномерного квантового пикторализма.

В4. *А как насчет уравнения Шрёдингера?*

О. Вы, наверное, обратили внимание, что мы тщательно избегаем термина «квантовая механика», употребляя вместо него «квантовая теория», под которой понимаем ядро квантовой механики, где игнорируются такие вещи, как положения, импульсы и непрерывная эволюция во времени. Для наших целей достаточно рассматривать только общее изменение систем между моментами t_1 и t_2 , не детализируя, что происходит в промежутке. Как и в случае бесконечномерных пространств, гигантский прогресс в области квантовой информации и квантовых вычислений показал, что, даже работая на этом уровне, мы имеем доступ ко многим чарующим явлениям. Вместе с тем обратим внимание на недавние волнующие исследования по включению динамики в квантовый пикторализм (Gogioso, 2015b, c) и отметим, что многие обсуждаемые в этой книге особенности (например, сильная дополнительность), вероятно, будут играть в этом главную роль.

В5. *Удалось ли с помощью квантового пикторализма открыть что-то новое?*

О. Люди, задающие этот вопрос, обычно имеют в виду следующее: «Помог ли квантовый пикторализм решить задачи, которые уже были поставлены, но не решались другими методами?» Ответ утвердительный, и некоторые примеры описаны в работах Duncan and Perdrix (2010), Coecke et al. (2011b), Horsman (2011) и Voixo and Neunen (2012). Однако в науке постановка новых интересных вопросов иногда важнее ответа на старые. Такие вопросы, как полнота исчисления, насколько нам известно, раньше в физике не задавались, а квантовый пикторализм дал целую серию результатов в этой области (Backens, 2014a,b; Schröder de Witt and Zamdzhiev, 2014; Hadzihasanovic, 2015). Трудно представить, как эти ответы

можно было бы получить, придерживаясь традиционного формализма гильбертова пространства. Еще один новый вопрос: можно ли автоматизировать рассуждения о физике, и для ответа на него уже разработана программа *Quantomatic*, рассматриваемая в главе 14 (Kissinger and Zamdzhiev, 2015). Наконец, идеи и методы квантового пикторализма находят применения и в других областях, например в композиционной дистрибутивной модели семантики естественного языка (Clark et al., 2014; Coecke, 2016), которая превзошла существовавшие раньше методы в применении к эмпирическим данным (Grefenstette and Sadrzadeh, 2011; Kartsaklis and Sadrzadeh, 2013).

Глава 3

Процессы как диаграммы

Мы не придавали особого значения мысли как процессу. Конечно, мысли у нас были, но мы обращали внимание лишь на содержание, а не на процесс.

– Дэвид Бом и Дэвид Пум, 1987

В этой главе мы представим практическое введение в основы диаграммных рассуждений, а именно покажем, как с помощью диаграмм производить вычисления и решать задачи. Мы также продемонстрируем, почему диаграммы во многих отношениях гораздо лучше традиционной математической нотации. Разработка и изучение диаграммных языков – весьма активная область исследований, а для того чтобы диаграммные рассуждения стали интуитивно очевидными, потребовалось много лет. По счастью, трудная работа, необходимая для формализации диаграмм, используемых в этой книге, уже проделана! Теперь можно пожинать плоды в виде изящного графического языка.

Попутно мы познакомимся с *нотацией Дирака*. Читатели, которые раньше изучали квантовую механику или квантовую теорию информации, наверное, уже встречались с нотацией Дирака в контексте линейных отображений. Здесь мы объясним, как она предстает в виде одномерного фрагмента двумерного графического языка. Таким образом, читатели, незнакомые с нотацией Дирака, будут воспринимать ее как частный случай графической нотации, используемой на протяжении всей книги.

Мы также введем понятие *процессной теории*, которая дает возможность интерпретировать диаграммы посредством фиксирования конкретной коллекции систем (физических, вычислительных, математических, съедобных и т. д.) и процессов, которым эти системы могут подвергаться (нагрев, сортировка, умножение на два, приготовление в пищу и т. д.).

Как было отмечено в главе 1, выбор процессных теорий в качестве отправной точки знаменует существенный отход от стандартной практики, принятой во многих дисциплинах. Вместо того чтобы принуждать себя полностью разобратся в одной системе, прежде чем даже помыслить о композиции и взаимодействии систем, мы стремимся понять системы преимущественно в терминах их взаимодействия с другими системами. Вместо того чтобы пытаться понять додо Дэйва, подвергнув его вивисекции (после чего он будет выглядеть так же, как любая другая жирная птица), мы отпустим его на свободу и будем наблюдать, что он станет делать.

Это очень близко по духу к целям теории категорий, с которой нам предстоит познакомиться в дополнительном материале в конце этой главы.

3.1. ОТ ПРОЦЕССОВ К ДИАГРАММАМ

Посмотрим, как диаграммный язык дает общий способ говорить о процессах и их композициях, и покажем, что диаграммы предлагают строгую математическую нотацию, ничем не уступающую традиционным математическим формулам.

3.1.1. Процессы – блоки, системы – провода

Мы будем употреблять термин *процесс* для обозначения любой сущности, имеющей ноль или более входов и ноль или более выходов. Например, функция

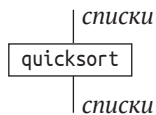
$$f(x, y) = x^2 + y \quad (3.1)$$

– это процесс, который на входе принимает два вещественных числа, а на выходе порождает одно вещественное число. Такой процесс представляется *блоком*, в который снизу входят *провода*, представляющие входные системы, а сверху выходят провода, представляющие выходные системы. Так, функцию (3.1) можно было бы записать в виде:



Метки на проводах называются *системными типами*, или просто *типами*.

Точно так же компьютерная программа – это процесс, которые принимает некоторые данные (например, из памяти) на входе и порождает новые данные на выходе. Например, программа сортировки списков могла бы выглядеть так:



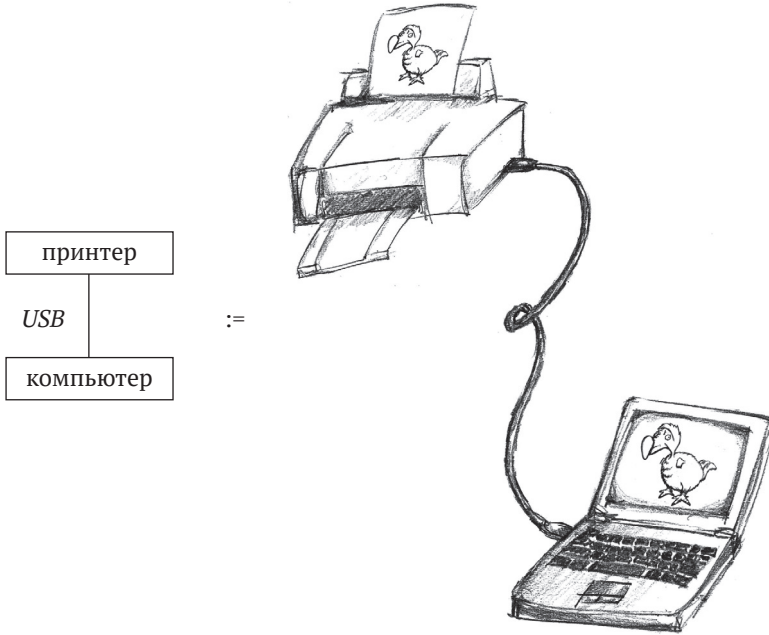
Ниже показано еще несколько допустимых процессов:



Смотрите, мир вокруг нас просто кишит процессами!

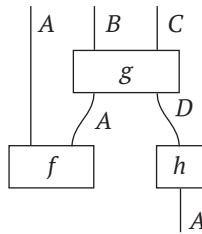
Заметим, что иногда блок помечен процессом, протекающим во времени (например, «процесс приготовления завтрака»), а иногда – аппаратом (например, «бинокль» или «младенец»). Обычно это означает «процесс использования данного аппарата для преобразования входных систем в выходные».

Бывает даже так, что провода на диаграмме соответствуют физическим проводам, например:

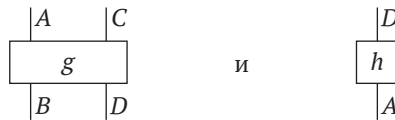


Хотя это, конечно, необязательно. Провода могут также представлять «совмещение отверстий» в лабораторном оборудовании или доставку чего-либо судном. Важно, что провода представляют поток данных (или вообще чего-то) от одного процесса к другому.

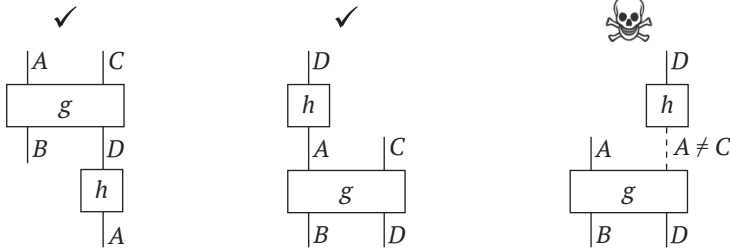
Как мы только что видели, простые процессы можно *соединить проводами* для получения более сложных, что отражается на *диаграмме*:



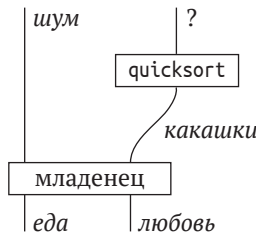
На такой диаграмме выходы могут быть соединены с входами, только если их типы совпадают. Например, следующие два процесса:



можно соединить одними способами и нельзя другими в зависимости от типов проводов:

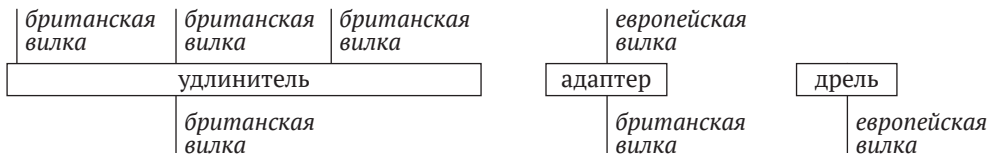


Ограничение на допустимые соединения – важная часть языка диаграмм, поскольку несет информацию о том, когда имеет смысл применять процесс к некоторой системе, и предотвращает такие ситуации:

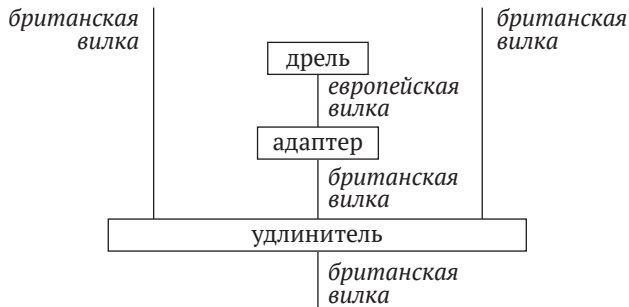


которые, скорее всего, были бы противопоказаны вашему компьютеру! Как *типы данных* в информатике, типы, указанные на проводах, говорят, какого вида данные (или что-то еще) процесс ожидает на входе и что он порождает на выходе. Например, программа-калькулятор ожидает получить на входе числа и возвращает тоже числа. Поэтому она не поняла бы, что означает «Дэйв» на входе, и не могла бы породить, скажем, морковку на выходе.

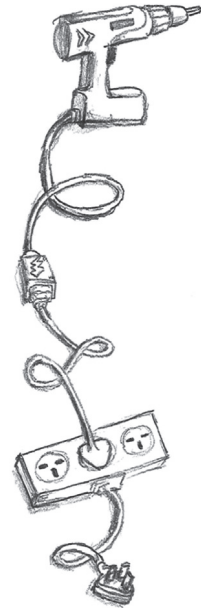
Еще один полезный пример – электрические устройства. Допустим, что рассматриваемые процессы – это устройства, которым на вход подаются вилки (т. е. «входом» является электричество), а на выходе порождаются розетки:



В этом случае системные типы – это просто форма вилки (британская, европейская и т. д.). Понятно, что мы не можем воткнуть вилку в несовместимую с ней розетку, поэтому информация о типе на проводах сообщает нам как раз то, что необходимо знать о допустимых соединениях. Вот, например, одно из возможных соединений:



:=



Хотя это несерьезный пример, часто он бывает полезен, когда нужно нарисовать диаграммы, где блоки соответствуют физическим устройствам (например, в лаборатории). Такие диаграммы мы будем называть *операционными*.

3.1.2. Процессные теории

Обычно нас интересуют не все возможные процессы, а некоторый класс процессов, имеющих что-то общее. Например, ученые в конкретной области, как правило, изучают определенный класс процессов: физические, химические, биологические, вычислительные, математические и т. д. Поэтому процессы организуются в *процессные теории*. На интуитивном уровне процессная теория говорит, как интерпретировать блоки и провода в диаграмме (см. (i) и (ii) ниже) и в чем смысл образования диаграммы, т. е. соединения блоков (см. (iii) ниже).

Определение 3.1. *Процессная теория* состоит из:

- (i) набора T *системных типов*, представленных проводами;
- (ii) набора P *процессов*, представленных блоками, такого, что входные и выходные типы каждого процесса берутся из T ;
- (iii) средства «соединения процессов проводами», т. е. операции, которая интерпретирует диаграмму процессов из P как процесс из P .

В частности, (iii) гарантирует, что

процессные теории «замкнуты относительно соединения процессов проводами»,

поскольку именно эта операция говорит нам, что означает «соединение процессов проводами». Иногда эта операция буквально означает соединение предметов физическими проводами, как в примере с дрелью. А иногда приходится подумать, причем бывает так, что очевидных вариантов выбора несколько. В разделе 3.2 мы увидим, что традиционный математический подход заключается в разделении

операции «соединения процессов проводами» на две подоперации: параллельная и последовательная композиции процессов.

Пример 3.2. Приведем несколько примеров процессных теорий, с которыми мы столкнемся далее:

- **функции** (типы = множества);
- **отношения** (типы = множества);
- **линейные отображения** (типы = векторные или гильбертовы пространства);
- **классические процессы** (типы = классические системы);
- **квантовые процессы** (типы = квантовые и классические системы).

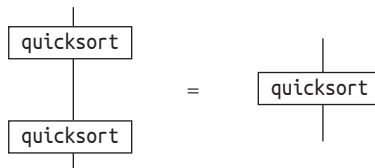
Первые два вида теорий мы будем использовать преимущественно в различных примерах и упражнениях, а остальные будут играть главенствующую роль в этой книге.

Замечание 3.3. Обратите внимание, что, говоря о конкретной процессной теории, мы сообщаем, что такое в ней «процессы», но типы явно не упоминаем. Это разумная практика, потому что именно процессы – наиболее важная часть. Например, мы увидим, что процессные теории функций и отношений совершенно различны, поэтому неправильно называть обе «множествами».

Поскольку процессная теория говорит о том, как интерпретировать диаграммы как процессы, она несет информацию и о том, когда две диаграммы представляют один и тот же процесс. Предположим, к примеру, что мы определяем простую процессную теорию **компьютерных программ**, в которой типы – это типы данных (например, целые, булевы, списки), а процессы – компьютерные программы. Ее можно было бы определить следующим образом (не переживайте, если не сможете прочесть код, половина авторов тоже не может этого сделать):

$$\boxed{\text{quicksort}} := \begin{cases} \text{qs } [] = [] \\ \text{qs } (x :: xs) = \\ \quad \text{qs } [y \mid y <- xs; y < x] ++ [x] ++ \\ \quad \text{qs } [y \mid y <- xs; y \geq x] \end{cases}$$

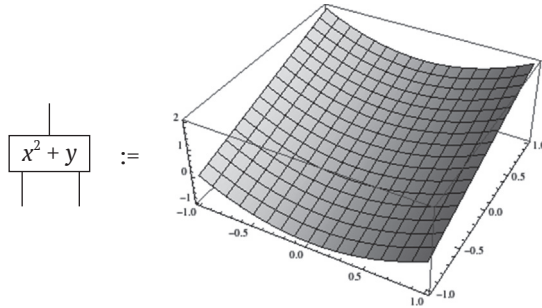
Соединение программ проводами означает передачу выхода одной программы на вход другой. Если считать, что две программы одинаковы, если они ведут себя одинаково (опуская такие детали, как время работы и прочее), то наша процессная теория порождает равенства вида:



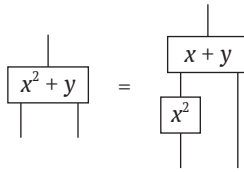
т. е. если отсортировать список дважды, то результат будет таким же, как после однократной сортировки.

Мы называем процессную теорию *теорией*, потому что она сопровождается уймой подобных равенств, и именно эти равенства позволяют нам делать выводы об изучаемых процессах.

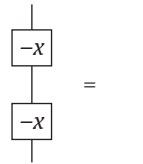
В качестве другого примера возьмем функцию, определенную в начале раздела 3.1.1. Она принадлежит процессной теории **функций**. Типами являются множества, а процессами – функции, отображающие одно множество в другое. Две функции считаются равными, если они одинаково ведут себя, т. е. имеют одинаковые графики:



(Заметим, что два входных провода означают, что это функция двух переменных, так что график у нее трехмерный). Поскольку графики функций одинаковы, имеем:



и по той же причине



Упражнение 3.4. Придумайте сами какие-нибудь процессные теории. Для каждой теории ответьте на следующие вопросы:

1. Каковы в ней системные типы?
2. Что в ней является процессами?
3. Как составляются композиции процессов?
4. Когда два процесса следует считать одинаковыми?

Кстати, мы еще толком не сказали, что же такое диаграмма. Полное описание диаграммы состоит из:

- 1) перечня блоков;
- 2) описания того, как эти блоки соединены.

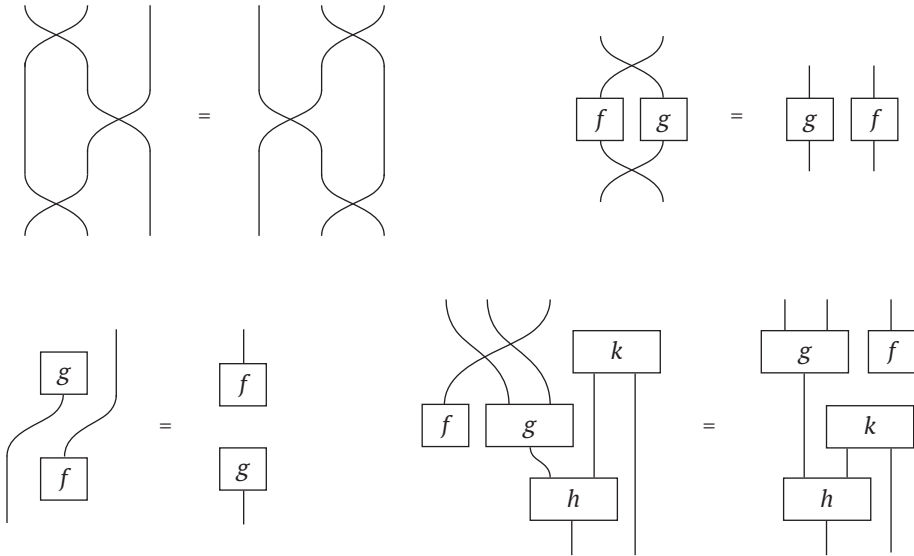
Поэтому слово «диаграмма» относится к рисованию блоков и проводов без какой-либо интерпретации в рамках процессной теории. Но нигде не говорится, как именно следует изображать блоки на странице. Отсюда сразу же вытекает

Следствие 3.5. Если две диаграммы можно преобразовать друг в друга деформацией (разумеется, не изменяя соединения), то они равны.

Или более кратко:

Важны только соединения!

Пример 3.6. Ниже приведено несколько пар равных диаграмм:



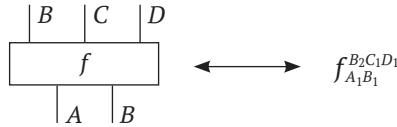
Замечание* 3.7. Первая пара равных диаграмм в примере 3.6 называется уравнением Янга–Бакстера. Некоторые читатели, возможно, встречали его в литературе по математической физике.

3.1.3. Диаграммы – это математика

Диаграммы предлагают строгий язык для выполнения математических операций, не уступающий традиционным математическим формулам. Как традиционные формулы можно использовать для определения новых концепций и рассуждений о многих математических структурах (множествах, группах, топологических пространствах, векторных пространствах), так и диаграммы можно использовать для определения новых концепций и рассуждений о процессных теориях.

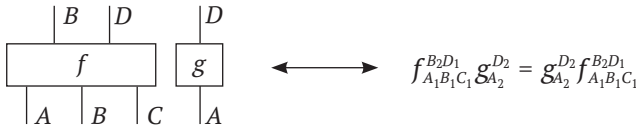
Быть может, в результате воспитания некоторые люди не согласны считать строгим математическим объектом ничего, что не может быть выражено некоторой формулой. Чтобы удовлетворить таких людей (а заодно предложить другой взгляд на диаграммы), мы кратко опишем нотацию, напоминающую формулы. Но после того как выработается надлежащая интуиция, мы будем опускать эту нотацию и (почти) всегда работать непосредственно с диаграммами.

Преобразовать блок в формулу можно следующим образом:

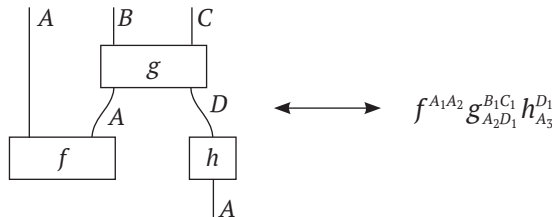


В правой части этой формулы нижние индексы A_1 и B_1 при f представляют входы, а верхние индексы B_2 , C_1 и D_1 – выходы. Зачем мы добавили в каждой букве еще и цифру? Нумерация сама по себе не несет никакого смысла, но необходима, чтобы устранить неоднозначность, когда на диаграмме присутствует несколько проводов одного и того же типа. Например, второй вход f – провод, отличный от проводов одного и того же типа. Например, второй вход f – провод, отличный от проводов одного и того же типа, поэтому мы обозначаем их B_1 и B_2 соответственно. Тип вместе с индексом называется *именем провода*, поскольку обозначает ровно один провод на диаграмме. В диаграммах индексы, конечно, необязательны, потому что и так ясно, что B_1 и B_2 – разные провода, ведь они занимают разное место на странице.

Выражение $f_{A_1 B_1 C_1}^{B_2 D_1}$ называется *именем блока*, потому что относится к конкретному блоку на диаграмме. Мы можем выразить несколько блоков, записав последовательность их имен, причем порядок следования имен неважен:



Отметим, что все верхние и нижние имена проводов в формуле справа различны, поскольку ни один провод не соединен ни с каким другим. Чтобы представить соединения, мы должны были бы повторить имя провода – один раз в виде верхнего индекса (соответствующего выходу блока) и другой раз в виде нижнего индекса (соответствующего входу):



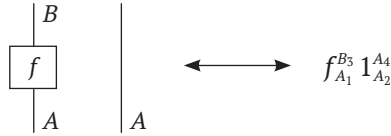
Мы можем указать в повторяющемся имени провода любой индекс, лишь бы он не конфликтовал с именами других проводов. Например, следующие две формулы представляют одну и ту же диаграмму:

$$f^{A_1 A_2} g_{A_2}^{B_1} = f^{A_1 A_4} g_{A_4}^{B_1}. \tag{3.3}$$

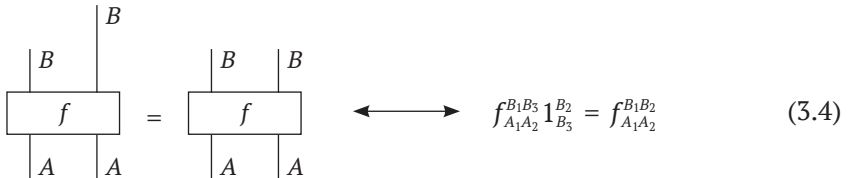
Мы также будем рассматривать одиночный провод типа A как «специальный» блок



с именем $1_{A_1}^{A_2}$. Таким образом, можно, например, написать:



Почти во всех отношениях эти специальные блоки ведут себя как обычные блоки и могут интерпретироваться как процесс, который «ничего не делает». Но когда мы соединяем такой блок с входом или выходом другого блока, он исчезает:



Всему вышесказанному подведен итог в следующем определении.

Определение 3.8. *Диаграммная формула* – это последовательность имен блоков, в которой все имена проводов уникальны, за исключением соответствующих друг другу пар имен в верхнем и нижнем индексах. Две диаграммные формулы равны, если их можно преобразовать друг в друга с помощью следующих операций:

- (а) изменение порядка следования имен блоков;
- (б) добавление и удаление тождественных блоков, как в (3.4);
- (с) изменение повторяющегося имени провода.

Вооружившись этой концепцией, мы теперь можем дать определение диаграммы, в котором напрямую упоминается ее формульный аналог.

Определение 3.9. *Диаграммой* называется графическое представление диаграммной формулы, в котором имена блоков изображены в виде блоков прямоугольной или иной формы, имена проводов – в виде линий, входящих в эти блоки и исходящих из них, а повторяющиеся имена проводов говорят о том, какие выходы соединены с какими входами.

Упражнение 3.10. Нарисуйте диаграммы, соответствующие следующим диаграммным формулам:

$$f_{B_1 C_2}^{C_4} g_{C_4}^{D_3} \quad f_{A_1}^{A_1} \quad g_{B_1}^{A_1} f_{A_1}^{B_1} \quad 1_{A_1}^{A_6} 1_{A_2}^{A_5} 1_{A_3}^{A_4}$$

Воспользуйтесь соглашением о том, что входы и выходы нумеруются слева направо.

Описанная выше конструкция показывает, что вся наша работа с диаграммами может быть однозначно транслирована на язык диаграммных формул. Мы будем в основном иметь дело с диаграммами, потому что их легче визуализировать, с ними проще работать, и мы избавлены от тяжелой необходимости возиться с дополнительными индексами. Однако иногда мы все же будем прибегать к диаграммным формулам как к удобному средству вычисления процесса, представленного данной диаграммой (см. разделы 3.3.3 и 5.2.4).

3.1.4. Процессные равенства

В примере 3.6 выше мы выписали несколько равенств, содержащих диаграммы в левой (ЛЧ) и правой (ПЧ) частях. Эти *диаграммные равенства* справедливы всегда, вне зависимости от интерпретации блоков и проводов. То есть они верны в любой процессной теории. С другой стороны, в конкретной процессной теории один и тот же *процесс* иногда можно представить двумя разными диаграммами. Два таких примера мы уже встречали в разделе 3.1.2.

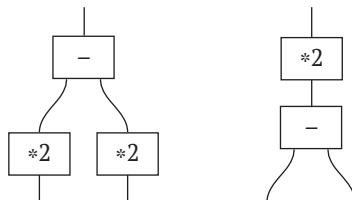
Возвращаясь к процессной теории **функций**, предположим, что мы определили два процесса: «минус» принимает два входа m и n и вычитает один из другого, порождая $m - n$:



а «умножить на 2» принимает один вход и умножает его на 2:



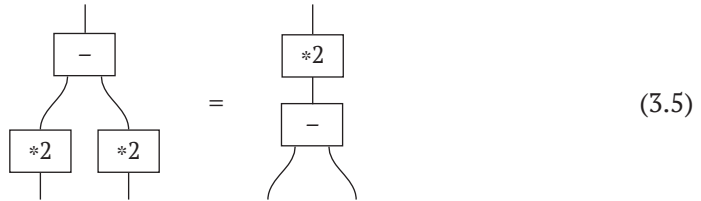
Здесь все провода имеют тип \mathbb{R} . Теперь рассмотрим следующие две диаграммы:



Как *диаграммы* они не равны. Но если взглянуть на представляемые ими *процессы*, то мы видим, что процесс слева умножает оба входа на 2, а затем вычитает один из другого. Процесс справа сначала вычитает входы, а затем умножает результат на 2. Несмотря на различие диаграмм, оба процесса вычисляют одну и ту же функцию, а именно:

$$2m - 2n = 2(m - n).$$

Следовательно, эти различные диаграммы представляют один и тот же процесс, если интерпретировать их в процессной теории **функций**, т. е. они *равны как процессы*, что можно записать в виде:



Это называется *процессным равенством*. Диаграммное равенство является тривиальным частным случаем процессного равенства, потому что равные диаграммы всегда интерпретируются как равные процессы.

Замечание* 3.11. Существует специальный класс теорий, в котором диаграммные и процессные равенства совпадают. То есть два процесса равны тогда и только тогда, когда их диаграммы совпадают. Они называются *свободными процессными теориями* по аналогии с употреблением слова «свободный» в алгебре. Здесь «свободный» означает «без дополнительных равенств». В общем случае введение дополнительных равенств между процессами налагает ограничение на допустимые интерпретации блоков (т. е. разрешены только блоки, удовлетворяющие дополнительным равенствам). Свободные процессные теории обладают тем свойством, что любая интерпретация их блоков как процессов (в какой-то другой процессной теории) расширяется до согласованной интерпретации диаграмм.

Упражнение 3.12. Напишите (диаграммные) равенства, выражающие алгебраические свойства ассоциативности, унитарности и коммутативности процесса с двумя входами и одним выходом. Можно ли сделать то же самое для дистрибутивности пары процессов с двумя входами (например, «плюс» и «умножить»)? Если нет, то в чем проблема?

Понятие диаграммного равенства может показаться совершенно очевидным (потому что так и есть!), но важно отметить, что такие равенства дают чуть больше информации, чем видится на первый взгляд. Чтобы понять, почему это так, заметим, что равенство (3.5) истинно, но следующее равенство **ложно**:

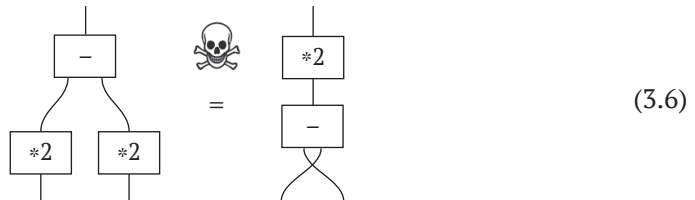
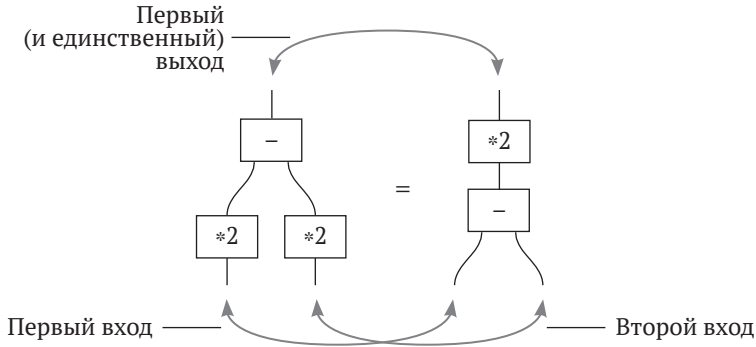


Диаграмма в левой части отображает входы m, n в выход $2m - 2n$, а диаграмма в правой части отображает те же входы в $2(n - m) \neq 2m - 2n$. Единственное различие между этим и истинным равенством (3.5) состоит в том, что входы на правой диаграмме переставлены местами. И хотя мы не пишем на диаграммах имена

проводов (в отличие от диаграммных формул в определении 3.8), входы и выходы, очевидно, можно различить. Кроме того, чтобы диаграммное равенство считалось правильным, в обеих частях должны быть *одни и те же* входы и выходы, т. е. между ними должно быть установлено соответствие:



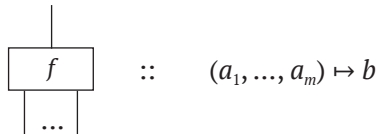
В терминах диаграммных формул это означало бы, что мы называем, к примеру, первый вход A_1 , а второй вход $- A_2$ в обеих частях равенства. На диаграмме соответствие входов и выходов показывается с помощью их положений на странице. Памятуя об этом, мы усматриваем очевидное различие между правильным равенством (3.5) и неправильным (3.6).

Равенства между процессами с одним «выходом» хорошо знакомы из алгебры. Записывая равенство вида

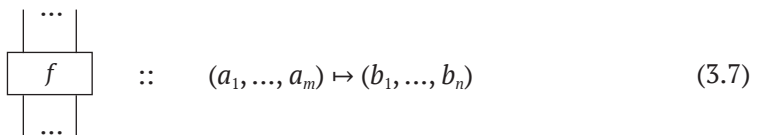
$$2m - 2n = 2(m - n),$$

мы различаем входы m, n формул в левой и правой частях, назначая им имена: m и n . У алгебраической формулы всегда только один «выход» – значение, вычисленное после того, как вместо всех переменных подставлены числа. Поэтому именовать этот выход нет необходимости. С другой стороны, у диаграмм в общем случае может быть *много* выходов, поэтому их надо различать, как и входы.

Мы привыкли думать, что функции многих переменных типа показанной выше алгебраической операции отображают один или несколько входов в один выход:



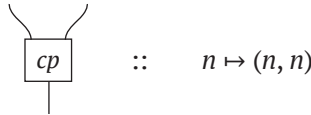
где символ \mapsto означает «отображает в» (см. приложение). Но в процессной теории **функций** можно рассматривать также функции вида:



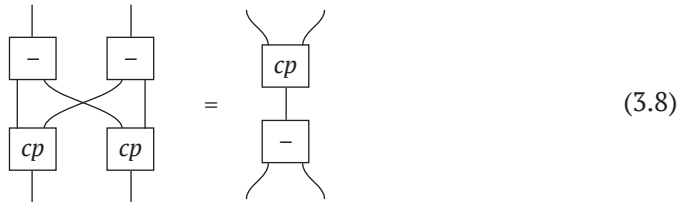
Замечание* 3.13. В функциональном программировании можно встретить функцию с несколькими выходами в смысле (3.7) в выражениях вида:

$$\text{let } (b_1, \dots, b_n) = f(a_1, \dots, a_m) \text{ in } \dots$$

Простой пример функции с двумя выходами дает *cp*, которая принимает число *n* и передает копию *n* по обоим выходным проводам:



Функция *cp* удовлетворяет следующему процессному равенству, включающему процесс «минус»:



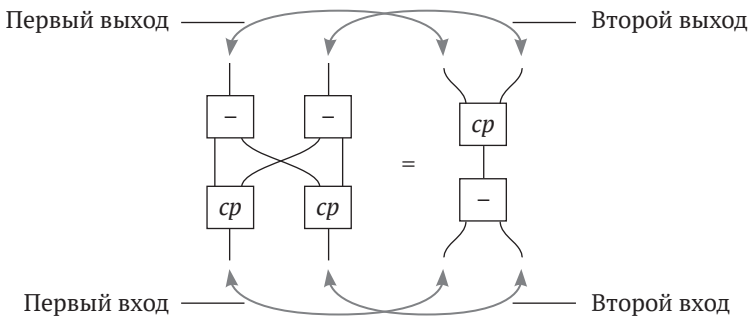
Процесс в левой части принимает два входа *t* и *n*, копирует оба и отправляет по одной копии каждой из двух операций вычитания. На выходе получается две копии разности *t - n*, по одной на каждом проводе:

$$(m, n) \mapsto (m, m, n, n) \mapsto (m, n, m, n) \mapsto (m - n, m - n).$$

Процесс в правой части принимает два входа *t* и *n*, вычитает один из другого и копирует результат. И снова мы получаем две копии *t - n*:

$$(m, n) \mapsto m - n \mapsto (m - n, m - n).$$

Как и раньше, соответствие между входами и выходами в (3.8) устанавливается неявно:



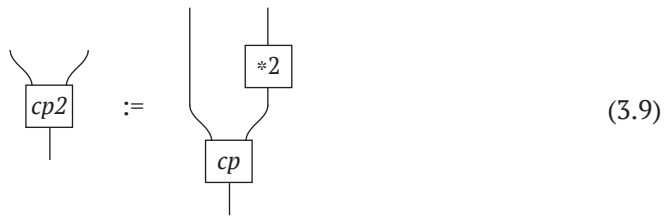
Упражнение 3.14. Запишите (3.8) в виде равенства между диаграммными формулами.

Упражнение* 3.15. Можно ли теперь, используя cp , выразить равенство дистрибутивности между процессами «плюс» и «умножить» из упражнения 3.12?

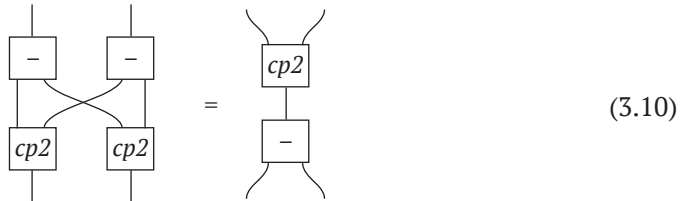
3.1.5. Подстановка диаграмм

Новые процессные равенства можно получить из существующих с помощью *подстановки диаграмм*. Подстановка, наряду с простой деформацией диаграмм, является одним из вычислений, к которым мы чаще всего будем прибегать в этой книге.

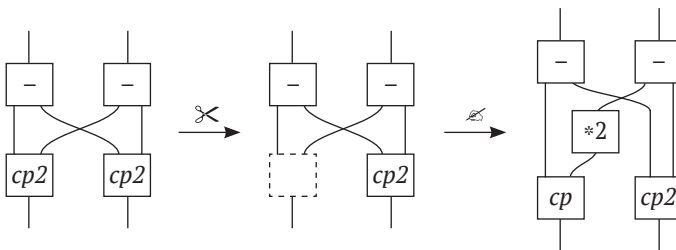
Под подстановкой диаграмм понимается замена некоторой поддиаграммы данной диаграммы другой поддиаграммой, связанной с первой процессным равенством. Результирующая диаграмма представляет эквивалентный процесс. Как это работает, проще всего показать на примере. Нам уже поднадоела функция копирования, порождающая две идентичные копии числа, поэтому определим более интересную функцию, которая еще и умножает правую копию на два:



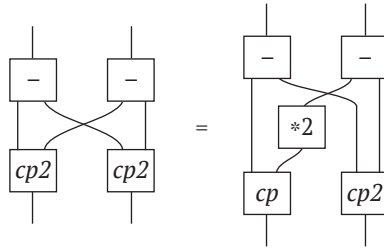
Теперь можно спросить, каким равенствам удовлетворяет $cp2$. Мы подозреваем, что она удовлетворяет равенству, аналогичному (3.8):



Начав с левой части (3.10), применим равенство (3.9), чтобы раскрыть определение $cp2$. Это означает, что мы вырезаем левую часть (3.9) и заменяем ее правой частью (3.9):

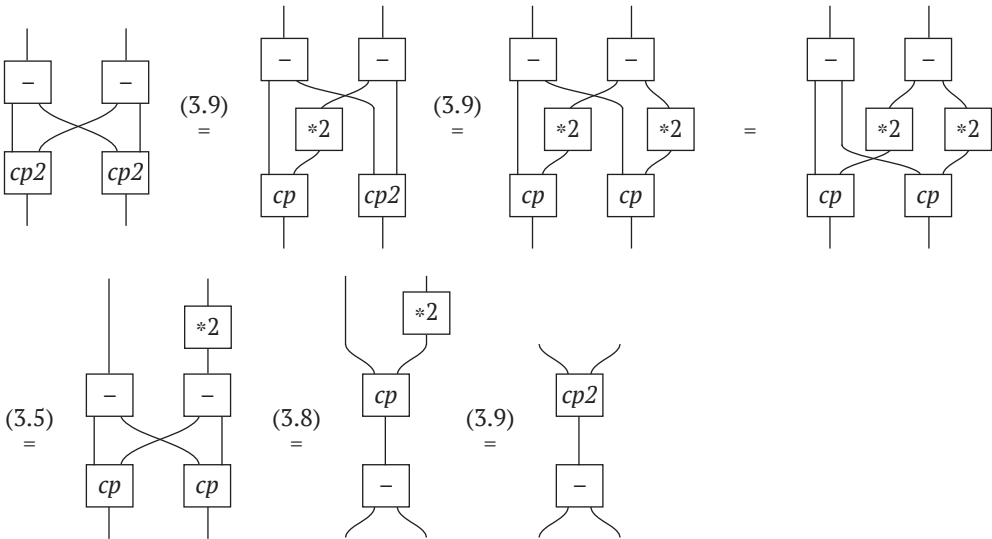


Таким образом, из (3.9) с помощью подстановки диаграммы мы можем вывести следующее равенство:



Замечание 3.16. Важный аспект подстановки диаграмм заключается в том, что правую часть следует вставить в *то же место*, где была левая. Например, первый вход правой части должен быть соединен с тем же проводом, который был первым входом замененной левой части, и т. д. Именно здесь обсуждавшееся в предыдущем разделе соответствие между входами и выходами в диаграммном равенстве играет важную роль.

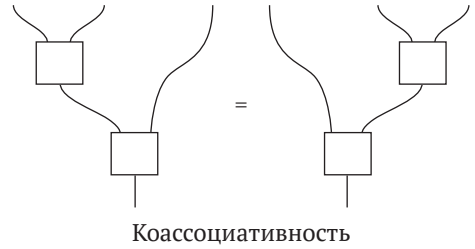
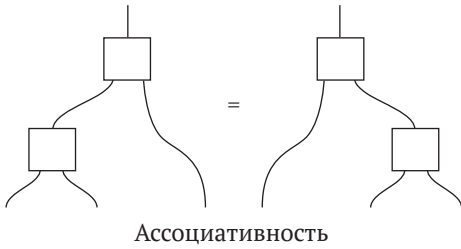
Продолжая эту процедуру, мы можем построить доказательство равенства (3.10):



Каждый шаг доказательства помечен использованным процессным равенством, за исключением шага 3, где просто применена деформация диаграммы. Отметим также, что на последнем шаге равенство (3.9) использовано справа на лево, что, конечно, допустимо.

Замечание* 3.17 (алгебра и коалгебра). Хотя действие cp совершенно очевидно, оно ничуть не похоже на операции, к которым мы привыкли в алгебре, например «сложение» и «умножение», – и именно потому, что имеет один вход и два выхода. Осознание того, что многие интересные операции действительно имеют несколько выходов, привело к появлению новой дисциплины – *коалгебры*. В терминах диаграмм приставка «ко» может рассматриваться как «вверх ногами». Так, например, если перевернуть операцию «умножение», то получится «коумножение». Если в обычной алгебре говорят об ассоциативности, унитар-

ности и коммутативности, то в коалгебре – о коассоциативности, коунитальности и кокоммутативности, и их определения получаются просто переворачиванием алгебраических выражений:



3.2. СХЕМНЫЕ ДИАГРАММЫ

Вспомнив, что блоки представляют процессы, мы можем определить две основные операции композиции процессов со следующей интерпретацией:

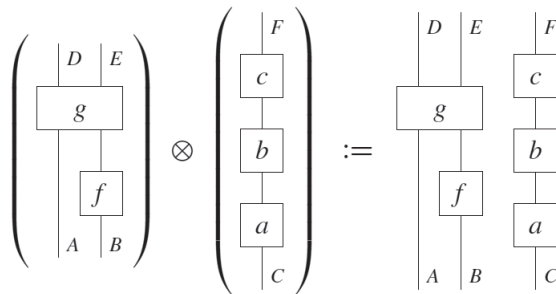
$$f \otimes g := \text{«процесс } f \text{ имеет место одновременно с процессом } g\text{»};$$

$$f \circ g := \text{«процесс } f \text{ имеет место после процесса } g\text{»}.$$

Эти операции позволяют определить важный класс диаграмм – *схемы*. Правда, в следующей главе мы увидим, что, несмотря на их важность, самые интересные процессы как раз схемами и не являются.

3.2.1. Параллельная композиция

Параллельная композиция означает, что две диаграммы располагаются бок о бок. Эта операция обозначается символом \otimes :



Любые две диаграммы можно скомпоновать таким образом, поскольку размещение бок о бок не подразумевает никаких соединений. Интуитивно это означает, что процессы протекают независимо друг от друга.

Эта операция композиции ассоциативна:

$$\left(\begin{array}{c} \boxed{f} \\ \boxed{g} \end{array} \otimes \boxed{h} \right) = \boxed{f} \boxed{g} \boxed{h} = \boxed{f} \otimes \left(\boxed{g} \otimes \boxed{h} \right) \quad (3.11)$$

и для нее существует нейтральный элемент, пустая диаграмма:

$$\begin{array}{c} | \\ \square \\ f \end{array} \otimes \begin{array}{c} \square \\ \square \\ \square \end{array} = \begin{array}{c} \square \\ \square \\ \square \end{array} \otimes \begin{array}{c} | \\ \square \\ f \end{array} = \begin{array}{c} | \\ \square \\ f \end{array} \quad (3.12)$$

Параллельную композицию можно определить и для системных типов. Если имеются типы A и B , то можно образовать новый тип $A \otimes B$, который называется *совместным системным типом*:

$$A \otimes B \quad | \quad := \quad \begin{array}{c} | \\ A \\ | \end{array} \quad \begin{array}{c} | \\ B \\ | \end{array}$$

Мы уже неявно использовали композицию системных типов, когда рисовали блоки с несколькими входами и выходами. Формально блок с тремя входами A, B, C и двумя выходами D и E – то же самое, что блок с одним входом $A \otimes B \otimes C$ и одним выходом $D \otimes E$:

$$\begin{array}{c} D \otimes E \\ | \\ \square \\ f \\ | \\ A \otimes B \otimes C \end{array} = \begin{array}{c} \begin{array}{c} | \\ D \\ | \end{array} \quad \begin{array}{c} | \\ E \\ | \end{array} \\ \square \\ f \\ \begin{array}{c} | \\ A \\ | \end{array} \quad \begin{array}{c} | \\ B \\ | \end{array} \quad \begin{array}{c} | \\ C \\ | \end{array} \end{array}$$

Существует также специальный «пустой» системный тип, обозначаемый символом I , который служит для представления «отсутствия входов», «отсутствия выходов» или того и другого сразу.

Примеры 3.18. Ниже показаны примеры блоков, не имеющих входных и (или) выходных проводов, записанные в терминах операции \otimes и типа I :

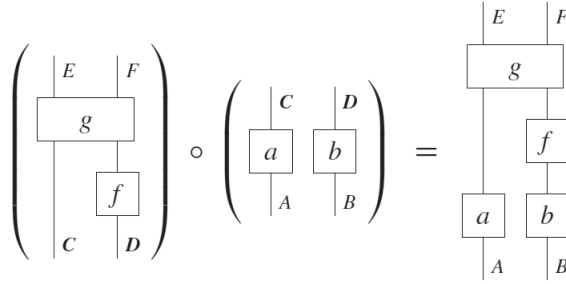
$$\begin{array}{c} I \\ | \\ \square \\ f \\ | \\ A \otimes B \otimes C \end{array} = \begin{array}{c} \square \\ f \\ \begin{array}{c} | \\ A \\ | \end{array} \quad \begin{array}{c} | \\ B \\ | \end{array} \quad \begin{array}{c} | \\ C \\ | \end{array} \end{array} \quad \begin{array}{c} A \otimes B \\ | \\ \square \\ g \\ | \\ I \end{array} = \begin{array}{c} \begin{array}{c} | \\ A \\ | \end{array} \quad \begin{array}{c} | \\ B \\ | \end{array} \\ \square \\ g \end{array} \quad \begin{array}{c} I \\ | \\ \square \\ s \\ | \\ I \end{array} = \begin{array}{c} \square \\ s \end{array}$$

Процессы, не имеющие входов и (или) выходов, играют в этой книге особую роль, а какую именно, мы впервые увидим в разделе 3.4.1.

В диаграммной нотации символ \otimes редко употребляется явно, поскольку предпочтительнее изображение совместных систем в форме с несколькими проводами.

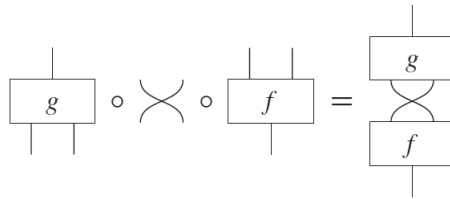
3.2.2. Последовательная композиция

Последовательная композиция заключается в соединении выходов первой диаграммы с входами второй. Она обозначается символом \circ :

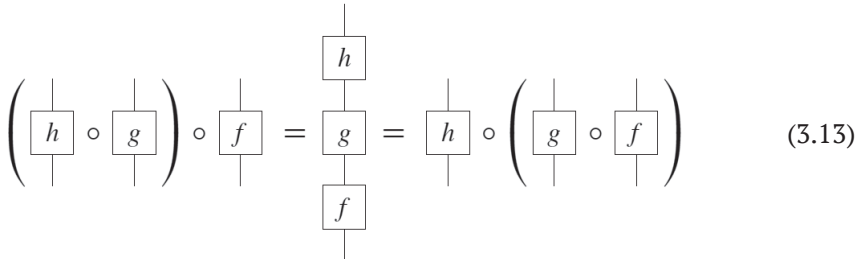


Интуитивно это означает, что сначала имеет место правый процесс, а затем левый, причем выходы первого подаются на входы второго. Очевидно, что так скомпоновать можно не всякую пару диаграмм; количество и типы входов левого процесса должны совпадать с количеством и типами выходов правого.

Мы предполагаем, что при последовательной композиции выходы соединяются с входами по порядку. Чтобы изменить этот порядок, можно воспользоваться символом *переконмутации*:



Левая часть этого равенства определена корректно, поскольку операция последовательной композиции тоже ассоциативна:



и тоже обладает нейтральным элементом – простым проводом подходящего типа:



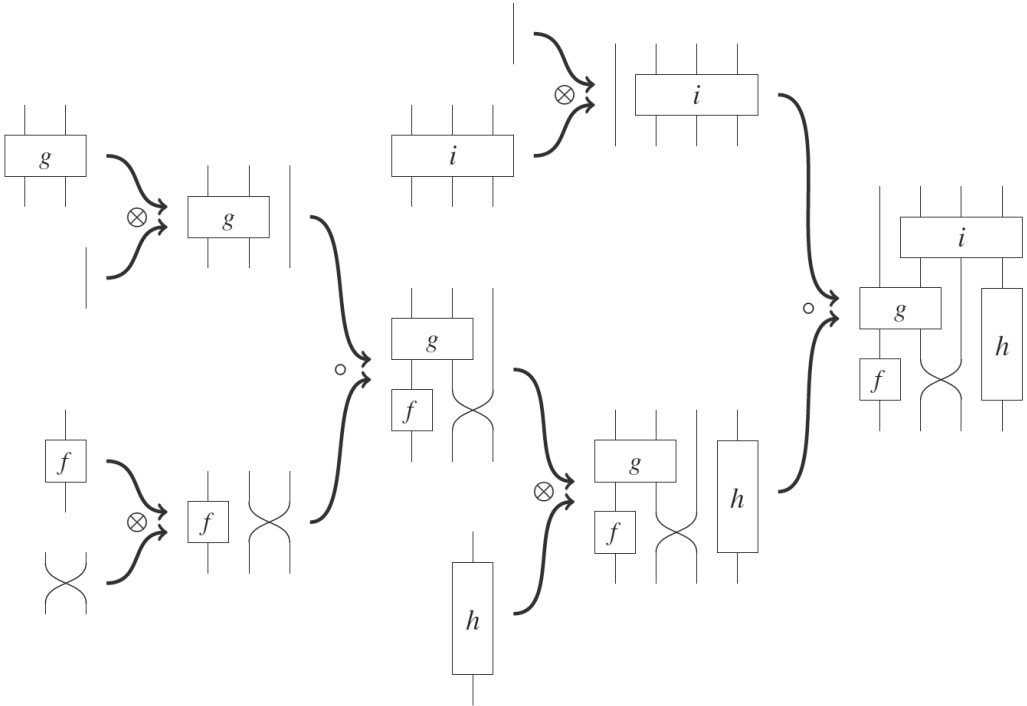
Мы уже встречали эти простые провода, или *тождественные* процессы, в разделе 3.1.3, где говорили, что их можно рассматривать как процессы, которые «ничего не делают» со своим входом. Если A – системный тип, то будем обозначать

тождественный процесс типа A символом 1_A . Пустая диаграмма – тоже тождественный процесс – системного типа I , поэтому будем обозначать ее 1_I .

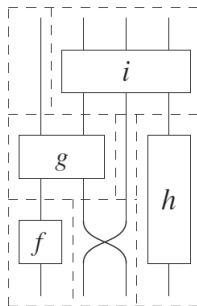
3.2.3. Два эквивалентных определения схем

Определение 3.19. Диаграмма называется *схемой*, если ее можно построить путем композиции блоков, включая тождественные процессы и перекоммутации, с применением операций \otimes и \circ .

Все диаграммы, приведенные в этой главе, являются схемами. Ниже приведен пример сборки схемы:



В результирующей диаграмме легко увидеть порядок сборки:



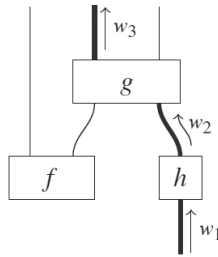
(3.15)

Отметим, однако, что такая декомпозиция диаграммы определяет порядок сборки неоднозначно (например, в силу ассоциативности операций \otimes и \circ три блока можно скомпоновать двумя способами), и у одной диаграммы может быть даже несколько разных декомпозиций. В следующем разделе мы увидим, что из-за этого обращение со схемами без привлечения диаграмм, только в терминах операций \otimes и \circ , оказывается исключительно неуклюжим.

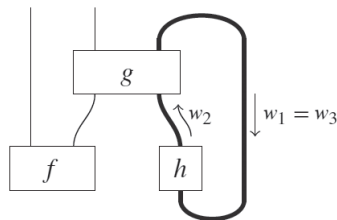
Не все диаграммы являются схемами. Чтобы понять, какие являются, мы дадим эквивалентную характеристику, которая опирается не на способ построения диаграмм, а на свойства, которыми они должны обладать.

Определение 3.20. *Ориентированным путем* называется список проводов (w_1, w_2, \dots, w_n) в диаграмме такой, что для любого $i < n$ провод w_i является входом в тот блок, для которого провод w_{i+1} является выходом. *Ориентированным циклом* называется ориентированный путь, который начинается и заканчивается в одном и том же блоке.

На рисунке ниже ориентированный путь изображен жирными линиями:



как и ориентированный цикл на следующем рисунке:



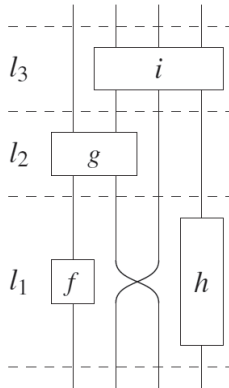
Замечание* 3.21. В разделе математики, который называется теорией графов, граф без ориентированных циклов называется *ориентированным ациклическим графом*.

Теорема 3.22. Следующие утверждения эквивалентны:

- диаграмма является схемой;
- диаграмма не содержит ориентированных циклов.

Доказательство. Существует (не единственный) способ выразить любую диаграмму без ориентированных циклов в терминах операций \otimes , \circ и перекмутации. Поскольку диаграмма не содержит ориентированных циклов, мы можем разбить ее на «слои» l_1, \dots, l_n , так что выходы каждого блока (включая тождественные процессы и перекмутации), принадлежащего слою l_i , будут соединены только

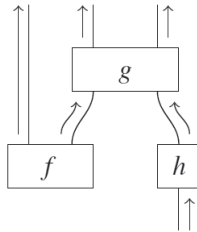
с блоками, принадлежащими слою l_{i+1} . Так, ниже показан один из способов разбивки на слои диаграммы (3.15):



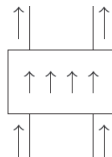
Внутри каждого слоя операция \otimes объединяет блоки в один, а операция \circ объединяет сами слои, так что мы действительно имеем схему. Наоборот, любую диаграмму, построенную только с применением операций \otimes и \circ , можно разложить на такие слои, откуда следует отсутствие ориентированных циклов. \square

Замечание* 3.23. В теории относительности «разбиение процесса на слои», описанное в доказательстве выше, называется *слоением*. В разделе 6.3.3 мы познакомимся со слоениями поближе.

Поскольку схемные диаграммы не содержат ориентированных циклов, мы можем придать им «темпоральную интерпретацию», считая, что время течет снизу вверх:



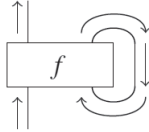
Главное, что ни один провод не направлен «назад во времени». В этой интерпретации неявно предполагается, что «внутри блоков» время течет от входов к выходам:



Так, в частности, обстоит дело с тождественными процессами и перекоммутациями:



Канонический пример диаграммы, не являющейся схемой, дает *петля обратной связи*, в которой выход блока соединен с его же входом



и образует ориентированный цикл, состоящий всего из одного провода.

Замечание* 3.24. У всех схемных диаграмм имеется свойство еще более фундаментальное, чем слоистость, – они обладают *причинно-следственной структурой*, т. е. для любых двух блоков f и g существует только три возможности:

- (1) f является причиной g ,
- (2) g является причиной f или
- (3) ни один блок не является причиной другого.

Мы еще вернемся к связи между схемами и причинно-следственной структурой пространства-времени в разделе 6.3, когда будем обсуждать связи между квантовой теорией и теорией относительности.

Схемные диаграммы предлагают подходящий язык для обсуждения экспериментальных установок, которые можно собрать в лаборатории, когда на входе имеются некоторые физические системы и (или) данные, а на выходе получаются другие физические системы и (или) данные. Тогда слова «параллельный» и «последовательный» описывают способ организации устройств.

Замечание 3.25. Может показаться странным выбор термина «схема» (circuit) для описания диаграмм, в которых запрещены петли обратной связи. Но эта терминология оправдана по двум причинам. Во-первых, она отражает терминологию, применяемую в литературе по квантовым вычислениям (ср. «квантовые схемы»). Во-вторых, хотя и невозможно включить петли обратной связи, мы все же можем симитировать поведение, похожее на обратную связь, введя в схему специальные блоки: «чашки» и «крышки». Как это работает, мы увидим в главе 4.

3.2.4. Диаграммы лучше алгебры

В разделе 3.1.3 мы показали представление диаграмм в терминах диаграммных формул, чтобы убедить читателя в том, что о диаграммах можно и нужно рассуждать как о математических объектах, ничем не уступающих формулам. Однако диаграммные формулы приводят к избыточному формализму, и производить их разбор отнюдь не легко. А только что мы видели, что, по крайней мере, схемные диаграммы можно описывать на более привычном алгебраическом языке с помощью операций \otimes и \circ . Быть может, это хорошая альтернатива диаграммам? Ответ – решительное НЕТ!

Алгебраический синтаксис с применением символов \otimes и \circ должен сопровождаться многочисленными дополнительными равенствами, которые уже встроены в диаграммный язык. Самый очевидный пример – тот факт, что ассоциативность и унитарность параллельной композиции обрабатываются автоматически.

- Изображение трех блоков рядом неявно подразумевает ассоциативность:

$$(f \otimes g) \otimes h = \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline g \\ \hline \end{array} \begin{array}{|c|} \hline h \\ \hline \end{array} = f \otimes (g \otimes h)$$

- Композиция с пустым блоком не делает ничего:

$$f \otimes 1_I = \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline \\ \hline \end{array} = \begin{array}{|c|} \hline f \\ \hline \end{array} = f$$

Ассоциативность и унитарность встроены также в последовательную композицию: для представления ассоциативности снова нужно убрать скобки, а для представления унитарности – изображать тождественные процессы в виде провода без блока.

Более впечатляющий пример получается, когда мы комбинируем две композиции. Рассмотрим такие два выражения:

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) \text{ и } (g_1 \circ f_1) \otimes (g_2 \circ f_2).$$

Очевидно, что в отсутствие дополнительных равенств, относящихся к символам \otimes и \circ , нельзя установить, что эти выражения равны. Но давайте вычислим соответствующие им диаграммы. Для первого выражения имеем:

$$\left(\begin{array}{|c|} \hline g_1 \\ \hline \end{array} \otimes \begin{array}{|c|} \hline g_2 \\ \hline \end{array} \right) \circ \left(\begin{array}{|c|} \hline f_1 \\ \hline \end{array} \otimes \begin{array}{|c|} \hline f_2 \\ \hline \end{array} \right) = \left(\begin{array}{|c|} \hline g_1 \\ \hline \end{array} \begin{array}{|c|} \hline g_2 \\ \hline \end{array} \right) \circ \left(\begin{array}{|c|} \hline f_1 \\ \hline \end{array} \begin{array}{|c|} \hline f_2 \\ \hline \end{array} \right) = \begin{array}{|c|} \hline g_1 \\ \hline f_1 \\ \hline \end{array} \begin{array}{|c|} \hline g_2 \\ \hline f_2 \\ \hline \end{array}$$

а для второго:

$$\left(\begin{array}{|c|} \hline g_1 \\ \hline f_1 \\ \hline \end{array} \right) \otimes \left(\begin{array}{|c|} \hline g_2 \\ \hline f_2 \\ \hline \end{array} \right) = \left(\begin{array}{|c|} \hline g_1 \\ \hline f_1 \\ \hline \end{array} \right) \otimes \left(\begin{array}{|c|} \hline g_2 \\ \hline f_2 \\ \hline \end{array} \right) = \begin{array}{|c|} \hline g_1 \\ \hline f_1 \\ \hline \end{array} \begin{array}{|c|} \hline g_2 \\ \hline f_2 \\ \hline \end{array}$$

Получились две одинаковые диаграммы!

Поскольку символы \otimes и \circ предполагается использовать в роли алгебраического синтаксиса для диаграмм, необходимо дополнить их новым равенством:

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2), \tag{3.16}$$

которое на диаграммном языке – просто тавтология! Так в чем же истинный смысл равенства (3.16)? Оно утверждает, что следующий составной процесс:

процесс g_1 протекает одновременно с процессом g_2
 после
 процесс f_1 протекает одновременно с процессом f_2

совпадает с таким составным процессом:

процесс g_1 имеет место после процесса f_1
 протекает одновременно
 процесс g_2 имеет место после процесса f_2 .

Это очевидно, и в диаграммном языке мы получаем это задаром, тогда как в алгебраическом должны явно формулировать.

На основе равенств, которые мы постулировали выше для символов \otimes и \circ , можно вывести много новых. Например, равенство

$$g \circ f = g \otimes f$$

выводится путем комбинирования (3.12), (3.14) и (3.16):

$$g \circ f = \left((g \circ 1_I) \otimes 1_I \right) \circ \left(1_I \otimes (f \circ 1_I) \right) = \left((g \circ 1_I) \otimes 1_I \right) \circ \left(1_I \otimes (f \circ 1_I) \right) = g \circ f$$

тогда как на диаграммном языке оно снова является тавтологией. Еще один пример дополнительного равенства для символов \otimes и \circ включает скрещивание:

$$f \otimes g = g \otimes f \tag{3.17}$$

Легко представить себе, сколько еще нетривиальных равенств можно вывести путем комбинирования (3.11), (3.12), (3.14), (3.16) и (3.17). И многие из них вовсе не очевидны без рисования диаграмм.

Упражнение* 3.26. Предположим, что справедливо следующее равенство:

$$\sigma_{A \otimes B, C} = (\sigma_{A, C} \otimes 1_B) \circ (1_A \otimes \sigma_{B, C}), \text{ где } \sigma_{A, B} := \begin{array}{c} B \quad A \\ \diagdown \quad \diagup \\ A \quad B \end{array}$$

Докажите первое и последнее равенства из примера 3.6, рассматривая их как алгебраические равенства. Используйте при этом равенство выше и другие алгебраические равенства из этого раздела.

Так почему же все так усложняется? Да просто потому, что мы пытаемся втиснуть нечто, вольготно располагающееся в двух измерениях (диаграмму), в одномерную клетку («линейную» алгебраическую нотацию). При попытке сделать это горизонтальное и вертикальное измерения на листе бумаги схлопываются в одно, и мы вынуждены прибегать к дополнительному синтаксису (например, скобкам), чтобы различить параллельную и последовательную композиции в новом «сжатом» мире. А затем на этот дополнительный синтаксис приходится накладывать дополнительные правила, чтобы обеспечить возможность преобразований, которые для диаграмм выглядят естественно. И вот кульминационный момент:

Диаграммы правят миром!

Можно еще много говорить о связи между алгебраическими равенствами и диаграммными рассуждениями, особенно в контексте *теории (моноидальных) категорий*. И хотя это необязательно для понимания книги, отсылаем интересующего читателя к дополнительному материалу в разделе 3.6.2.

3.3. ФУНКЦИИ И ОТНОШЕНИЯ КАК ПРОЦЕССЫ

Сейчас мы введем в рассмотрение две простые процессные теории: **функций** и **отношений**. Они полезны не только как конкретные примеры процессных теорий, помогающие понять некоторые концепции, которые пока еще не описаны, но и для установления двух важных фактов:

- традиционные математические конструкции (в данном случае множества) могут образовывать типы процессных теорий и
- даже для некоторых фиксированных системных типов выбор процессов оказывает существенное влияние на характер процессной теории. В частности, хотя и теория **функций**, и теория **отношений** основаны на множествах, в этой и следующей главах мы увидим, что их свойства как процессных теорий кардинально различаются.

По этим причинам указанные примеры процессных теорий и в особенности, как ни странно, теория **отношений** оказываются полезными ступеньками на пути к процессным теориям **линейных отображений** и **квантовых отображений**.

3.3.1. Множества

Чтобы определить процессную теорию, мы должны сначала определить системные типы, а затем сами процессы. В случае **функций** и **отношений** системными типами являются просто множества. Мы встретим некоторые знакомые множества, например: множество натуральных чисел \mathbb{N} , множество вещественных чисел \mathbb{R} , множество комплексных чисел \mathbb{C} (свойства которого будут рассмотрены в разделе* 5.3.1) и множество

$$\mathbb{B} := \{0, 1\},$$

которое называется множеством *булевых*, или *битовых*, значений. Совместные системные типы образуются путем построения *декартова произведения* множеств:

$$A \otimes B := A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Для трех и более множеств определение аналогично, просто пары элементов заменяются *кортежами*:

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \mid a_i \in A_i\}.$$

Если не обращать внимания на скобки в кортежах, т. е. положить:

$$((a, b), c) = (a, b, c) = (a, (b, c)),$$

то параллельная композиция систем ассоциативна:

$$A \times (B \times C) = (A \times B) \times C,$$

как и должно быть.

Пример 3.27. Множество *битовых строк* длины n можно выразить в виде декартова произведения n множеств:

$$\underbrace{\mathbb{B} \times \dots \times \mathbb{B}}_n.$$

Результат можно интерпретировать как множество натуральных чисел от 0 до $2^n - 1$, если рассматривать битовую строку как двоичное представление числа. Например, для $n = 4$ мы представляем 0 в виде (0, 0, 0, 0), 1 – в виде (0, 0, 0, 1), 2 – в виде (0, 0, 1, 0) и т. д. до 15, которое представляется в виде (1, 1, 1, 1). Этот прием, часто используемый в информатике, важен и в нашей книге.

Тривиальный тип I определяется как множество $\{*\}$, состоящее из единственного элемента, который здесь обозначен $*$. Если всегда опускать $*$ в кортежах, т. е. считать, что

$$(a, *) = a = (*, a),$$

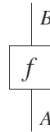
то $\{*\}$ становится нейтральным элементом для параллельной композиции проводов:

$$A \times \{*\} = A = \{*\} \times A.$$

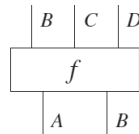
Замечание* 3.28. Строго говоря, множества $(A \times B) \times C$ и $A \times (B \times C)$, а также множества $A \times \{*\}$ и A не равны, а *изоморфны*, т. е. между их элементами можно установить взаимно однозначное соответствие. На самом деле они не просто изоморфны, а *естественно изоморфны*, а это значит, что для всех практических целей их можно рассматривать как равные. Отсутствие строгого равенства объясняется в основном «алгебраическим формализмом», на который мы сетовали в разделе 3.2.4, поэтому на работу с диаграммами не влияет. В разделе* 3.6.2 будут приведены дополнительные сведения об этом тонком моменте.

3.3.2. Функции

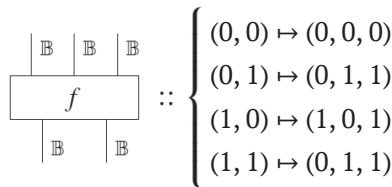
В процессной теории **функций** каждый процесс



является функцией, отображающей множество A в множество B . Поскольку совместные системы образуются с помощью декартова произведения, функция с несколькими входами и выходами, например



является функцией из декартова произведения $A \times B$ в декартово произведение $B \times C \times D$. Таким образом, f отображает пары $(a, b) \in A \times B$ в тройки $(b', c, d) \in B \times C \times D$. Конкретно, функция из $\mathbb{B} \times \mathbb{B}$ в $\mathbb{B} \times \mathbb{B} \times \mathbb{B}$ переводит битовые строки длины 2 в битовые строки длины 3, например:



Зная, что такое системные типы и процессы, мы теперь должны определить, что означает «соединение процессов проводами» (см. определение 3.1). Для этого мы определим семантику параллельной и последовательной композиций функций. Последовательная композиция – это обычная композиция функций:

$$(g \circ f)(a) := g(f(a)). \tag{3.18}$$

Параллельная композиция определяется как применение каждой функции к соответствующему элементу пары:

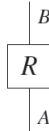
$$(f \otimes g)(a, b) := (f(a), g(b)). \tag{3.19}$$

Теперь мы знаем все, что необходимо для вычисления функции, представленной схемной диаграммой, поскольку можем разложить такую диаграмму на операции \otimes и \circ :

Прочитав эту книгу, вы сможете без труда написать ответ для обеих диаграмм (не по памяти, а потому что с помощью предлагаемых нами инструментов вычисление оказывается совсем простым!).

3.3.3. Отношения

В процессной теории **отношений** каждый процесс



является отношением между множеством A и множеством B , т. е. подмножеством их декартова произведения:

$$R \subseteq A \times B.$$

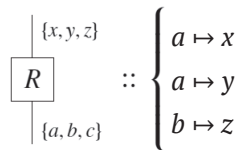
Говорят, что a и b *связаны отношением* R , если $(a, b) \in R$. Полезно использовать нотацию, больше напоминающую функцию:

$$a \mapsto b \text{ вместо } (a, b) \in R, \tag{3.20}$$

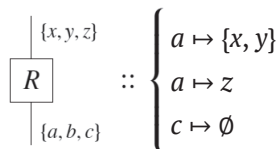
a в качестве аналога обозначения $f(a)$ для функций можно положить:

$$R(a) := \{b \mid R : a \mapsto b\}.$$

Таким образом, отношения, являющиеся функциями, можно записать в той же нотации, что и выше. Однако для отношений более общего вида разрешается отображать один входной элемент в любое число выходных. Например:



что можно записать также в виде:

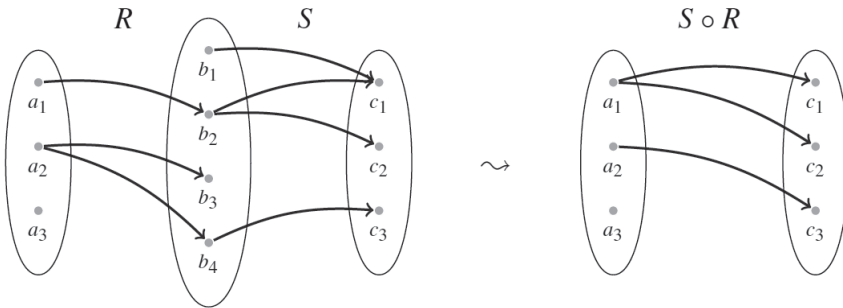


Будучи интерпретировано как процесс, такое отношение похоже на функцию, в которую добавлена *недетерминированность*: один вход может отображаться в несколько выходов или не отображаться ни в один.

Последовательная композиция отношений производится следующим образом: элемент a находится в отношении $S \circ R$ с элементом c тогда и только тогда, когда существует такой элемент b , что $R :: a \mapsto b$ и $S :: b \mapsto c$. В символическом виде:

$$\begin{array}{c} \boxed{S} \\ | \\ \boxed{R} \end{array} :: a \mapsto c \iff \exists b \left(\begin{array}{c} | \\ \boxed{R} \\ | \end{array} :: a \mapsto b \text{ и } \begin{array}{c} | \\ \boxed{S} \\ | \end{array} :: b \mapsto c \right) \quad (3.21)$$

Здесь фраза «тогда и только тогда» определяет новое отношение, т. е. точно описывает, какие элементы a и c связаны отношением $S \circ R$. В школе вы, наверное, видели такую картинку с изображением композиции отношений:



Здесь элементы связаны отношением $S \circ R$ тогда и только тогда, когда на левой диаграмме существует соединяющий их путь.

Параллельная композиция отношений определяется следующим образом:

$$\begin{array}{c} \boxed{R} \\ | \\ \boxed{S} \end{array} :: (a, b) \mapsto (c, d) \iff \left(\begin{array}{c} | \\ \boxed{R} \\ | \end{array} :: a \mapsto c \text{ и } \begin{array}{c} | \\ \boxed{S} \\ | \end{array} :: b \mapsto d \right) \quad (3.22)$$

Как и в случае функций, мы теперь можем вычислить отношение, представленное диаграммой, разложив его на операции \otimes и \circ и применив затем равенства (3.21) и (3.22), но это может оказаться довольно трудоемко. По счастью, существует общая процедура непосредственного вычисления диаграмм отношений. Предположим, что известны отношения R, S, T , а мы хотим вычислить их композицию P :

$$\begin{array}{c} | A | B | C \\ \boxed{P} \\ | B | A \end{array} \quad := \quad \begin{array}{c} | A | B | C \\ \boxed{S} \\ | A | D \\ \boxed{R} \quad \boxed{T} \\ | B | A \end{array} \quad (3.23)$$

Шаг 1: записать P в виде диаграммной формулы:

$$P_{B_1 A_1}^{A_2 B_2 C_1} = R_{B_1}^{A_2 A_3} S_{A_3 D_1}^{B_2 C_1} T_{A_1}^{D_1}.$$

Шаг 2: заменить имена проводов элементами соответствующего множества. Например, B_2 заменяется элементом $b_2 \in B$:

$$P_{b_1 a_1}^{a_2 b_2 c_1} = R_{b_1}^{a_2 a_3} S_{a_3 d_1}^{b_2 c_1} T_{a_1}^{d_1}.$$

Шаг 3: заменить имена блоков отношениями, которые отображают элемент(ы) в нижнем индексе в элемент(ы) в верхнем индексе, и присоединить « $\exists x$ » к каждому повторяющемуся элементу x :

$$P :: (b_1, a_1) \mapsto (a_2, b_2, c_1) \Leftrightarrow \exists a_3 \exists d_1 \left(\begin{array}{l} R :: b_1 \mapsto (a_2, a_3) \text{ и} \\ S :: (a_3, d_1) \mapsto (b_2, c_1) \text{ и} \\ T :: a_1 \mapsto d_1 \end{array} \right).$$

Если входы и (или) выходы отсутствуют, то следует использовать $*$, т. е. единственный элемент множества $I = \{*\}$.

Шаг 4: теперь выражение в правой части эквиваленции \Leftrightarrow однозначно характеризует все связанные отношения кортежи в левой части, и поэтому его можно использовать для вычисления P .

Для частных случаев последовательной и параллельной композиций отношений мы вновь получаем равенства (3.21) и (3.22) соответственно. Чтобы убедиться в этом, нарисуйте диаграммы $f \otimes g$ и $g \circ f$, примените шаги 1–3 и посмотрите, что получится.

Упражнение 3.31. Предположим, что A, B, C и D – следующие множества:

$$\begin{aligned} A &= \{a1, a2, a3\} \\ B &= \mathbb{B} \\ C &= \{\mathbf{red}, \mathbf{green}\} \\ D &= \mathbb{N} \end{aligned}$$

Вычислите P , как предписано диаграммой (3.23) для таких отношений R, S, T :

$$R :: \begin{cases} 1 \mapsto (a_1, a_1) \\ 1 \mapsto (a_1, a_2) \end{cases} \quad S :: \begin{cases} (a_1, 5) \mapsto (0, \mathbf{red}) \\ (a_1, 5) \mapsto (1, \mathbf{red}) \\ (a_2, 6) \mapsto (1, \mathbf{green}) \end{cases} \quad T :: \begin{cases} a_1 \mapsto 200 \\ a_3 \mapsto 5 \end{cases}$$

и для таких отношений R, S, T :

$$R :: \begin{cases} 0 \mapsto A \times \{a_2, a_3\} \\ 1 \mapsto A \times \{a_2, a_3\} \end{cases} \quad S :: \begin{cases} (a_1, 0) \mapsto \mathbb{B} \times \{\mathbf{red}, \mathbf{green}\} \\ (a_1, 1) \mapsto \mathbb{B} \times \{\mathbf{red}, \mathbf{green}\} \\ (a_1, 2) \mapsto \mathbb{B} \times \{\mathbf{red}, \mathbf{green}\} \\ \vdots \end{cases} \quad T :: \begin{cases} a_1 \mapsto \mathbb{N} \\ a_2 \mapsto \mathbb{N} \\ a_3 \mapsto \mathbb{N} \end{cases}$$

Замечание* 3.32. В силу похожести процессных теорий **отношений** и **линейных отображений** и особенно того факта, что обе теории допускают *матричное исчисление* (см. главу 5), этот прием вычисления диаграмм отношений применим также к вычислению диаграмм линейных отображений, как мы увидим в разделе 5.2.4, а стало быть, касается и **квантовых процессов**. На самом деле если рассматривать отношения как матрицы с булевыми элементами, то вычисления оказываются в точности идентичными.

3.3.4. Сравнение функций с отношениями

Если ограничить определения (3.21) и (3.22) функциями, то получатся соответственно определения (3.18) и (3.19). В обоих случаях мы пользуемся тем фактом, что функции соотносят каждый входной элемент с единственным выходным, поэтому запись получается проще. Например, в случае параллельной композиции функций $f: A \mapsto C$ и $g: B \mapsto D$ для любых $a \in A$ и $b \in B$ существуют единственные элементы $c \in C$ и $d \in D$ такие, что $f:: a \mapsto c$ и $g:: b \mapsto d$, и потому построение $f \otimes g$ сводится к сопоставлению этих элементов функциям, как в (3.19). С другой стороны, для отношений $R \otimes S:: (a, b) \mapsto (c, d)$, если существуют элементы $c \in C$ и $d \in D$ такие, что $R:: a \mapsto c$ и $S:: b \mapsto d$, и, конечно, может существовать более одной такой пары (c, d) .

Далее, поскольку:

- 1) и для **функций**, и для **отношений** системными типами являются множества и, в частности, системные типы теории **отношений** включают системные типы теории **функций**;
- 2) функции являются частным случаем отношений и, следовательно, процессы теории **отношений** включают процессы теории **функций**;
- 3) последовательная композиция **функций** является частным случаем последовательной композиции **отношений**, а параллельная композиция \otimes **функций** является частным случаем параллельной композиции **отношений**, –

мы говорим, что процессная теория **функций** является *подтеорией* процессной теории **отношений**, и записываем этот факт в виде:

функции \subseteq отношения.

Разумеется, отношений гораздо больше, чем функций, и в этой книге мы встретим много важных отношений, которые функциями не являются. Именно благодаря этим дополнительным отношениям процессная теория **отношений** в гораздо большей степени напоминает **линейные отображения**, а не **функции**.

3.4. СПЕЦИАЛЬНЫЕ ПРОЦЕССЫ

В этом разделе мы остановимся на нескольких типах процессов, которые будут играть центральную роль в этой книге.

3.4.1. Состояния, эффекты и числа

До сих пор мы относились к блокам, не имеющим ни входов, ни выходов, как к любым другим блокам. Однако при интерпретации в качестве процессов такие блоки обладают одним очень важным свойством.

- *Состояниями* называются процессы без входов. Если говорить о предназначении, то это «подготовительные процедуры». Они представляются символом



Если система A может находиться в любом состоянии из некоторого множества допустимых, то подготовительная процедура порождает систему типа A в конкретном состоянии ψ , выбранном из этого множества. Отсутствие проводов означает, что мы не знаем (или не хотим знать), откуда взялась эта система, важно лишь, что она есть и находится в определенном состоянии. Например, если мы говорим «этот бит находится в начальном состоянии 0», значит, нас не интересует его предыстория, коль скоро гарантируется, что сейчас он равен 0 и готов для выполнения дальнейших вычислений. Другой пример: когда мы говорим «это свежий сырой картофель», нам не важно, на какой ферме он был выращен и чьим навозом его удобряли; главное, что картофель сырой, свежий и, стало быть, годится для жарки.

- *Эффектами* называются процессы без выходов. Мы заимствовали эту терминологию из квантовой теории, в которой эффекты играют важнейшую роль. Мы будем представлять их таким символом:



Понятие эффекта двойственно понятию состояния в том смысле, что в начале эффекта существует система, а после него не остается ничего – или нас не интересует, что осталось. Простейший пример эффекта – *отбрасывание* системы, когда система уничтожается (или просто игнорируется). Менее тривиальные эффекты связаны с вещами, которые могут произойти или не произойти в зависимости от состояния системы. Например, события «бомба взорвалась», «фотон был поглощен», «всю еду съели» или «додо вымерли» можно считать эффектами, поскольку после них не остается ни бомбы, ни фотона, ни еды, ни додо.

С точки зрения использования, эффекты служат для моделирования «испытаний». Говоря, что эффект «имеет место», мы имеем в виду, что подвергли систему проверке на обладание некоторым свойством и получили утвердительный ответ, после чего можем отбросить систему, или, как часто бывает, система уничтожается в процессе проверки. В общем и целом испытание состоит из следующих частей:

- 1) вопрос о системе;
- 2) процедура, позволяющая получить ответ на этот вопрос;
- 3) событие, состоящее в получении утвердительного ответа, означающего, что эффект «имел место».

Таким образом, испытание не сводится к одному лишь ответу на вопрос. Например, если мы рисуем, то можно задать вопрос: «Ручка красная?» Соответствующее испытание выглядело бы так: взять лист бумаги, что-то написать на нем ручкой и убедиться, что цвет написанного красный. Разумеется, в этом случае обязательно затем ломать ручку (и обычно так не делают). Настоящее уничтоже-

ние имеет место, когда задан вопрос: «Это хорошая спичка?» Испытание заключается в том, чтобы попытаться зажечь спичку и убедиться в том, что она горит. После чего спички уже не существует. Акт отбрасывания системы также является испытанием, пусть и тривиальным. Убедившись, что некоторое свойство выполняется для любого состояния системы (например, «существует ли эта система?»), мы отбрасываем ее. Конечно, это глупое испытание, потому что мы не получили никакой информации, но системы больше нет.

На первый взгляд кажется, что испытания – нечто большее, чем «подготовительные процедуры наоборот». Но если допустить, что подготовительные процедуры могут завершаться неудачно (как часто бывает в лаборатории), то оказывается, что оба понятия в действительности симметричны. Подготовительная процедура состоит из следующих частей:

- 1) состояние, в котором должна оказаться система;
- 2) процедура перевода системы в это состояние;
- 3) событие, состоящее в получении утвердительного ответа, означающего, что состояние успешно подготовлено.

Конечно, в отличие от испытаний, мы можем продолжать попытки, пока подготовка не окажется успешной (или не кончатся деньги), поэтому часть 3 обычно игнорируется.

В результате композиции состояния и эффекта возникает специальный блок третьего вида:

$$\begin{array}{c} \triangle \\ \pi \\ | \\ \circ \\ | \\ \nabla \\ \psi \end{array} = \begin{array}{c} \triangle \\ \pi \\ | \\ \nabla \\ \psi \end{array}$$

- *Числами* называются процессы без входов и выходов. Мы будем обозначать их символом

$$\lambda$$

Наверное, вы сейчас подумали: «Минуточку! Я же знаю, что такое числа, они не имеют никакого отношения к процессам без входов и выходов!» Так-то оно так, но те числа, которые вы учили в школе (целые, вещественные, возможно, даже комплексные), – частные случаи очень общего понятия «числа».

А что такое процесс без входов и выходов? Это просто набор чего-то, что можно «перемножить» благодаря наличию операции \otimes (или, что в данном случае все равно, операции \circ). То есть если λ и μ – числа, то

$$\lambda \otimes \mu := \begin{array}{c} \diamond \\ \lambda \\ \diamond \end{array} \begin{array}{c} \diamond \\ \mu \\ \diamond \end{array}$$

– тоже число. Кроме того, в разделе 3.2.4 мы видели, что диаграммы правят миром, поэтому такое «умножение» ассоциативно:

$$(\lambda \otimes \mu) \otimes \nu = \begin{array}{c} \diamond \\ \lambda \\ \diamond \end{array} \begin{array}{c} \diamond \\ \mu \\ \diamond \end{array} \begin{array}{c} \diamond \\ \nu \\ \diamond \end{array} = \lambda \otimes (\mu \otimes \nu)$$

и обладает нейтральным элементом, который представляется пустой диаграммой:

$$\lambda \otimes 1_I = \diamond_{\lambda} \boxed{} = \lambda$$

И наконец, в силу отсутствия входов и выходов числа можно беспрепятственно двигать в пределах диаграммы и даже устраивать танцы:

$$\begin{array}{ccccccc} \diamond_{\lambda} & = & \diamond_{\lambda} & & \diamond_{\mu} & = & \diamond_{\mu} \\ \diamond_{\mu} & = & \diamond_{\mu} & = & \diamond_{\lambda} \diamond_{\mu} & = & \diamond_{\mu} \diamond_{\lambda} \end{array} \quad (3.24)$$

Этот танец показывает, что умножение чисел еще и *коммутативно*. Таким образом, объекты, которые мы называем «числами», допускают операцию умножения, являющуюся ассоциативной, коммутативной и обладающей единицей (т. е. числом, которое означает «1»). Знакомо звучит? В математике такое множество называют *коммутативным моноидом*. А кто-то скажет проще: «практически любые виды чисел, которые только можно вообразить».

Замечание* 3.33. Замечательно простое доказательство, показанное на (3.24), известно под названием *аргумента Экмана–Хилтона*. Оно показывает, что если имеется пара ассоциативных операций (в данном случае операции \otimes и \circ , применяемые к числам), которые обладают общей единицей (в обоих случаях 1_I) и удовлетворяют перестановочному закону (3.16) (который для диаграмм мы получаем даром), то обе эти операции коммутативны и на самом деле представляют собой одну и ту же операцию. Здесь мы воспользовались этим аргументом, чтобы доказать, что \otimes (или, эквивалентно, \circ) – коммутативная операция «умножения» чисел в любой процессной теории.

Но как интерпретировать тот факт, что при встрече состояния с эффектом на свет появляется число? Одна исключительно полезная интерпретация заключается в том, что это число дает *вероятность* эффекта, при условии что система находится в определенном состоянии. Или, в терминах испытаний, это вероятность того, что при проверке состояния ψ на эффект π мы получим утвердительный ответ:

$$\boxed{\begin{array}{l} \text{Испытание} \left\{ \begin{array}{c} \triangle_{\pi} \\ \downarrow \\ \triangle_{\psi} \end{array} \right\} \\ \text{Состояние} \left\{ \begin{array}{c} \triangle_{\psi} \\ \downarrow \\ \triangle_{\pi} \end{array} \right\} \end{array}} \text{Вероятность} \quad (3.25)$$

Мы называем это *обобщенным правилом Борна*. Слово «обобщенный» употребляется, потому что это правило имеет смысл в любой процессной теории. В главе 6 мы увидим, что если ограничиться теорией **квантовых отображений**, то получится правило, применяемое для вычисления всех вероятностей в квантовой теории и называемое просто *правилом Борна*.

Замечание* 3.34. Читатель, знакомый с квантовой теорией, может подумать, что в (3.25) мы получаем не вероятность, а комплексное число (иначе говоря, «амплитуду»), которое для получения вероятности нужно еще умножить на сопряжен-

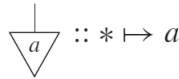
ное к нему. Так оно и есть, если мы имеем дело со старыми добрыми **линейными отображениями**. Но в **квантовые отображения** этот шаг уже «встроен», поэтому числа всегда оказываются положительными вещественными числами. В примере 3.37 ниже мы покажем, что диаграмма (3.25) действительно порождает правильные вероятности в квантовой теории, а в разделе 6.1.1 объясним, как переход от комплексных чисел к вероятностям путем умножения числа на комплексно-сопряженное к нему изящно встроен в теорию **квантовых отображений**.

Во многих физических теориях и в квантовой теории в частности состояния трактуются как элементы некоторого множества (или пространства), а процессы – как функции из одного множества (пространства) в другое. Числа снова выглядят как нечто совсем иное, а у эффектов в ряде случаев не просматривается никакого очевидного аналога. Но в диаграммном языке мы рассматриваем состояния, эффекты и числа единообразно – как частные случаи процессов. Это очень удобно, потому что позволяет определить многие концепции сразу для произвольных процессов, а ко всем частным случаям они будут применимы автоматически.

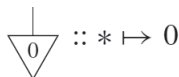
Теперь мы посмотрим, как эти специальные процессы выглядят в уже встречавшихся нам процессных теориях.

Пример 3.35 (функции)

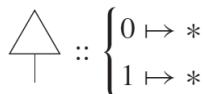
1. *Состояния соответствуют элементам множества.* Поскольку «отсутствие проводов» означает множество из одного элемента $\{*\}$ (см. раздел 3.3.1), то состояние – это функция из $\{*\}$ в другое множество A . Эта функция «указывает» на единственный элемент $a \in A$, а именно образ $*$:



Обратно, для любого $a \in A$ существует единственная функция, которая переводит $*$ в a , поэтому элементы A и функции из $\{*\}$ в A – по существу, одно и то же, что позволяет нам просто называть эту функцию a . Если положить $A := \mathbb{B}$, то существует ровно два состояния:



2. *Эффекты тривиальны.* Для любого множества A существует ровно одна функция из A в $\{*\}$, а именно функция, отображающая любой элемент в $*$. Поэтому ей и имя-то присваивать не стоит. В случае $A := \mathbb{B}$ этот единственный эффект имеет вид:



3. *Числа тривиальны.* По той же причине, что эффекты. Поскольку число – частный случай эффекта, существует всего одно число, а именно функция, переводящая $*$ в $*$. Это единственное число уже представлено пустой диаграммой, поэтому мы даже рисовать его не будем!

Эти два числа интерпретируются как «невозможно» и «возможно», что выглядит вполне разумно, если подумать, что происходит, когда мы проверяем, находится ли система в определенном состоянии. Сначала рассмотрим диаграмму

$$\begin{array}{c} \triangle \\ 0 \\ \hline 0 \\ \triangle \end{array} = \square$$

Если система находится в состоянии 0, то при тестировании на эффект 0 можно получить положительный результат. Конечно, это возможно, и на самом деле это должно происходить всегда! Однако, поскольку в **отношениях** нет числа «определенное», «возможное» – это максимум, что мы можем получить. Далее рассмотрим:

$$\begin{array}{c} \triangle \\ 0 \\ \hline 1 \\ \triangle \end{array} = \square$$

Если система находится в состоянии 0 или 1, то *возможно* (хотя и не наверняка), что проверка на 0 даст положительный результат. Затем рассмотрим диаграмму

$$\begin{array}{c} \triangle \\ 0 \\ \hline 1 \\ \triangle \end{array} = \emptyset$$

Если система находится в состоянии 0, то абсолютно *невозможно* получить положительный результат при проверке на 1.

В следующем примере со звездочкой используется нотация, которая будет введена в последующих двух главах. Однако читателям, знакомым с квантовой теорией, они могут оказаться полезными. Остальным лучше пока пропустить этот пример.

Пример* 3.37 (квантовые отображения). Квантовые отображения дают весьма элегантный способ выразить вполне положительные отображения, частными случаями которых являются смешанные квантовые состояния, квантовые эффекты и вероятности. Им посвящена большая часть главы 6, а этот пример – лишь первое знакомство. Для удобства знакомых с квантовой теорией мы пользуемся традиционной терминологией и обозначениями, а не их аналогами, в большей степени ориентированными на процессную теорию, которые будут введены в главе 6.

1. *Состояния соответствуют операторам плотности.* Они изображаются в виде



Действие вполне положительного отображения \mathcal{E} на состояние ρ , то есть

$$\mathcal{E} :: \rho \mapsto \sum_i A_i^\dagger \rho A_i,$$

изображается в виде:



2. Эффекты – это положительные линейные функционалы. Они изображаются в виде



для некоторого положительного оператора A . Их действие на состояние ρ , то есть

$$\rho \mapsto \text{tr}(A\rho),$$

(где tr – след матрицы) изображается в виде



(3.26)

Частным случаем является сам след:

$$\rho \mapsto \text{tr}(\rho),$$

который представляет «отбрасывание системы» и обозначается символом



Условия «след 1» (для состояний) и «сохранение следа» (для вполне положительных отображений) имеют соответственно вид:

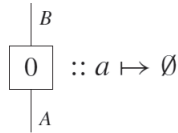


3. Числа положительные вещественные. Правило Борна (3.25) теперь принимает вид (3.26) и действительно порождает положительные вещественные числа, которые интерпретируются как вероятности.

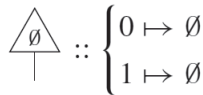
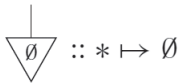
Читателю может показаться странным, что матрицы плотности изображаются как состояния, т. е. без входов, а не как процессы с входами и выходами (ср. с «оператором» плотности), и что вполне положительные отображения изображаются как процессы с входами и выходами, а не объекты, которые принимают и возвращают процессы с входами и выходами (ср. с «супероператором»). Это следствие того, как мы определяем *квантовые отображения*, и, конечно, правильно, потому что теперь диаграммы отражают истинную природу квантовых состояний, эффектов и процессов.

3.4.2. Как выразить невозможное: нулевые диаграммы

Примером (нефункциональных) отношений являются *нулевые отношения*, которые «не соотносят ничего ни с чем», т. е. не существует таких $a \in A$ и $b \in B$, для которых $R :: a \mapsto b$, или эквивалентно:



Нам уже встречались такие диаграммы, а именно:



$$\emptyset :: * \mapsto \emptyset$$

Все они представляют нечто невозможное.

Поскольку эффект представляет испытание, в котором мы успешно проверяем ответ на некоторый вопрос, то может случиться, что для каких-то состояний такой эффект попросту невозможен. И что получится, если представить композицию этого состояния и этого эффекта на диаграммном языке? Конечно, мы должны получить число, соответствующее понятию «невозможно». Такие невозможные числа и, более общо, невозможные процессы допускают элегантную характеристику в процессной теории.

В частном случае **отношений** легко видеть, что как последовательная, так и параллельная композиция нулевого отношения с любым отношением снова является нулевым отношением. Для общих процессных теорий, если эффект π невозможен в состоянии ψ , то число

$$0 = \begin{array}{c} \triangle \pi \\ | \\ \nabla \psi \end{array}$$

должно представлять невозможность. Конечно, если некоторая часть процесса невозможна, то и весь процесс невозможен, следовательно:

$$\begin{array}{c} | \\ \square \\ 0 \\ | \end{array} := 0 \begin{array}{c} | \\ \square \\ f \\ | \end{array}$$

также должно быть невозможно при любом f . Таким образом, если мы хотим включить концепцию невозможного в наш язык, то для любых возможных типов входов и выходов должен существовать *нулевой процесс*, подчиняющийся следующим правилам композиции:

$$\begin{array}{c} | \\ \square \\ 0 \\ | \end{array} \begin{array}{c} | \\ \square \\ f \\ | \end{array} = \begin{array}{c} | \\ \square \\ f \\ | \end{array} \begin{array}{c} | \\ \square \\ 0 \\ | \end{array} = \begin{array}{c} | \\ \square \\ 0 \\ | \end{array} \quad \begin{array}{c} | \\ \square \\ 0 \\ | \end{array} \begin{array}{c} | \\ \square \\ f \\ | \end{array} = \begin{array}{c} | \\ \square \\ 0 \\ | \end{array} \quad (3.27)$$

Упражнение 3.38. Докажите, что если нулевой процесс, удовлетворяющий правилам (3.27), существует, то для любой комбинации типов входов и выходов системы он единственный.

Итак, по аналогии с тем, что умножение на ноль дает ноль, нулевой процесс «поглощает» любую диаграмму, в которой встречается. Иными словами, диаграмма, содержащая нулевой процесс, сама является нулевым процессом. В силу единственности нулевого процесса мы будем записывать его просто как 0, игнорируя входные и выходные провода:

$$\begin{array}{c} | \\ | \\ | \\ \square \\ h \\ | \\ \square \\ 0 \\ | \end{array} \begin{array}{c} | \\ | \\ | \\ \square \\ f \\ | \end{array} = 0 \begin{array}{c} | \\ | \\ | \\ \square \\ g \\ | \end{array}$$

Главное – помнить, что 0 не является пустой диаграммой, поскольку пустую диаграмму можно присоединить к любой другой, не изменяя последней. Нули же просто «сжирают» все, что их окружает!

3.4.3. Процессы, равные «с точностью до числа»

В этой книге немало мест, где числа играют важнейшую роль, и прежде всего это использование правила Борна (3.25) для вычисления вероятностей. Но есть и такие места, где числа только мешают. Например, нас может интересовать только некий качественный аспект процесса, скажем, можно ли его разделить на несвязанные части (см. раздел 4.1.1 в следующей главе), и числа здесь не играют никакой роли. А иногда можно упростить себе жизнь, если игнорировать числа на протяжении вычисления и лишь в самом конце поинтересоваться, какими они должны быть. Поэтому определим понятие, полезное в такого рода ситуациях.

Определение 3.39. Два процесса называются *равными с точностью до числа*:

$$\boxed{f} \approx \boxed{g}$$

если существуют отличные от нуля числа λ и μ такие, что:

$$\lambda \boxed{f} = \mu \boxed{g} \quad (3.28)$$

Мы требуем, чтобы λ и μ были отличны от нуля, потому что иначе любой процесс был бы связан отношением \approx с любым другим:

$$0 \boxed{f} = 0 = 0 \boxed{g}$$

что не слишком полезно. На самом деле нужно, чтобы единственным процессом, который ≈ 0 , был сам нулевой процесс.

Упражнение 3.40. Предположим, что в процессной теории *нет делителей нуля*, т. е. для процесса f и числа λ равенство $\lambda f = 0$ имеет место тогда и только тогда, когда либо $\lambda = 0$, либо $f = 0$. Покажите, что в этом случае:

$$\boxed{f} \approx 0 \implies \boxed{f} = 0$$

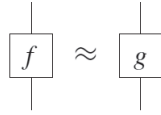
Отношение \approx хорошо тем, что отлично согласуется с диаграммами. Предположим, к примеру, что $h \approx h'$, тогда:

$$\begin{array}{c} \diamond \lambda \\ \mid \\ \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \boxed{h} \end{array} = \begin{array}{c} \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \diamond \lambda \quad \boxed{h} \end{array} = \begin{array}{c} \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \diamond \mu \quad \boxed{h'} \end{array} = \begin{array}{c} \diamond \mu \\ \mid \\ \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \boxed{h'} \end{array}$$

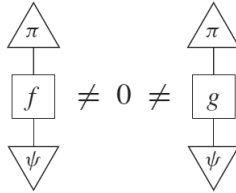
Следовательно, для любой диаграммы, содержащей h , имеем:

$$\begin{array}{c} \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \boxed{h} \end{array} \approx \begin{array}{c} \boxed{g} \\ \mid \quad \mid \\ \boxed{f} \quad \boxed{h'} \end{array}$$

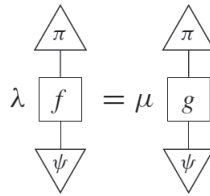
Даже если по ходу вычисления числа игнорируются, мы можем восстановить их в конце. Допустим, установлено, что



Если существует состояние ψ и эффект π такие, что:



то из равенства (3.28) получаем:



где все числа отличны от нуля. Как следствие, если числа в процессной теории не слишком безумные, то мы можем понять, какими должны быть λ и μ , чтобы имело место равенство.

3.4.4. Нотация Дирака

В этой главе мы всячески превозносили достоинства диаграмм, большая часть которых проистекает из возможности записывать процессы в двух измерениях. Современные технологии позволяют без особого труда включать такие диаграммы в печатные тексты, например в учебники. Но так было не всегда. Посмотрим, как далеко мы сможем зайти, если попытаемся заменить диаграммы нотацией, которая была бы приспособлена к старой доброй печатной машинке.

Для начала примем следующие соглашения о состояниях и эффектах:

D1: $\begin{array}{c} | \\ \triangle \psi \end{array}$ записывается в виде $|\psi\rangle$ и называется «кет Дирака»;

D2: $\begin{array}{c} \triangle \pi \\ | \end{array}$ записывается в виде $\langle \pi|$ и называется «бра Дирака».

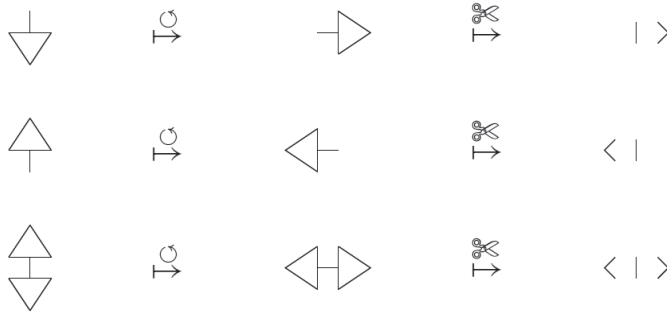
Можно также рассмотреть композицию состояния и эффекта:

D3: $\begin{array}{c} \triangle \pi \\ | \\ \triangle \psi \end{array}$ записывается в виде $\langle \pi|\psi\rangle$ и называется «скобкой Дирака».

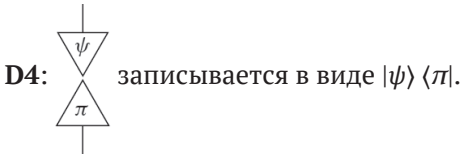
Эти обозначения были введены физиком Полем Дираком специально для описания квантовой теории. И по сей день они широко используются в большинстве книг по квантовой теории.

Замечание 3.41. Мы немного отошли от обычных обозначений Дирака, поскольку пока еще отсутствует уточнение диаграммного языка, необходимое для полноты картины, а точнее для преобразования кет в бра. Этот пробел будет восполнен в разделе 4.3.3, где представлены модифицированные варианты **D2** и **D3**.

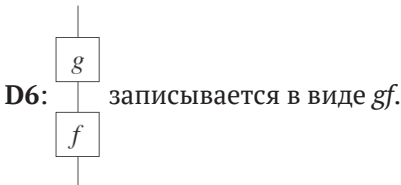
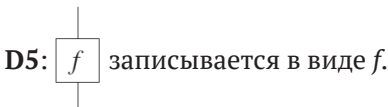
Отметим, что существует простой рецепт перехода от диаграмм состояний и эффектов к нотации Дирака:



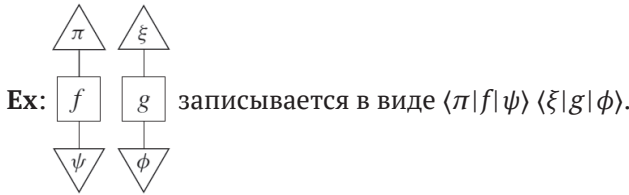
Таким образом, с точностью до вырезания и поворота некоторых элементов нотация Дирака является одномерным подмножеством нашей диаграммной нотации. Памятуя об этом, продолжим попытки разместить наши диаграммы в одной строке:



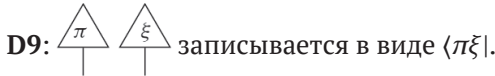
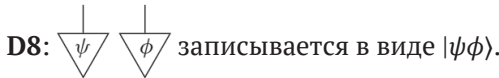
Для процессов, не являющихся ни состояниями, ни эффектами, мы вырезаем блоки целиком и представляем последовательную композицию, записывая процессы справа налево:



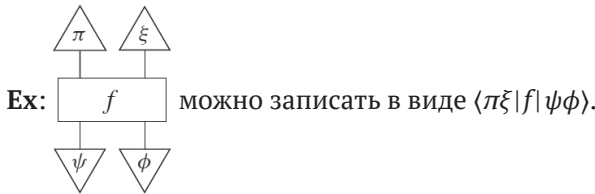
Далее, воспользовавшись тем фактом, что для чисел λ, μ имеет место тождество $\lambda \otimes \mu = \lambda \circ \mu$, мы можем получать выражения вида:



Но, конечно, все становится гораздо хитрее, когда провода и блоки расположены буквально бок о бок, например если мы рассматриваем блоки с двумя входными и (или) выходными проводами. Некоторого прогресса можно достичь, если записывать несколько состояний или эффектов внутри символа кет или бра, чтобы обозначить параллельную композицию:



Таким образом:



Но по мере усложнения диаграмм придется прибегать к явной параллельной композиции с использованием символа \otimes или изобретать еще какие-то трюки, например положить $f_A := f \otimes 1_B, g_B := 1_A \otimes g$, и тогда:

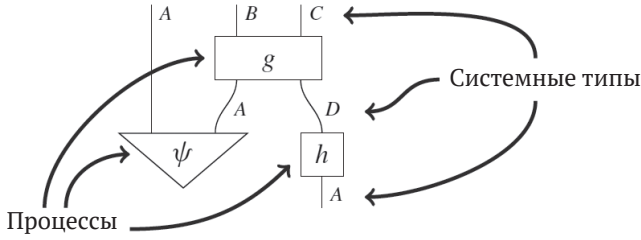


Понятно, что такая запись неоднозначна, если только мы заранее не знаем, что работаем с некоторой системой $A \otimes B$. И довольно скоро нам понадобятся дополнительные равенства, как в разделе 3.2.4.

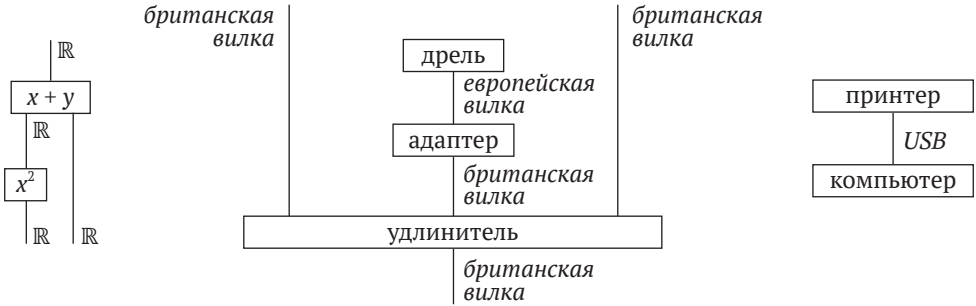
Диаграммы без труда решают все эти проблемы, и, к счастью, очень немногие еще пользуются пишущими машинками. Технологии не стоят на месте, и сейчас без труда можно найти замечательные средства для рисования диаграмм, которые ничуть не сложнее набора формул в обозначениях Дирака на клавиатуре.

3.5. Итоги: что следует запомнить

1. Диаграммы состоят из блоков, помеченных процессами, и проводов, помеченных системными типами:

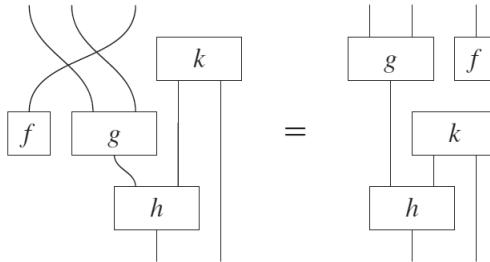


Диаграммы встречаются повсюду:

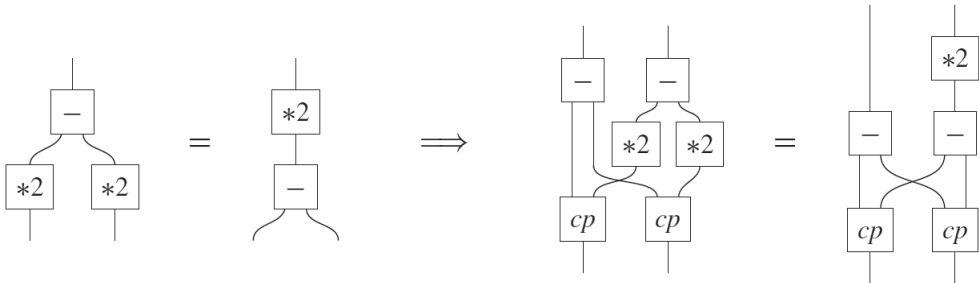


Мы можем получить новые *диаграммные равенства* из старых двумя способами:

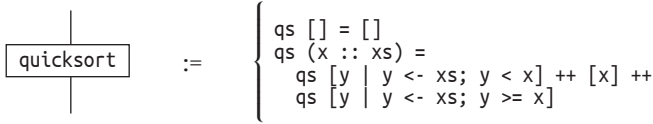
1) деформация диаграмм:



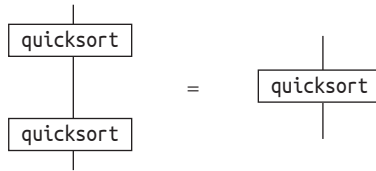
2) подстановка диаграмм:



2. *Процессная теория* – это набор процессов, которые можно соединять между собой. Она говорит, как следует интерпретировать блоки и провода в диаграмме, например:

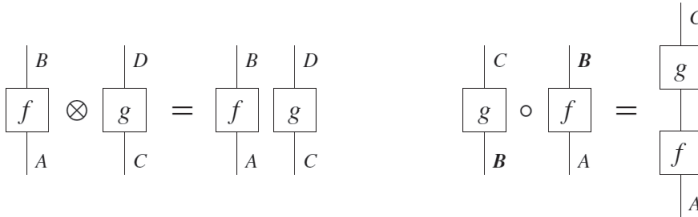


и что означает «соединить процессы проводами». Как следствие, теория говорит, какие диаграммы представляют один и тот же процесс, например:



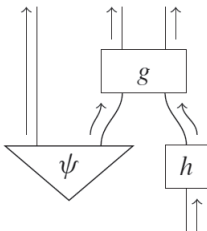
Примерами могут служить процессные теории **функций, отношений, линейных отображений** (определена в главе 5), **классических процессов** (определена в главе 8), **квантовых отображений** (определена в главе 6) и **квантовых процессов** (также определена в главе 8).

- Параллельная композиция '⊗' и последовательная композиция «∘» определяются следующим образом:

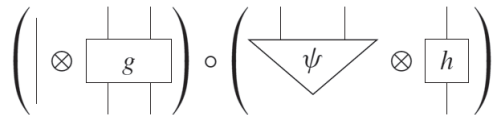


- Важным классом диаграмм являются *схемные диаграммы*. Их можно охарактеризовать двумя эквивалентными способами:

В диаграмме нет ориентированных циклов, т. е. информация течет снизу вверх и не подается на вход более ранним процессам:



Диаграмму можно построить из блоков, включая тождественные процессы и перекмутации, с помощью операций ⊗ и ∘:



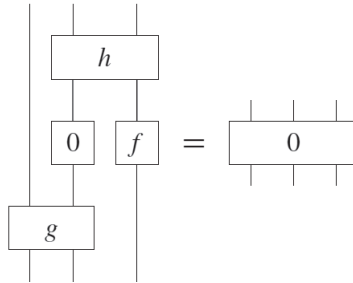
- Для процессов без входов, без выходов или без того и другого имеются специальные названия:



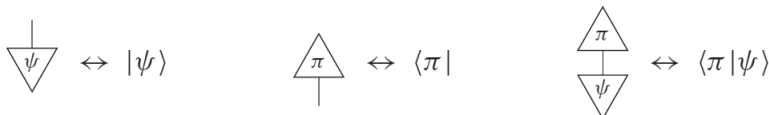
Эти специальные процессы подчиняются обобщенному правилу Борна:



6. Нулевой процесс «пожирает» все:



7. Нотация Дирака – стандартный язык для изображения квантовых процессов. Он является подмножеством диаграммного языка:



3.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

Центральной концепцией в этой книге являются процессные теории, которые говорят, как интерпретировать блоки и провода, изображенные на диаграмме, и как образовывать диаграммы, т. е. что означает соединение блоков проводами. Ниже мы представим два способа определения процессных теорий: *абстрактные тензорные системы* и *симметричные моноидальные категории*. На самом деле мы уже немного познакомились с первым, когда описывали диаграммные формулы в разделе 3.1.3, и со вторым, когда определяли операции параллельной и последовательной композиции в разделе 3.2.

Итак, как можно подойти к построению символического определения процессных теорий? В первых двух частях определения:

- (i) набор T системных типов, представленных проводами;
- (ii) набор P процессов, представленных блоками, такой, что входные и выходные типы каждого процесса берутся из T ...

– диаграммы не играют существенной роли, и мы можем просто опустить часть фразы, начинающуюся словом «представленных», при условии что явно потребу-

ем, чтобы каждый процесс сопровождался списками входных и выходных типов, взятых из T . Нетривиальных усилий требует третья часть определения, касающаяся «образования диаграмм», а именно

(iii) средство «соединения процессов проводами», т. е. операция, которая интерпретирует диаграмму процессов из P как процесс из P .

В частности, мы должны предложить символический аналог «соединения процессов проводами», который не ссылался бы на диаграммы. И более того, символические операции должны порождать процессы данной теории.

3.6.1. Абстрактные тензорные системы*

Мы ввели диаграммные формулы как символический аналог диаграмм. А можно ли определить соответствующее понятие процессной теории? Именно это и сделано в приведенном ниже определении. Чтобы упростить обозначения, мы будем предполагать, что все системные типы одинаковы, и, следовательно, разные имена проводов – это просто различные экземпляры одной и той же системы.

Определение 3.42. Абстрактная тензорная система (АТС) состоит из:

1) множества *тензоров* для всех имен проводов A_1, \dots, A_m и B_1, \dots, B_n :

$$f_{A_1 \dots A_m}^{B_1 \dots B_n} \in \mathcal{T}(\{A_1, \dots, A_m\}, \{B_1, \dots, B_n\}),$$

где A_1, \dots, A_m называются *входами* и B_1, \dots, B_n – *выходами*;

2) *единичного* тензора:

$$1 \in \mathcal{T}(\{\}, \{\})$$

и для всех имен проводов A и B – *тождественных* тензоров:

$$\delta_A^B \in \mathcal{T}(\{A\}, \{B\});$$

3) операции *тензорного произведения*, которая комбинирует тензоры, при условии что их входы и выходы различаются, и записывается с помощью конкатенации:

$$f_{A_1 \dots A_m}^{B_1 \dots B_n} g_{C_1 \dots C_k}^{D_1 \dots D_l} \in \mathcal{T}(\{A_1, \dots, A_m, C_1, \dots, C_k\}, \{B_1, \dots, B_n, D_1, \dots, D_l\});$$

4) операции *свертки тензора* c_A^B , определенной для любых имен проводов A и B , которая записывается либо явно, либо путем повторения имени верхнего (нижнего) провода:

$$f_{A_1 \dots A_m}^{B_1 \dots B_{j-1} A_j B_{j+1} \dots B_n} := c_{A_j}^{B_j} (f_{A_1 \dots A_m}^{B_1 \dots B_n}).$$

Интуитивно она означает, что выход B_j «соединен» с входом A_j ;

5) операций *переиндексирования*, которые изменяют имена проводов:

$$f_{A_1 \dots A_m}^{B_1 \dots B_n} [A_i \mapsto A'_i] = f_{A_1 \dots A_{i-1} A'_i A_{i+1} \dots A_m}^{B_1 \dots B_n}.$$

Эти операции должны удовлетворять следующим условиям.

1. Тензорное произведение ассоциативно, коммутативно и обладает единицей 1:

$$(fg)h = f(gh); \quad fg = gf \quad 1f = f.$$

2. Порядок выполнения операций свертки и произведения тензоров не имеет значения:

$$c_A^B(c_C^D(f)) = c_C^D(c_A^B(f)); \quad c_A^B(f)g = c_A^B(fg).$$

3. Свертка с тождественным тензором только изменяет имена проводов:

$$c_A^B(\delta_C^B(f \dots c \dots)) = f \dots c \dots; \quad c_B^A(\delta_B^C(f \dots A \dots)) = f \dots C \dots.$$

4. Переиндексация учитывает тождественные тензоры, тензорное произведение и свертку.

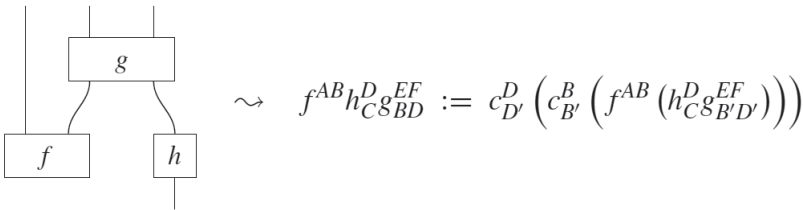
В совокупности операции тензорного произведения и свертки играют роль «соединения процессов проводами». Например, символическим аналогом диаграммы



является такое выражение:

$$c_{B'}^B(f_A^B g_{B'}^C).$$

Вообще, чтобы вычислить тензор, соответствующий некоторой диаграмме, мы можем сначала записать ее в виде диаграммной формулы, а затем представить в терминах тензорного произведения и свертки. Например:



Выражение вида $f^{AB} h_C^D g_{BD}^{EF}$ называется *абстрактной тензорной нотацией*. Как и разложение диаграмм на операции \otimes и \circ , это выражение может быть не единственным. Однако требования в определении 3.42 гарантируют, что любые два таких разложения будут равны.

Как и при разложении диаграмм на операции \otimes и \circ в разделе 3.2, здесь «соединение процессов проводами» разлагается на две подоперации. Эта нотация часто

применяется в математической физике (и особенно в общей теории относительности), где приходится иметь дело с операциями, имеющими много входов и выходов, соединенными так, что использовать для их записи только символы \otimes и \circ было бы слишком громоздко.

Абстрактная тензорная нотация в таких приложениях оказывается лучше, потому что в простом перечислении блоков и их соединений выражена идея о том, что «только соединения имеют значение». Это также объясняет, почему переход к абстрактной тензорной нотации (читай, диаграммным формулам), который мы изучали в разделе 3.1.3, осуществляется так легко.

Упражнение* 3.43. Определите абстрактные тензорные системы для более общего случая, когда имеются различные системные типы.

Упражнение* 3.44. Как бы вы определили процессную теорию **отношений** в виде абстрактной тензорной системы? (Указание: см. «алгоритм» вычисления отношений диаграммы в конце раздела 3.3.3.)

3.6.2. Симметричные моноидальные категории*

Еще один символический способ определения процессных теорий специалисты по теории категорий назвали бы *строгой симметричной моноидальной категорией*. По существу, он сводится к аксиоматизации операций параллельной (\otimes) и последовательной (\circ) композиций из раздела 3.2. Воспринять все сразу за один присест довольно трудно, поэтому давайте временно забудем о «симметричности» и рассмотрим такое определение.

Определение 3.45. *Строгая моноидальная категория (СМК) \mathcal{C} состоит из:*

- 1) набора объектов $\text{ob}(\mathcal{C})$;
- 2) для каждой пары объектов A, B множества морфизмов $\mathcal{C}(A, B)$;
- 3) для каждого объекта A специального тождественного морфизма:

$$1_A \in \mathcal{C}(A, A);$$

- 4) операции последовательной композиции морфизмов:

$$\circ : \mathcal{C}(B, C) \times \mathcal{C}(A, B) \mapsto \mathcal{C}(A, C);$$

- 5) операции параллельной композиции объектов:

$$\otimes : \text{ob}(\mathcal{C}) \times \text{ob}(\mathcal{C}) \mapsto \text{ob}(\mathcal{C});$$

- 6) единичного объекта

$$I \in \text{ob}(\mathcal{C});$$

- 7) операции параллельной композиции морфизмов:

$$\otimes : \mathcal{C}(A, B) \times \mathcal{C}(C, D) \mapsto \mathcal{C}(A \otimes C, B \otimes D),$$

удовлетворяющей следующим условиям:

- а) \otimes для объектов ассоциативна и унитарна:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C), \quad A \otimes I = A = I \otimes A;$$

б) \otimes для морфизмов ассоциативна и унитарна:

$$(f \otimes g) \otimes h = f \otimes (g \otimes h), \quad f \otimes 1_I = f = 1_I \otimes f;$$

в) \circ для морфизмов ассоциативна и унитарна:

$$(h \circ g) \circ f = h \circ (g \circ f), \quad 1_B \circ f = f = f \circ 1_A;$$

г) \otimes и \circ удовлетворяют *перестановочному закону*:

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2).$$

Ого, как много-то всего! Однако если приглядеться, то кое-что начинает казаться знакомым. Прежде всего то, что мы называли типами или системными типами, в теории категорий называется *объектами*. А то, что мы называли процессами, теперь именуется *морфизмами*. Множество $\mathcal{C}(A, B)$ следует представлять себе как множество всех морфизмов с входным типом A и выходным типом B . Обычно мы пишем $f: A \mapsto B$, а не $f \in \mathcal{C}(A, B)$. *Категория* – это набор таких множеств, наделенный операцией последовательной композиции. *Моноидальная категория* – то же самое, только добавляется еще операция параллельной композиции. О том, к чему относится слово «строгая», мы скажем чуть позже. А сначала заметим, что у нас есть почти все необходимое для построения схемных диаграмм – кроме перекоммутаций. Вот тут и вступает в игру *симметричность*.

Определение 3.46. *Строгой симметричной моноидальной категорией* называется строгая моноидальная категория с *коммутационным морфизмом*:

$$\sigma_{A,B} : A \otimes B \mapsto B \otimes A,$$

который определен для всех объектов A, B и удовлетворяет условиям:

$$\begin{aligned} \sigma_{B,A} \circ \sigma_{A,B} &= 1_{A \otimes B}; & \sigma_{A,I} &= 1_A; \\ (f \otimes g) \circ \sigma_{A,B} &= \sigma_{B',A'} \circ (g \otimes f); \\ (1_B \otimes \sigma_{A,C}) \circ (\sigma_{A,B} \otimes 1_C) &= \sigma_{A,B \otimes C}. \end{aligned}$$

Говоря, что моноидальная категория является *строгой*, мы требуем, чтобы операция \otimes была «в точности» ассоциативной и унитарной, т. е. объекты в левой и правой частях должны быть равны, тогда как в нестрогой моноидальной категории требуется только, чтобы они были *изоморфны*.

Определение 3.47. Объект A называется *изоморфным* объекту B :

$$A \cong B,$$

если существует пара морфизмов

$$f : A \mapsto B, \quad f^{-1} : B \mapsto A,$$

такая, что:

$$f^{-1} \circ f = 1_A, \quad f \circ f^{-1} = 1_B.$$

В этом случае морфизм f называется *изоморфизмом*.

Большинство моноидальных категорий, встречающихся на практике, нестрогие, т. е. операция параллельной композиции удовлетворяет только условиям:

$$(A \otimes B) \otimes C \cong A \otimes (B \otimes C), \quad A \otimes I \cong A \cong I \otimes A.$$

В разделе 3.3.1 мы уже мимоходом сталкивались с этой ситуацией. Напомним, что операция \otimes была определена в терминах декартова произведения. Множества $(A \times B) \times C$ и $A \times (B \times C)$ (а также множества A и $A \times \{*\}$) не равны, но между их элементами может быть установлено взаимно однозначное соответствие:

$$((a, b), c) \leftrightarrow (a, (b, c)), \quad a \leftrightarrow (a, *).$$

Чтобы определить нестрогую моноидальную категорию, мы должны включить эти соответствия в определение категории в виде так называемых *структурных изоморфизмов*, а также постулировать (еще!) несколько *условий когерентности*, гарантирующих разумное поведение и возможность композиции.

Однако мы, недолго думая, упустили из виду этот факт, когда определяли процессные теории функций и отношений в разделе 3.3. Почему? В силу следующей *теоремы о когерентности*.

Теорема 3.48. Любая (симметричная) моноидальная категория \mathcal{C} эквивалентна некоторой строгой (симметричной) моноидальной категории \mathcal{C}' .

Для всех практических надобностей эквивалентные категории одинаковы. Мы еще вернемся к этому вопросу в разделе* 5.6.4. Доказательство теоремы 3.48 сводится к явному построению категории \mathcal{C}' с помощью процедуры *стриктификации*. Эта процедура используется неявно, когда мы, например, решаем рассматривать элементы $((a, b), c)$, $(a, (b, c))$ и (a, b, c) как «одинаковые», что и будем делать дальше без дальнейших оговорок.

Далее, наше использование схемных диаграмм для обсуждения симметричных моноидальных категорий оправдано следующей теоремой.

Теорема 3.49. Схемные диаграммы корректны и полны относительно симметричных моноидальных категорий. Иначе говоря, доказать, что два морфизма f и g равны, используя определение симметричной моноидальной категории, можно тогда и только тогда, когда они выражаются одной и той же схемной диаграммой.

Подведем итоги. Многие концепции чистого диаграммного языка и теории категорий можно перевести друг в друга, пользуясь следующим соответствием:

$$\begin{aligned} \text{процессная теория} &\leftrightarrow (\text{строгая}) \text{ симметричная моноидальная категория}; \\ \text{процесс} &\leftrightarrow \text{морфизм}; \\ \text{системный тип} &\leftrightarrow \text{объект}. \end{aligned}$$

3.6.3. Диаграммы общего вида и схемы*

Некоторые читатели, возможно, заметили, что абстрактные тензорные системы и симметричные моноидальные категории – не совсем одно и то же. Симметричные моноидальные категории соответствуют схемам, тогда как абстрактные тензорные системы представляют более общие диаграммы, в которых допускаются ориентированные циклы (см. определение 3.20). Однако мы можем совместить оба понятия.

С одной стороны, можно сделать абстрактные тензорные системы эквивалентными строгим симметричным моноидальным категориям, потребовав только, чтобы операция свертки c_A^B считалась корректной, если она не приводит к образованию ориентированного цикла.

Обратно, можно ввести «петли обратной связи» в симметричные моноидальные категории, получив тем самым *симметричные моноидальные категории со следом*. В таких категориях предполагается наличие дополнительной операции следа:

$$\begin{array}{c} \text{C} \\ | \\ \text{---} \text{f} \text{---} \\ | \\ \text{B} \end{array} \quad \text{with a loop from B to A} \quad := \quad \text{tr}_A \left(\begin{array}{cc} | & | \\ \text{A} & \text{C} \\ | & | \\ \text{---} \text{f} \text{---} \\ | & | \\ \text{A} & \text{B} \end{array} \right)$$

с которой мы встретимся в разделе 4.2.3. Эта операция удовлетворяет ряду аксиом, гарантирующих, что она ведет себя как «петля обратной связи» и согласована с прочей канонической структурой. Тогда строгие симметричные моноидальные категории со следом эквивалентны абстрактным тензорным системам в том смысле, что одну можно преобразовать в другую без потери значимой информации.

Итог всему вышесказанному подведен в следующей таблице:

| | | |
|------------------|--|---|
| Диаграммы | <p>Диаграмма «общего вида»</p> <p>т. е. выход подается на вход</p> | <p>Схемная диаграмма</p> <p>т. е. имеет причинно-следственную структуру</p> |
| АТС | АТС | АТС без циклов |
| СМК | СМК со следом | СМК |

3.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Идея представления композиции математических объектов с помощью узлов и соединений очень стара. В качестве широко известного примера приведем блок-схемы, датируемые (по меньшей мере) 20-ми годами XX века (Gilbreth and Gilbreth, 1922). В физике хорошо известны диаграммы Фейнмана. Несмотря на их название, ныне признано, что впервые они появились в работе Эрнста Штюкельберга, датируемой приблизительно 1941 годом, а только потом были независимо открыты Ричардом Фейнманом примерно в 1947 году. В лекции, прочитанной в ЦЕРНе после присуждения Нобелевской премии, Фейнман упомянул этот факт в тот момент, когда Штюкельберг вышел из зала: «Он сделал всю работу и в оди-

ночестве уходит на закат, а я стою здесь, в лучах славы, которая по праву должна принадлежать ему!» (Mehra, 1994).

Пенроуз (Penrose, 1971) первым ввел в рассмотрение диаграммы того вида, которые мы используем в этой книге в качестве альтернативы абстрактной тензорной нотации (см. раздел * 3.6.1), которую предложил он же. На самом деле он начал использовать диаграммы еще в бытность студентом старших курсов (Penrose, 2004).

Поль Дирак ввел свою систему обозначений в работе Dirac (1939). Связь между нотацией Дирака и использованием треугольников для обозначения состояний и эффектов в струнных диаграммах была замечена в работе Coecke (2005). Идея рассматривать сами диаграммы как базовую структуру, а не категории, недавно завладела умами исследователей, занимающихся основаниями квантовой теории. В частности, она нашла применение в попытках разработать альтернативные формулировки квантовой теории и теории квантовой гравитации (Chiribella et al., 2010; Coecke, 2011; Hardy, 2011, 2013b).

Нежелание многих ученых принять диаграммы в качестве математически строгого языка (мы говорили об этом в разделе 3.1.3) можно в значительной мере связать с духом группы Бурбаки, который превалировал в обучении математике на протяжении большей части прошлого столетия. Коллектив математиков, называвший себя Бурбаки, поставил целью выстроить все здание математики на фундаменте теории множеств (Bourbaki, 1959–2004). Следует отдать должное Джону Баэсу (John Baez), пионеру научного блоггинга, чей выдающийся педагогический талант помог убедить многих в чудодейственной силе диаграмм. Его еженедельная колонка «ThisWeek's Finds in Mathematical Physics» и по сей день является прекрасным источником по диаграммным рассуждениям (Baez, 1993–2010).

Связь между схемными диаграммами и алгебраической структурой (конкретно симметричными моноидальными категориями, см. теорему 3.49) была установлена в работе Joyal and Street (1991), где схемные диаграммы назывались «прогрессивными поляризованными диаграммами». Симметричные моноидальные категории со следом и графическая нотация для них были предложены в работе Joyal et al. (1996); однако близкое понятие «компактной замкнутой категории» (ему соответствуют струнные диаграммы, с которыми мы очень скоро познакомимся) к тому времени уже было известно. Соответствующие ссылки приведены в следующей главе.

Наметки доказательства корректности графического языка в применении к симметричным моноидальным категориям со следом встречаются в различных работах (например, Hasegawa et al., 2008), а полное доказательство было дано в работе Kissinger (2014a). За работой Джойала и Стрита последовали многообразные вариации диаграмм и соответствующих алгебраических структур (см. Selinger, 2011b).

Сами моноидальные категории впервые были введены в работе Benabou (1963). Теорема 3.48 о когерентности дает основу для связывания моноидальных категорий с диаграммами, она была сформулирована и доказана Маклейном (1963). «Танец» на рис. 3.24, известный также под названием «аргумент Экмана–Хилтона», взят из работы Eckmann and Hilton (1962).

Абстрактные тензорные системы и ассоциированная с ними «абстрактная индексная нотация» были введены в работе Penrose (1971) одновременно с соот-

ветствующей диаграммной нотацией, чтобы можно было говорить о различных видах мультилинейных отображений без предварительной корректировки базисов. Эта нотация теперь повсеместно применяется в теоретической физике и особенно в общей теории относительности. Пенроуз написал введение для широкой аудитории в работе Penrose (2004). Эквивалентность абстрактных тензорных систем и симметричных моноидальных категорий со следом установлена в работе Kissing (2014a).

Желающим почитать еще об общей теории категорий стоит начать с книг Abramsky and Tzevelekos (2011) – связь между категориями и логикой, Соеcke and Paquette (2011) – общность понятия симметричной моноидальной категории, а также Baez and Lauda (2011) – роль структур на основе категорий в физике. Для математиков стандартными учебниками являются книги Vorceux (1994a, b) и Mac Lane (1998); для компьютерщиков – Barr and Wells (1990) и Pierce (1991); для специалистов по математической логике – Lambek and Scott (1988) и Awodey (2010). В контексте теории категорий идея о том, что морфизмы представляют процессы, возникла в основном в связи с приложениями к информатике, где программы представляются морфизмами категорий, а типы данных являются объектами. Аналогично в логике доказательства можно представлять морфизмами, а высказывания являются объектами. Эта тройка – морфизмы, программы и доказательства – связана *изоморфизмом Карри–Ховарда–Ламбека* (Lambek and Scott, 1988).

Цитата, приведенная в начале главы, взята из работы Bohm and Peat (1987). Как было отмечено в разделе 1.3, воззрения Бома сыграли ключевую роль в продвижении онтологии процессов в физику.

Глава 4

Струнные диаграммы

Если две системы, о состоянии которых нам известно по их представителям, вступают во временное физическое взаимодействие, обусловленное известными действующими на них силами, и если по прошествии некоторого периода взаимовлияния системы снова разделяются, то их уже нельзя описать так же, как прежде, а именно наделив каждую собственным представителем. Я бы назвал это не одной из, а самой характерной чертой квантовой механики – той, что вынуждает отказаться от классических способов рассуждения.

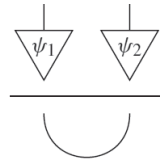
– Эрвин Шрёдингер, 1935

К 1935 году Шрёдингер уже осознал, что самая глубокая пропасть между квантовой теорией и привычными классическими предрассудками заключается в том, что в квантовых системах целое больше суммы частей. Например, в классической физике, чтобы полностью описать состояние двух систем – скажем, двух предметов на столе, – можно поступить следующим образом: сначала полностью описать состояние первой системы, а затем также полностью описать состояние второй системы. Это фундаментальное свойство, которого мы ожидаем от классической *разделимой* Вселенной. Однако, как отмечает Шрёдингер, существуют состояния, предсказанные квантовой теорией (и наблюдаемые в лабораторных условиях!), которые не подчиняются этому «очевидному» закону физического мира. Шрёдингер называл этот новый, совершенно не укладывающийся в классические рамки феномен *Verschränkung*, позже это слово было переведено на преобладающий в науке английский язык *entanglement*, а на русский – *запутанность*.

Квантовый пикторализм как раз и заключается в изучении способов образования целого из частей. Вместе со Шрёдингером – неплохая компания, кстати, – мы полагаем, что рассмотрение роли нескольких взаимодействующих систем (особенно неразделимых систем) должно занимать центральное место в исследованиях по квантовой теории.

В следующем разделе мы увидим, что в терминах диаграмм легко описать, что такое *разделимый* процесс. Это буквально означает, что его можно разделить на не связанные между собой части. С другой стороны, требование обеспечить неразделимость заставляет уточнить наш диаграммный язык. Для этого мы введем

специальные состояния и эффекты – соответственно *чашки* (cup) и *крышки* (cap). На интуитивном уровне их можно представлять себе «согнутыми» проводами. В классическом мире все состояния делимы, а эти состояния и эффекты, очевидно, неразделимы и потому являют собой важнейшую квантовую особенность:

$$\frac{\begin{array}{c} \downarrow \\ \nabla \psi_1 \\ \downarrow \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \psi_2 \\ \downarrow \end{array}}{\text{-----}} = \frac{\text{Разделимы}}{\text{Неразделимы}} = \frac{\text{Классические}}{\text{Квантовые}}. \quad (4.1)$$


Помимо чашек и крышек, мы добавим в диаграммный язык *адьюнкты*, которые будем изображать в виде отражения диаграммы относительно вертикальной оси. Эта операция отражения ассоциирует с каждым состоянием ψ соответствующий эффект, который проверяет, «насколько похоже на ψ » данное состояние. У нее есть прямой аналог в нотации Дирака, а именно отражение кет в бра. Она играет ключевую роль в моделировании таких вещей, как обратимая эволюция состояний (унитарные процессы), квантовые измерения (проекторы и позитивные процессы) и вероятности, связанные с квантовыми измерениями (посредством внутреннего произведения).

Новые диаграммы, получаемые добавлением крышек, чашек и отражения, называются *струнными диаграммами*, и уже совсем скоро мы увидим примеры абсолютно неклассического поведения, вытекающие из использования языка струнных диаграмм.

Например, в разделе 4.4.4 мы встретимся с квантовой телепортацией. А с ней тесно связан тот факт, что чашки и крышки ограничивают возможность вводить фиксированный временной порядок в процессы, скомпонованные в последовательность (см. раздел 4.4.3). Мы также увидим несколько теорем о невозможности для струнных диаграмм. То есть мы покажем, что некоторые свойства, которые ожидаемо выполняются для классических (детерминированных) физических процессов, невозможны в процессной теории, допускающей струнные диаграммы. В частности, *теорема о запрете клонирования* утверждает, что в любой процессной теории, допускающей струнные диаграммы, невозможен *клоняющий процесс*, который принимает на входе произвольное состояние и возвращает две его копии.

Замечание 4.1. В этой главе мы употребляем слово «неразделимый», а не «запутанный». Для класса «чистых» квантовых состояний (см. раздел 6.1) понятия «неразделимый» и «запутанный» на самом деле совпадают. Но для более общих состояний определение квантовой запутанности оказывается более тонкой задачей. Поэтому мы отложим рассмотрение более общего понятия квантовой запутанности до раздела 8.3.5.

4.1. ЧАШКИ, КРЫШКИ И СТРУННЫЕ ДИАГРАММЫ

В этом разделе мы сначала дадим формальное определение *разделимости* и, соответственно, *неразделимости*. Затем мы обоснуем введение струнных диаграмм принципом *двойственности процессов и состояний*, т. е. соответствия между со-

стояниями составных систем и процессами. Этот принцип, который в частном случае квантовой теории известен под названием *изоморфизма Чоя–Жамиolkовского*, фундаментально связан с неразделимостью.

Далее мы опишем два эквивалентных подхода к определению струнных диаграмм. Первый основан на *расширении* языка схемных диаграмм «крышками» и «чашками», используемыми, чтобы определить двойственность между процессами и состояниями. Второй, более простой подход состоит в том, чтобы разрешить проводам соединять процессы в диаграмме произвольными способами, включая соединение входов с входами и выходов с выходами.

4.1.1. Разделимость

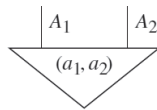
Определение 4.2. *Двухкомпонентным состоянием* ψ называется состояние двух систем. Такое состояние называется \otimes -разделимым, если существуют состояния ψ_1 и ψ_2 такие, что:

$$\begin{array}{c} | \\ | \\ \hline \psi \\ \hline \end{array} = \begin{array}{c} | \\ \hline \psi_1 \\ \hline \end{array} \begin{array}{c} | \\ \hline \psi_2 \\ \hline \end{array} \quad (4.2)$$

Ниже приведен пример процессной теории, в которой все двухкомпонентные состояния \otimes -разделимы.

Предложение 4.3. Все двухкомпонентные состояния в теории **функций** \otimes -разделимы.

Доказательство. В примере 3.35 мы видели, что состояния **функций** полностью определены элементом, на который «указывают». Если для двухкомпонентного состояния это элемент $(a_1, a_2) \in A_1 \times A_2$, то будем обозначать такое состояние



Имеем:

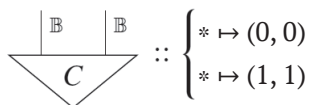
$$\begin{array}{c} | A_1 \quad | A_2 \\ \hline (a_1, a_2) \\ \hline \end{array} = \begin{array}{c} | A_1 \\ \hline a_1 \\ \hline \end{array} \begin{array}{c} | A_2 \\ \hline a_2 \\ \hline \end{array}$$

поскольку оба состояния указывают на один и тот же элемент. □

С другой стороны, существует много (гораздо более интересных!) процессных теорий, которые содержат двухкомпонентные состояния, не являющиеся \otimes -разделимыми.

Предложение 4.4. В теории **отношений** существуют \otimes -неразделимые двухкомпонентные состояния.

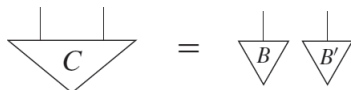
Доказательство. Напомним (см. пример 3.36), что в теории **отношений** состояния представляются подмножествами. Рассмотрим двухкомпонентное состояние:



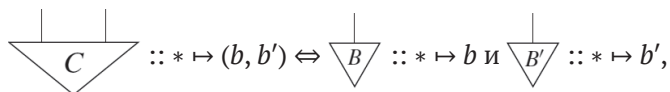
Тогда

$$C = \{(0, 0), (1, 1)\} \subseteq \mathbb{B} \times \mathbb{B}.$$

Предположим, что высказанное утверждение неверно, т. е.



для некоторых $B, B' \subseteq \mathbb{B}$. Тогда в силу (3.22):



то есть

$$(b, b') \in C \Leftrightarrow b \in B \text{ и } b' \in B'.$$

Из того, что $(0, 0) \in C$, следует, что $0 \in B$. Аналогично из $(1, 1) \in C$ следует, что $1 \in B'$. Но из этих двух фактов вытекает, что $(0, 1) \in C$, т. е. мы пришли к противоречию. \square

Доказательство основано на том факте, что множество (содержащее более одного элемента)

$$\{(0, 0), (1, 1)\}$$

нельзя представить в виде декартова произведения подмножеств \mathbb{B} . Если, как в теории **функций**, любое такое множество содержит только один элемент, то это всегда возможно.

К понятию \otimes -разделимости тесно примыкает следующее.

Определение 4.5. Процесс



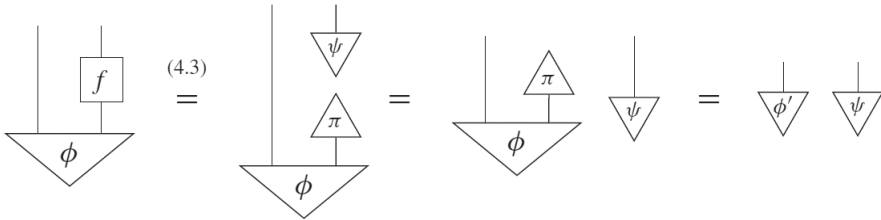
называется \circ -разделимым, если существует эффект π и состояние ψ такие, что:

(4.3)

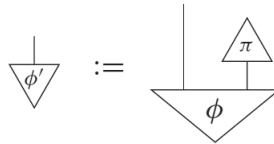
\otimes -разделимость двухкомпонентных состояний и \circ -разделимость процессов – примеры «несвязности» соответствующих диаграмм. Если не возникает двусмысленности, то в обоих случаях мы будем говорить просто «разделимый».

Между обоими понятиями разделимости имеются следующие связи:

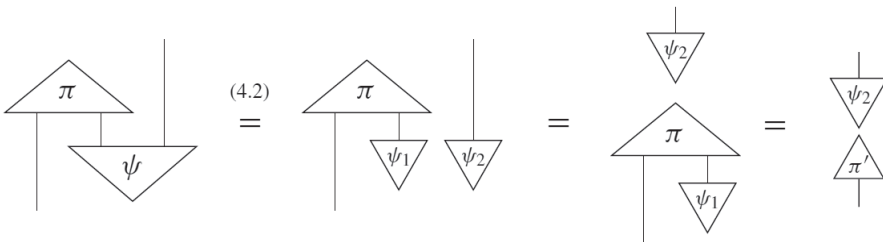
- если процесс f \circ -разделимый, то для любого двухкомпонентного состояния ϕ следующее состояние является \otimes -разделимым:



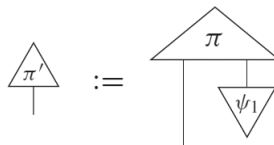
где



- если состояние ψ \otimes -разделимое, то для любого двухкомпонентного эффекта π следующий процесс является \circ -разделимым:



где



Ранее мы уже видели, что для **функций** все двухкомпонентные состояния \otimes -разделимы. А в каких процессных теориях все процессы являются \circ -разделимыми? Ответ: «только в совсем неинтересных!» Применив \circ -разделимый процесс к произвольному состоянию:

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \nabla\psi \end{array} \quad (4.3) \quad = \quad \begin{array}{c} \downarrow \\ \nabla\phi \\ \downarrow \\ \nabla\pi \\ \downarrow \\ \nabla\psi \end{array} \quad = \quad \begin{array}{c} \nabla\pi \\ \downarrow \\ \nabla\psi \end{array} \quad \begin{array}{c} \downarrow \\ \nabla\phi \end{array}$$

мы не сможем получить ничего, кроме фиксированного состояния ϕ (число $\pi \circ \psi$ игнорируем), независимо от того, каким был вход ψ . То есть любой процесс, по существу, является *постоянным*. Иными словами:

не происходит ровным счетом ничего!

Поэтому не должно вызывать удивления, что теория **функций** содержит \circ -неразделимые процессы.

Упражнение 4.6. Покажите, что тождественные процессы (т. е. простые провода) в теории **функций** являются \circ -неразделимыми, и охарактеризуйте \circ -разделимые функции.

Замечание 4.7. Принципиальная тривиальность процессных теорий, в которых все процессы \circ -разделимы, играет важную роль в нескольких теоремах о невозможности, которые мы приведем ниже в этой главе. В частности, мы сможем показать, что некоторое утверждение P неверно, доказав теорему вида:

Если P верно, то все процессы \circ -разделимы.

Поскольку этого никак не может быть для любой разумной процессной теории и в особенности для физической теории, значит, утверждение P ложно.

4.1.2. Двойственность процессов и состояний

Одна из особенностей квантовой теории состоит в том, что процесс можно преобразовать в двухкомпонентное состояние, и наоборот. Само по себе это не очень интересно: мы уже продемонстрировали такое преобразование в предыдущем разделе, чтобы связать \otimes -разделимость двухкомпонентных состояний с \circ -разделимостью процессов. А важно для квантовой теории то, что это можно сделать обратимым способом. То есть можно преобразовать процесс в двухкомпонентное состояние, а затем обратно в процесс таким образом, что получится исходный процесс. Обратное также верно. Иными словами, операции преобразования процессов в двухкомпонентные состояния и двухкомпонентных состояний в процессы являются взаимно обратными. Следовательно, в квантовой теории между процессами и двухкомпонентными состояниями существует взаимно однозначное соответствие.

Как и в предыдущем разделе, мы будем использовать двухкомпонентные состояния и эффекты для взаимного преобразования процессов и состояний. Однако мы будем брать не любую пару состояние–эффект, а зафиксируем специальное состояние и эффект:

$$\begin{array}{c} \text{A} \quad \text{A} \\ | \quad | \\ \text{U} \end{array} \quad \text{и} \quad \begin{array}{c} \cap \\ | \quad | \\ \text{A} \quad \text{A} \end{array} \quad (4.4)$$

для каждой системы A . Будем называть эти состояния и эффекты соответственно *чашками* и *крышками*. Их можно использовать для преобразования процессов в состояния и наоборот посредством следующих операций:

$$\begin{array}{c} \square \\ | \\ f \end{array} \xrightarrow{(*)} \begin{array}{c} \square \\ | \quad | \\ f \\ \text{U} \end{array} \quad \begin{array}{c} \text{U} \\ | \quad | \\ \psi \end{array} \xrightarrow{(\diamond)} \begin{array}{c} \cap \\ | \quad | \\ \text{U} \\ \psi \end{array} \quad (4.5)$$

Теорема 4.8. Операции на рис. (4.5) являются взаимно обратными, т. е. определяют двойственность процессов и состояний тогда и только тогда, когда

$$\begin{array}{c} \cap \\ | \quad | \\ \text{U} \end{array} = (a) \quad \begin{array}{c} \cap \\ | \quad | \\ \text{U} \end{array} = (b) \quad \begin{array}{c} \cap \\ | \quad | \\ \text{U} \end{array} \quad (4.6)$$

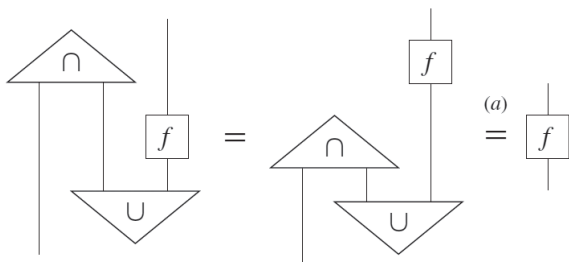
В этом случае существует взаимно однозначное соответствие между множеством всех процессов с входным типом A и выходным типом B и множеством всех двухкомпонентных состояний типа $A \otimes B$:

$$\left\{ \begin{array}{c} B \\ | \\ \square \\ | \\ A \end{array} \right\}_f \cong \left\{ \begin{array}{c} A \quad B \\ | \quad | \\ \psi \end{array} \right\}_\psi$$

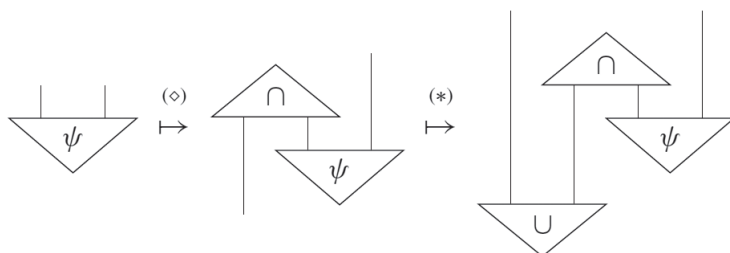
Доказательство. Сначала предположим, что равенства (a) и (b) выполняются. Тогда если сначала преобразовать процесс в состояние и обратно:

$$\begin{array}{c} \square \\ | \\ f \end{array} \xrightarrow{(*)} \begin{array}{c} \square \\ | \quad | \\ f \\ \text{U} \end{array} \xrightarrow{(\diamond)} \begin{array}{c} \cap \\ | \quad | \\ \text{U} \\ \psi \end{array}$$

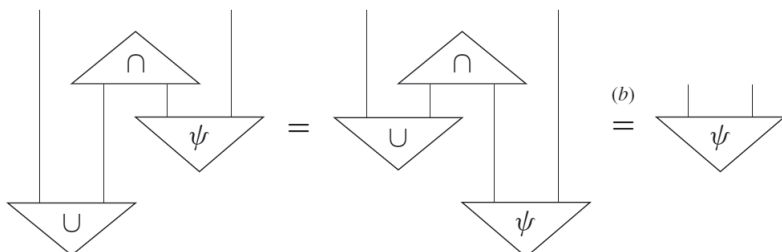
то в силу (a) мы сможем упростить диаграмму и вернуться к исходному процессу:



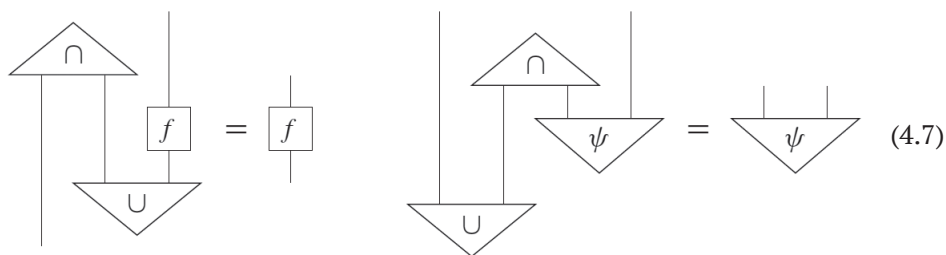
Аналогично, начав с состояния



мы сможем воспользоваться (b):

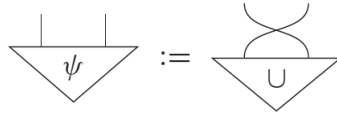


Обратно, если операции в (4.5) взаимно обратны, то



для всех f и ψ . Взяв в качестве f тождественный процесс, мы сразу же получаем (a). Доказательство (b) оставляем читателю в качестве упражнения. \square

Упражнение 4.9. Докажите справедливость равенства (4.6b), воспользовавшись условиями двойственности процессов и состояний (4.7) и положив



Упражнение 4.10. Покажите, что двойственность процессов и состояний не имеет места для **функций**, но имеет место для **отношений**.

Замечание* 4.11. Читатель, знакомый с квантовой теорией, возможно, знает о соответствии между процессами и состояниями, называемом *изоморфизмом Чоя–Жамиолковского*. На самом деле двойственность между процессами является обобщением этого изоморфизма. В главе 6 мы познакомимся с процессной теорией **квантовых отображений**, где обобщенный изоморфизм Ч–Ж окажется знакомым соответствием между двухкомпонентными (возможно, смешанными) квантовыми состояниями и вполне положительными отображениями.

4.1.3. Уравнения разгибания

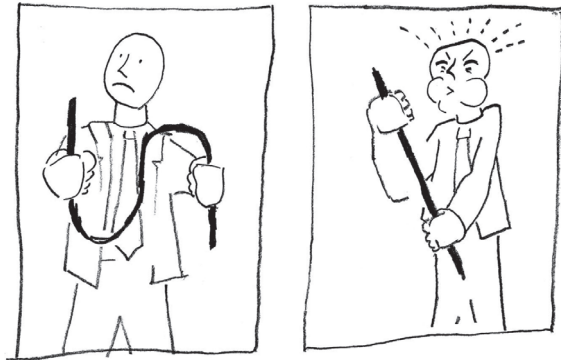
Равенство (4.6) в виде диаграммы интуитивно не слишком понятно, но это можно исправить, немного изменив нотацию. Мы будем записывать специальные состояния и специальные эффекты с помощью U-образных и ∩-образных проводов соответственно:



Тогда равенство (4.6) принимает вид:

$$\text{U-shaped wire} = | = \text{∩-shaped wire} \quad (4.8)$$

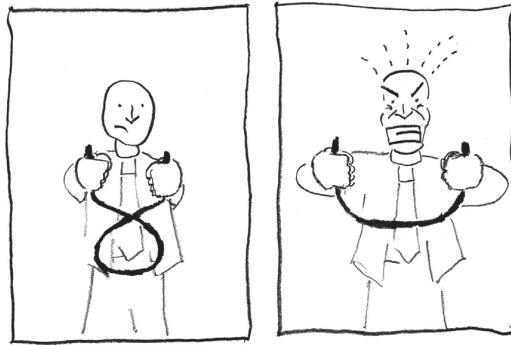
Эта нотация выражает тот факт, что изогнутые в форме U и ∩ провода можно, применив усилие, разогнуть, сделав прямыми:



Если серьезно подойти к этой диаграммной интерпретации, то обнаружатся и другие равенства, которые также должны удовлетворяться для чашек и крышек. Например, должна быть возможность «разогнуть переклесты»:

$$\begin{array}{c} \infty \\ \cup \end{array} = \cup \qquad \begin{array}{c} \circ \\ \cap \end{array} = \cap \qquad (4.9)$$

То же самое можно изобразить более экспрессивно:



Из (4.6) и (4.9) можно вывести уравнение распрямления петель:

$$\begin{array}{c} \infty \\ \cap \end{array} = | \qquad (4.10)$$

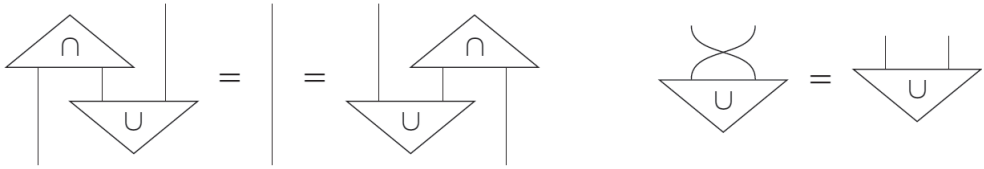
Упражнение 4.12. Выведите из (4.6) и (4.9) равенство (4.10) или эквивалентное ему

Этих равенств достаточно, чтобы «разогнуть» любой спутанный провод. На самом деле присутствует даже некоторая избыточность, как видно из следующего предложения.

Предложение 4.13. Следующие диаграммы эквивалентны:

(i) состояние и эффект, удовлетворяющие условиям:

(ii) состояние и эффект, удовлетворяющие условиям:



Упражнение 4.14. Докажите предложение 4.13.

Далее мы будем называть три равенства

$$\begin{array}{l}
 \text{[Diagram: wavy line] = [Diagram: vertical line]} \\
 \text{[Diagram: figure-eight] = [Diagram: arc]} \\
 \text{[Diagram: figure-eight] = [Diagram: arc]}
 \end{array} \tag{4.11}$$

уравнениями разгибания.

Пример* 4.15. Состояние Белла и эффект Белла в квантовой теории

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)$$

дают типичный пример чашек и крышек.

В предложениях 4.3 и 4.4 мы уже видели, что если в теории **функций** все двух-компонентные состояния \otimes -разделимы, то в теории **отношений** это уже не так, поскольку для любой системы легко можно найти чашки и крышки.

Упражнение 4.16. Докажите, что для любого множества A следующие отношения:

$$\cup :: * \mapsto \{(a, a) \mid a \in A\} \quad \cap :: \forall a \in A : (a, a) \mapsto *$$

удовлетворяют равенствам (4.11).

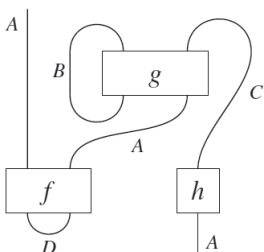
Пример 4.17. Положив $A := \mathbb{B}$, мы снова получим состояние, которое брали в качестве примера неразделимости в доказательстве предложения 4.4:

$$\cup :: * \mapsto \{(0, 0), (1, 1)\}.$$

4.1.4. Струнные диаграммы

Равенства (4.11) уже выглядят очень симпатично, но можно пойти еще дальше. Если в любом системном типе имеются чашки и крышки, удовлетворяющие (4.11), то можно ввести более либеральное понятие диаграммы, в которое они уже встроены.

Определение 4.18. Струнная диаграмма состоит из блоков и проводов, и дополнительно разрешается соединять входы с входами, а выходы с выходами, на-пример:



(4.12)

Выше мы уже отмечали, что можно заменить специальные состояния и специальные эффекты, введенные в предыдущем разделе, крышкообразными и чашеобразными проводами соответственно. Именно так мы получаем струнную диаграмму из схемной, в которой состояния и эффекты удовлетворяют (4.11). Обрато, начав со струнной диаграммы, мы можем заменить провод, соединяющий два входа, специальным состоянием «чашка», а провод, соединяющий два выхода, – специальным эффектом «крышка». Отсюда вытекает следующая теорема.

Теорема 4.19. Следующие два понятия эквивалентны:

- (i) струнные диаграммы;
- (ii) схемные диаграммы, к которым присоединены специальное состояние и специальный эффект для каждого типа и выполняются равенства (4.11).

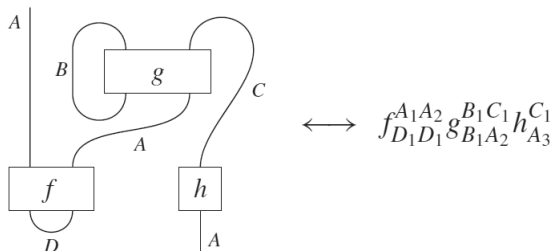
Эквивалентность понимается в том смысле, что диаграммы вида (ii) можно однозначно выразить в виде (i) и наоборот.

Готово! Мы выразили неразделимость в чисто диаграммных терминах и не просто добавили новые блоки в (уже порядком наскучившие) схемные диаграммы, а ввели в рассмотрение другой, более либеральный вид диаграмм. Таким образом, самая важная особенность квантовой теории (согласно Шрёдингеру) встроена прямо в используемые диаграммы!

Упражнение 4.20. Запишите диаграмму (4.12) в нотации \circ и \otimes с применением чашек и крышек.

Струнные диаграммы также допускают представление в виде формул (см. раздел 3.1.3).

Определение 4.21. Струнная диаграммная формула – это то же самое, что диаграммная формула, за исключением того факта, что соответственные пары имен проводов могут состоять не только из верхнего и нижнего имен, но также из двух верхних или двух нижних имен, например:

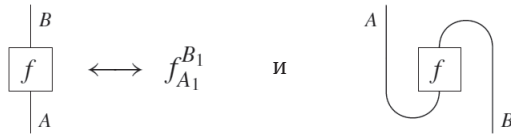


Замечание 4.22. В разделе 3.1.3 мы ввели специальные имена блоков $1_{A_1}^{A_2}$ для представления простых проводов в диаграммных формулах. Если в струнной ди-

аграммной формуле понадобится явно выразить чашки или крышки, то можно использовать два «простых провода», у которых соединены между собой соответственно входы или выходы:

$$\cup^{A_1 A_2} := 1_{A_3}^{A_1} 1_{A_3}^{A_2}, \quad \cap_{A_1 A_2} := 1_{A_1}^{A_3} 1_{A_2}^{A_3}.$$

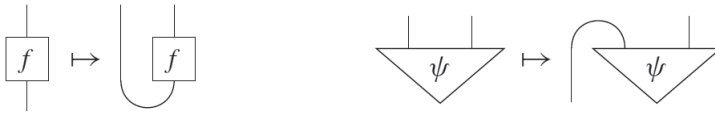
Это позволяет, например, различить следующие диаграммы:



Теперь перейдем к исследованию возможностей этих диаграмм.

4.2. ТРАНСПОНИРОВАНИЕ И СЛЕД

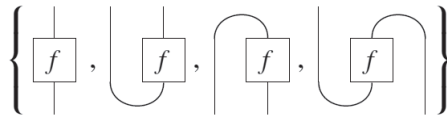
Что такое транспонирование и след, вы, наверное, знаете из курса линейной алгебры. Удивительно, что они возникают на самом общем уровне струнных диаграмм. Из предыдущего раздела мы знаем, что чашки и крышки позволяют создавать новые процессы из старых, преобразуя входы в выходы и наоборот. В случае двойственности между процессами и состояниями имеем:



Вообще, мы всегда можем превратить входы в выходы и наоборот:



Для процессных теорий, допускающих струнные диаграммы, эта возможность замены входов на выходы означает, что роль входов и выходов не столь велика, как в других процессных теориях, которые допускают только схемы. В частности, любой процесс с одним входом и одним выходом имеет (по меньшей мере) следующие четыре взаимозаменяемых представления:



а если входов и выходов несколько, то представлений будет гораздо больше. Мы можем также получать новые процессы, соединяя между собой входы и выходы с помощью чашек и крышек:

Замечание* 4.26. Тот простой факт, что операцию транспонирования в линейной алгебре можно записать с помощью чашки и крышки, как в разложении (4.14), на удивление малоизвестен даже специалистам.

Упражнение 4.27. Докажите, что в теории **отношений** результат транспонирования отношения R совпадает с обратным отношением, т. е.



Состояние



не имеет входов, поэтому мы должны только преобразовать выход во вход:

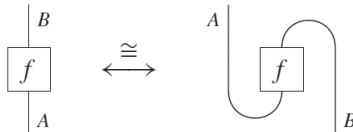


Следовательно, не является случайным совпадением, что в теории **отношений** для любого системного типа A состояний столько же, сколько эффектов (см. упражнение 3.36), поскольку имеет место взаимно однозначное соответствие между состояниями и эффектами:



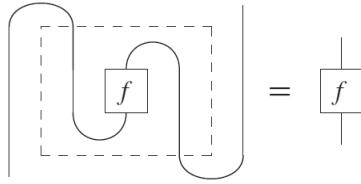
Это общее явление.

Предложение 4.28. Для любой процессной теории, допускающей струнные диаграммы, существует взаимно однозначное соответствие между состояниями и эффектами одного и того же типа. Вообще, соответствие



определяет биективное отображение множества процессов с фиксированными типами входов и выходов на множество процессов с противоположными типами входов и выходов.

Повторное транспонирование дает исходный процесс:



Или в символическом виде:

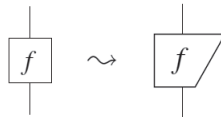
$$(f^T)^T = f.$$

Операция, которая «отменяет себя», как показано выше, называется *инволюцией*.

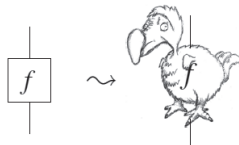
Пример 4.29. Результатом транспонирования чашки является крышка, и наоборот:



Вот мы и подошли к действительно интересной части. Определение транспонирования можно встроить в нашу диаграммную нотацию. Сначала немного деформируем блоки:



Характер деформации не играет роли, важно лишь нарушить симметрию. Деформация



ничем не хуже, но Дэйву может не понравиться, когда его переворачивают. Теперь выразим результат транспонирования f в виде блока, помеченного тоже f , но повернутого на 180° :

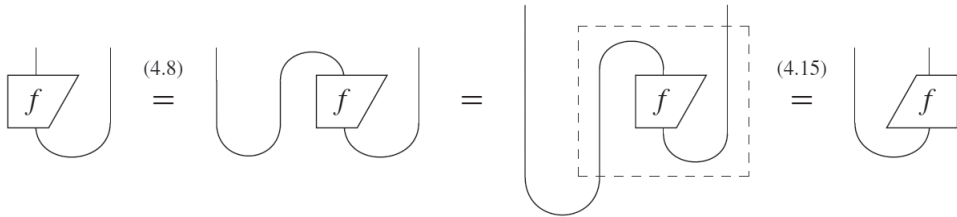
$$\begin{array}{c} \diagup \\ f \\ \diagdown \end{array} := \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \quad (4.15)$$

Эта нотация хорошо согласуется с тем фактом, что транспонирование – инволюция, поскольку если повернуть на 180° дважды, то получится исходный блок. Но истинные достоинства такого выбора обозначений проявляются при взаимодействии транспонирования с чашками и крышками.

Предложение 4.30. Для любого процесса f имеем:

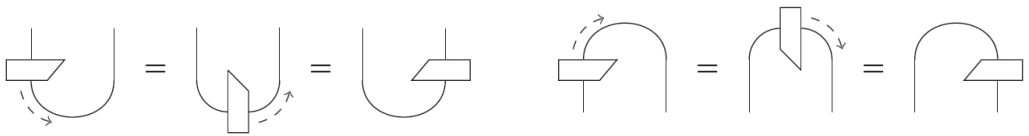


Доказательство. Первое равенство устанавливается следующим образом:

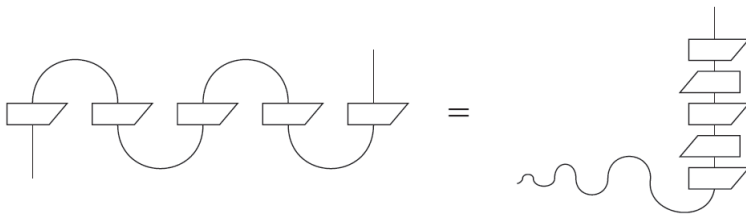


Второе доказывается аналогично. □

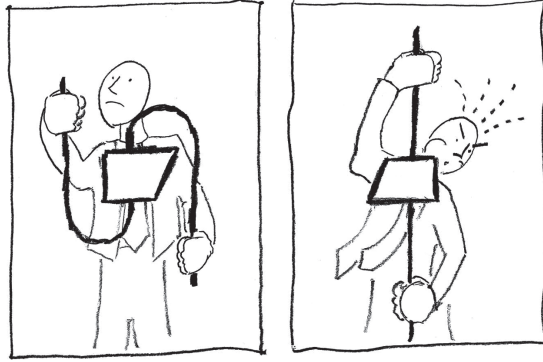
Благодаря удачному выбору обозначения транспонирования мы как бы можем двигать блоки вдоль U-образных и \cap -образных проводов:



Стало быть, блоки можно перемещать по проводам, как бусинки на ожерелье. Например, справедливо показанное ниже равенство:



Запомнить это очень легко. Просто представьте, что произошло бы, если бы мы взяли определение транспонирования (4.15) и разогнули провода:



Тот же прием применим к состояниям и эффектам. Чтобы было понятно, что они повернуты, мыотрежем уголок:

$$\begin{array}{c} \downarrow \\ \psi \end{array} \sim \begin{array}{c} \downarrow \\ \psi \end{array} \quad \text{и положим} \quad \begin{array}{c} \uparrow \\ \psi \end{array} := \begin{array}{c} \curvearrowright \\ \psi \end{array} \quad (4.16)$$

В данный момент неочевидно, для чего это нужно, поскольку и так понятно, что треугольник перевернут. Однако скоро (в разделе 4.3) это окажется очень важным, поэтому будем потихоньку привыкать.

У транспонирования есть и операционная интерпретация. Будем интерпретировать две системы в первом равенстве из предложения 4.30 как отстоящие далеко друг от друга в пространстве, и пусть каждой управляет некий агент, например Алекс и Боб. Тогда имеем:



$$\begin{array}{|c|c|} \hline \text{Алекс} & \text{Боб} \\ \hline \begin{array}{c} \downarrow \\ f \end{array} & \downarrow \\ \hline \end{array} = \begin{array}{|c|c|} \hline \text{Алекс} & \text{Боб} \\ \hline \downarrow & \begin{array}{c} \uparrow \\ f \end{array} \\ \hline \end{array} \quad (4.17)$$

Это равенство означает следующее: если две такие системы находятся в состоянии «чашка» и Алекс применит f к своей системе, то результат будет таким же, как если бы Боб применил транспонированный f к своей системе.

Теперь рассмотрим (4.17) в частном случае состояний и эффектов:

$$\begin{array}{|c|c|} \hline \text{Алекс} & \text{Боб} \\ \hline \begin{array}{c} \uparrow \\ \psi \end{array} & \downarrow \\ \hline \end{array} = \begin{array}{|c|c|} \hline \text{Алекс} & \text{Боб} \\ \hline & \begin{array}{c} \downarrow \\ \psi \end{array} \\ \hline \end{array}$$

Учитывая, что существует взаимно однозначное соответствие между

- состояниями Боба  и
- эффектами Алекса ,

Алекс и Боб располагают парой *идеально коррелированных* систем. Что это значит? Вспомним, что эффект можно интерпретировать как успешное испытание. При такой интерпретации имеет место следующее свойство: для каждого состояния системы Боба существует единственное испытание системы Алекса такое, что:

коль скоро Алекс получает , система Боба находится в состоянии .

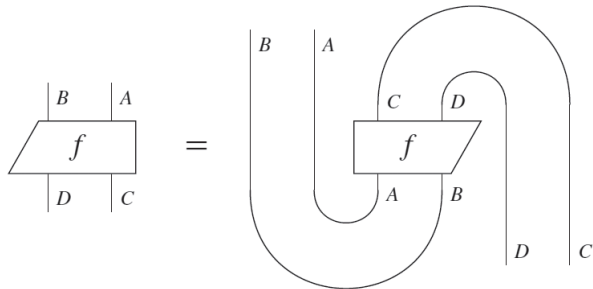
Процесс, равный транспонированному к себе, называется *самотранспонированным*.

Пример 4.31. Числа всегда являются самотранспонированными. По определению, транспонирование изгибает все входные провода вверх, а все выходные провода вниз. Поскольку у числа нет проводов, то и делать ничего не надо:

$$(\diamond \lambda)^T = \diamond \lambda \tag{4.18}$$

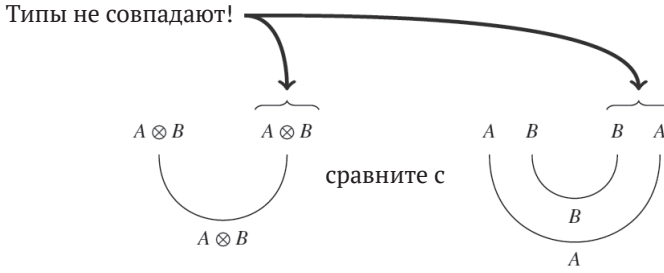
4.2.2. Транспонирование составных систем

При работе с совместными системными типами следует быть аккуратнее. С одной стороны, чтобы сохранить совместимость с обозначением транспонирования как «поворота на 180°», следует определить операцию транспонирования следующим образом:



$$\tag{4.19}$$

Получается, что для определения чашек и крышек для $A \otimes B$ необходимы вложенные чашки и крышки. Однако при таком определении $\cup_{A \otimes B}$ и $\cap_{A \otimes B}$ возникает проблема.



Замечание* 4.32. Это несовпадение типов исчезает, если для каждого типа A определить *двойственный тип* A^* , но тогда мы получаем два разных типа для двух систем, участвующих в определении чашек и крышек, хотя на самом деле эти типы зачастую совпадают. В разделе* 4.6.2 мы покажем, как можно разработать теорию струнных диаграмм с двойственными типами.

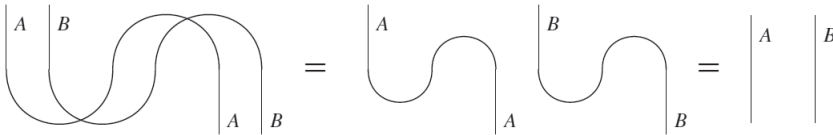
Избежать несовпадения типов можно, если определить чашки и крышки для $A \otimes B$ немного по-другому – как «перекрещенные»:

$$A \otimes B \quad \text{cup} \quad := \quad A \quad B \quad \text{cup} \quad A \quad B \quad (4.20)$$

$$A \otimes B \quad \text{cap} \quad := \quad A \quad B \quad \text{cap} \quad A \quad B \quad (4.21)$$

Предложение 4.33. Определения чашки и крышки (4.20) и (4.21) удовлетворяют уравнениям разгибания (4.11).

Доказательство. Для первого уравнения разгибания имеем:



Остальные два доказываются аналогично. □

С такими «перекрещенными» чашками и крышками мы получаем альтернативное понятие транспонирования, подразумевающее перекрещивание для составных систем:

$$\begin{array}{c} A \otimes B \\ \hline f \\ \hline C \otimes D \end{array} = \begin{array}{c} A \quad B \\ \text{cup} \\ C \quad D \\ \hline f \\ \hline A \quad B \\ \text{cap} \\ C \quad D \end{array} = \begin{array}{c} A \quad B \\ \text{cup} \\ C \quad D \\ \hline f \\ \hline C \quad D \\ \text{cap} \\ A \quad B \end{array} \quad (4.22)$$

Это перекрещивание и восстанавливает совпадение типов, а поскольку мы определяем чашки и крышки для $A \otimes B$ в терминах чашек и крышек для A и B по отдельности, то не возникает неоднозначности в случае применения такого транспонирования к процессам, в которых участвуют составные системы. Но попутно мы потеряли элегантную нотацию «поворота на 180° ».

На самом деле полезны могут быть оба варианта транспонирования. Мы примем первый вариант (4.19) по умолчанию и будем называть его просто «транспонированием». А второй вариант, с перекрещенными чашками и крышками, будем называть *алгебраическим транспонированием*, поскольку именно он используется в линейной алгебре (см. раздел 5.2.2). Транспонирование по-прежнему обозначается поворотом на 180° , а для алгебраического транспонирования будем применять символическую нотацию $(\)^T$. Равенство

$$\left(\begin{array}{c|c} C & D \\ \hline f \\ \hline A & B \end{array} \right)^T = \begin{array}{c} \begin{array}{c} \text{A} \quad \text{B} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \begin{array}{c} \text{C} \quad \text{D} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \end{array}$$

связывает транспонирование с алгебраическим транспонированием. Разумеется, если блок имеет не более одного входного и выходного проводов, оба варианта совпадают. Неудивительно, что процесс, который совпадает с результатом своего алгебраического транспонирования, называется *алгебраически самотранспонированным*.

4.2.3. След и частичный след

Струнные диаграммы дают простой способ сопоставлять процессам числа.

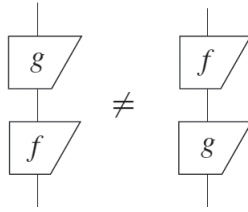
Определение 4.34. Для процесса f с одинаковыми типами входа и выхода *следом* называется

$$\text{tr} \left(\begin{array}{c|c} A \\ \hline f \\ \hline A \end{array} \right) := \begin{array}{c} \text{A} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \quad (4.23)$$

а для процесса g , для которого тип одного из входов совпадает с типом одного из выходов, *частичным следом* называется

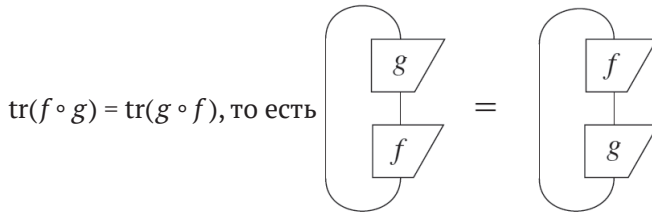
$$\text{tr}_A \left(\begin{array}{c|c} A & C \\ \hline g \\ \hline A & B \end{array} \right) := \begin{array}{c} \text{A} \\ \text{---} \\ \text{---} \\ \text{---} \end{array}$$

След обладает любопытным свойством: хотя в общем случае



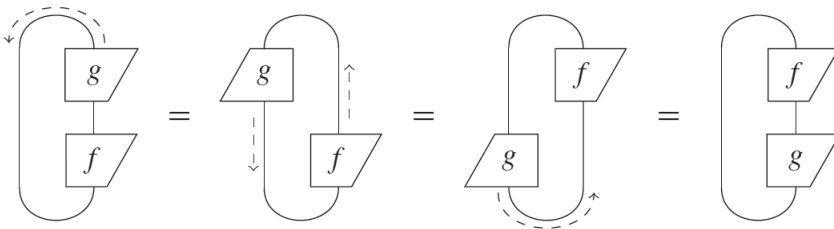
следы левой и правой частей равны.

Предложение 4.35 (цикличность следа). Имеет место тождество:

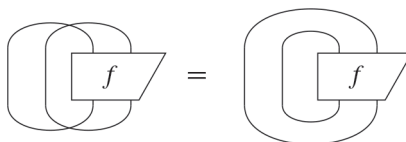


Доказательство. Это следует из того факта, что обе диаграммы равны, т. е. левую часть можно деформировать в правую, не изменяя способа соединения блоков. □

Можно дать и другое, пошаговое доказательство предложения 4.35, воспользовавшись предложением 4.30. Это альтернативное доказательство необязательно, но оно интересно тем, что слово «цикличность» понимается в нем буквально – мы видим чертовое колесо блоков:



Замечание 4.36. В предыдущем разделе мы решили различать транспонирование (в котором участвуют вложенные чашки и крышки) и алгебраическое транспонирование (в котором чашки и крышки перекрещены). Поскольку в равенство (4.23) тоже входят чашки и крышки, возникает вопрос, нужно ли проводить аналогичное различие между «вложенным» и «перекрещенным» следом для составных систем. К счастью, не нужно:



Упражнение 4.37. Покажите, что существует только один след, т. е. любая пара чашка–крышка, удовлетворяющая уравнениям разгибания (4.11), определяет один и тот же след (4.23).

4.3. ОТРАЖЕНИЕ ДИАГРАММ

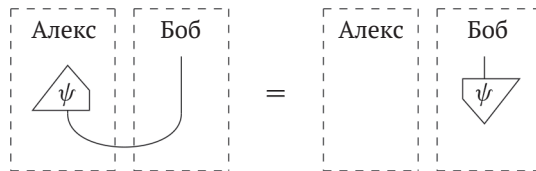
Наличие под рукой струнных диаграмм – уже большой шаг в направлении квантового мира, поскольку гарантирует существование неразделимых состояний. К тому же они приводят к математическим понятиям, играющим центральную роль в квантовой теории: транспонированию и следу.

Теперь мы рассмотрим еще одну возможность, благодаря которой струнные диаграммы становятся гораздо выразительнее: *вертикальное отражение*. Оно позволяет определить такие вещи, как *адьюнкция* (adjoint), *сопряжение* (conjugate), *внутреннее произведение*, *унитарность* и *положительность* – все они играют важную роль в изложении квантовой теории.

Более того, вертикальное отражение – не просто дополнительная степень свободы, существующая у струнных диаграмм, но у нее есть четкая операционная семантика в терминах пригодности состояний к испытаниям. И эта семантика влечет за собой ряд условий, имеющих весьма важное значение для квантовой теории. Все они перечислены в стандартных учебниках, но обычно излагаются формально, без концептуального обоснования.

4.3.1. Адьюнкция

В предыдущем разделе мы показали, что графически транспонирование сводится к повороту блоков на 180° и что с операционной точки зрения оно отражает прямолинейную корреляцию между эффектами Алекса на одной стороне чашки и состояниями Боба на другой стороне:



Но что сказать о связи между эффектами и состояниями Алекса?

Напомним (см. раздел 3.4.1), что эффекты можно интерпретировать как испытание на наличие некоторого свойства у состояния. Обычно мы хотим проверить, находится ли система в определенном состоянии. Поэтому нам необходимы средства, позволяющие соотнести состояние ψ с эффектом, который испытывает систему на нахождение в ψ . Струнные диаграммы ничего не говорят о том, как это сделать, поэтому мы расширим наш язык, представив эффект, проверяющий состояние ψ , его вертикальным отражением:

$$\begin{array}{c} \downarrow \\ \triangle \\ \psi \end{array} \mapsto \begin{array}{c} \triangle \\ \psi \\ \downarrow \end{array} \quad (4.24)$$

Вместо «эффект, проверяющий нахождение в состоянии ψ » мы будем говорить просто *адьюнкт* ψ .

Эта операция отражения естественно обобщается на все процессы. Если f преобразует состояние ψ в состояние ϕ :

$$\begin{array}{c} | \\ \square f \triangle \\ | \\ \triangle \psi \\ | \end{array} = \begin{array}{c} | \\ \triangle \phi \\ | \end{array} \quad (4.25)$$

то адьюнктом f является процесс, преобразующий адьюнкт ψ в адьюнкт ϕ :

$$\begin{array}{c} \triangle \psi \\ | \\ \square f \triangle \\ | \end{array} = \begin{array}{c} \triangle \phi \\ | \end{array} \quad (4.26)$$

Заметим, что, как и в случае состояний, адьюнкт произвольного процесса изображается в виде его вертикального отражения:

$$\begin{array}{c} | B \\ \square f \triangle \\ | A \end{array} \xrightarrow{\dagger} \begin{array}{c} | A \\ \square f \triangle \\ | B \end{array}$$

Таким образом, равенство (4.26) – это просто равенство (4.25), перевернутое вверх ногами. Мы будем употреблять символ \dagger для операции, которая переводит f в его адьюнкт f^\dagger . Отметим частный случай – адьюнкт эффекта (4.24) совпадает с ψ :

$$\begin{array}{c} \triangle \psi \\ | \end{array} \xrightarrow{\dagger} \begin{array}{c} | \\ \triangle \psi \end{array}$$

Как и транспонирование, операция адьюнкции определяет биективное отображение состояний и эффектов и, более общо, устанавливает взаимно однозначное соответствие между процессами, отображающими тип A в тип B , и процессами, отображающими тип B в тип A . Кроме того, она, как и транспонирование, является инволюцией, что видно из диаграммной нотации:

$$\begin{array}{c} | \\ \square f \triangle \\ | \end{array} \xrightarrow{\dagger} \begin{array}{c} | \\ \triangle f \\ | \end{array} \xrightarrow{\dagger} \begin{array}{c} | \\ \square f \triangle \\ | \end{array} \quad (4.27)$$

При переходе от (4.25) к (4.26) мы видели только один пример, где адьюнкция процесса выливалась в отражение всей его диаграммы. На самом деле это справедливо для всех диаграмм, например:

(4.28)

Иначе можно сказать (в силу теоремы 4.19), что адьюнкция сохраняет параллельную композицию и тождественность:

(4.29)

обращает последовательную композицию и переводит чашки в крышки:

(4.30)

а также изменяет направление перекоммутации на противоположное:

(4.31)

Упражнение 4.38. Воспользовавшись упражнением 3.38, докажите, что

$$0^\dagger = 0.$$

Итак, мы теперь знаем, что адьюнкты представляются на диаграммах с помощью вертикального отражения. Однако мы ничего не сказали о том, как следует вычислять адьюнкт процесса. Ответ зависит от теории. Поскольку процессная теория дает интерпретацию всех диаграмм (см. раздел 3.1.2), она должна давать и интерпретацию вертикального отражения диаграммы. При этом возникает два вопроса:

- 1) всегда ли существует такая интерпретация?
- 2) возможно ли более одной такой интерпретации?

На первый вопрос ответ утвердительный, поскольку мы всегда можем интерпретировать вертикальное отражение как алгебраическое транспонирование.

Упражнение 4.39. Проверьте, что алгебраическое транспонирование дает одну из возможных интерпретаций адьюнктов. Иными словами, покажите, что оно удовлетворяет равенствам (4.27) и (4.28). Объясните, почему мы выбрали алгебраическое, а не обычное транспонирование.

В определенном смысле алгебраическое транспонирование – это тривиальная интерпретация вертикального отражения, поскольку она ничего не добав-

ляет к тому, чем уже располагают струнные диаграммы без адьюнктов. Конечно, если бы никакой другой интерпретации не было, то не стоило бы вообще вводить адьюнкты в рассмотрение. В следующей главе мы встретим очень важный нетривиальный пример адьюнктов, который нельзя заменить транспонированием. Поэтому ответ на второй вопрос тоже утвердительный: существует несколько (тривиальных и нетривиальных) способов интерпретации адьюнктов. Но если так, то возникает следующий вопрос:

3) какие интерпретации адьюнктов считать хорошими?

Любая интерпретация адьюнктов в процессной теории должна быть инволюцией и отражать диаграммы в смысле равенства (4.28). Однако чтобы считаться «хорошим», адьюнкт должен быть согласован с идеей о том, что он переводит состояние в эффект, проверяющий нахождение в этом состоянии. Отсюда вытекает несколько следствий, которые мы сейчас и обсудим.

При проверке состояния ψ на ϕ есть два крайних случая:

$$\begin{array}{c} \phi \\ \downarrow \\ \psi \end{array} = 0 \quad \text{и} \quad \begin{array}{c} \phi \\ \downarrow \\ \psi \end{array} = \square$$

или эквивалентно:

$$\begin{array}{c} \phi \\ \uparrow \\ \psi \end{array} = 0 \quad \text{и} \quad \begin{array}{c} \phi \\ \uparrow \\ \psi \end{array} = 1$$

поскольку «1» – это просто символическое обозначение пустой диаграммы. В первом случае мы говорим, что невозможно получить результат «да» при проверке ψ на ϕ . Для процессных теорий, рассматриваемых в этой книге, второе равенство имеет две интерпретации: результат «да» либо «возможен» (в случае теории **отношений**), либо «достоверен» (для большинства прочих теорий).

В свете интерпретации первого равенства мы ожидаем, что:

$$\begin{array}{c} \psi \\ \downarrow \\ \psi \end{array} \neq 0$$

Это означает, что невозможно получить ответ «да» при проверке состояния ψ на самого себя. Однако мы упустили из виду одну вещь: само ψ может быть равно 0, т. е. это «невозможное состояние». В разделе 3.4.2 мы видели, что 0 поглощает все, и, в частности, композиция 0 с 0 всегда будет равна... точно, 0. Поэтому показанное выше условие следует сформулировать аккуратнее:

$$\begin{array}{c} \psi \\ \downarrow \\ \psi \end{array} = 0 \iff \begin{array}{c} | \\ \downarrow \\ \psi \end{array} = 0 \tag{4.32}$$

Иными словами: если невозможно получить ответ «да» при проверке ψ на самого себя, то ψ изначально должно быть невозможным состоянием.

Далее рассмотрим другое равенство: когда проверка ψ на ϕ дает 1. Если интерпретировать 1 как «возможно», то это будет означать, что ψ и ϕ нельзя уверенно различить с помощью испытаний, но сверх того мы ничего не получаем. В частности, невозможно сказать, равны ли они (см. пример 4.40).

Если же 1 означает «достоверно», то можно высказать гораздо более сильное утверждение:

$$\begin{array}{c} \phi \\ \hline \psi \end{array} = 1 \iff \begin{array}{c} \downarrow \\ \psi \end{array} = \begin{array}{c} \downarrow \\ \phi \end{array} \quad (4.33)$$

То есть мы уверенно заключаем, что « ψ совпадает с ϕ ».

Пример 4.40. В примере 3.36 мы установили, что в процессной теории **отношений** состояния для множества A соответствуют подмножествам $B \subseteq A$. Мы рассматриваем их как недетерминированные состояния, состоящие из множества возможных «фактических» состояний $b \in B$. Эффектам для A также соответствуют подмножества, которые мы рассматриваем как испытания на предмет совпадения фактического состояния системы с одним из элементов B . Если проверка B на B' дает 0, значит, ни один из элементов $b \in B$ не принадлежит B' . То есть

$$\begin{array}{c} B' \\ \hline B \end{array} = 0 \iff B \cap B' = \emptyset \quad (4.34)$$

На самом деле существует только один эффект B' , который переводит состояние B в 0 тогда и только тогда, когда пересечение $B \cap B'$ пусто. Это *реляционное обращение* B' :

$$\begin{array}{c} \downarrow \\ B' \end{array} :: * \mapsto a \iff \begin{array}{c} B' \\ \hline \downarrow \end{array} :: a \mapsto *$$

В силу эквиваленции (4.25) \Leftrightarrow (4.26) это обобщается на любое отношение:

$$\begin{array}{c} \downarrow \\ R \end{array} :: a \mapsto b \iff \begin{array}{c} R \\ \hline \downarrow \end{array} :: b \mapsto a \quad (4.35)$$

Следовательно, адьюнкт отношения совпадает с алгебраическим транспонированием (см. упражнение 4.27).

Равенство (4.34) возникло как пример (4.32), поэтому первое равенство «доброкачественности» однозначно определяет адьюнкты в теории **отношений** как реляционное обращение. Но удовлетворяет ли такое определение равенству (4.33)? И следует ли этого ожидать? Поскольку число 1 в теории **отношений** означает

«возможно», а не «достоверно», ответ отрицательный. На самом деле существует много неравных состояний, для которых:

$$\begin{array}{c} \triangleup \\ B' \\ \downarrow \\ \triangleleft \\ B \end{array} = 1 \tag{4.36}$$

поскольку это просто означает, что $B \cap B' \neq \emptyset$. Однако в теории **отношений** существует одна ситуация, когда число 1 все-таки означает достоверность: при сравнении «фактических» (т. е. детерминированных) состояний. То есть для $b, b' \in A$:

$$\begin{array}{c} \triangleup \\ b' \\ \downarrow \\ \triangleleft \\ b \end{array} = 1 \iff b = b' \tag{4.37}$$

Ниже приведен основной пример адьюнктов, который будет играть важную роль на протяжении всей книги и принципиально отличается от транспонирования. Мы поместили этот пример звездочкой, поскольку он, вероятно, уже знаком некоторым читателям. Если вы не из их числа, то не расстраивайтесь – в следующей главе мы опишем его как должно.

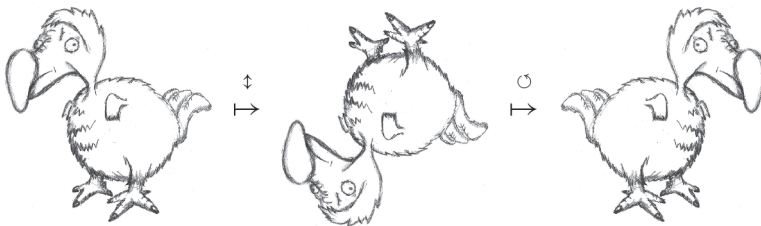
Пример* 4.41. В процессной теории **линейных отображений** адьюнкция соответствует операции *линейно-алгебраического сопряжения*, которая каждому линейному отображению f сопоставляет единственное отображение f^\dagger такое, что (в традиционной нотации)

$$\langle \psi | f(\phi) \rangle = \langle f^\dagger(\psi) | \phi \rangle$$

для всех ψ, ϕ . В терминах матриц это *сопряженная транспонированная матрица*. Такие адьюнкты удовлетворяют условиям (4.32) и (4.33), причем в случае (4.33) мы ограничиваемся только нормированными состояниями. В разделе 5.3.2 мы увидим, что если бы мы интерпретировали адьюнкты с помощью транспонирования, то ни одно из этих условий не было бы выполнено. Поэтому транспонирование, очевидно, не годится для определения адьюнкции в теории **линейных отображений**.

4.3.2. Сопряжение

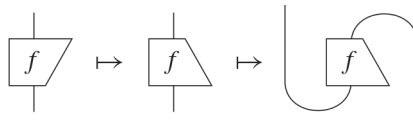
А что, если скомбинировать адьюнкцию с транспонированием? В геометрии вертикальное отражение и поворот на 180° можно производить в любом порядке – так:



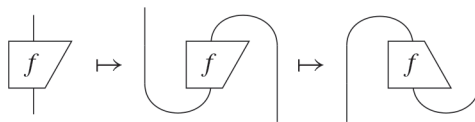
или так:



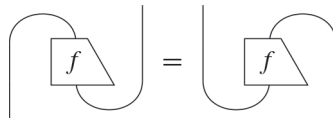
В любом случае, в итоге получается горизонтальное отражение. Воспользовавшись определением транспонирования в терминах чашек и крышек, получаем, что транспонирование адьюнкта дает:



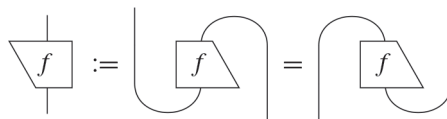
а адьюнкция транспонирования:



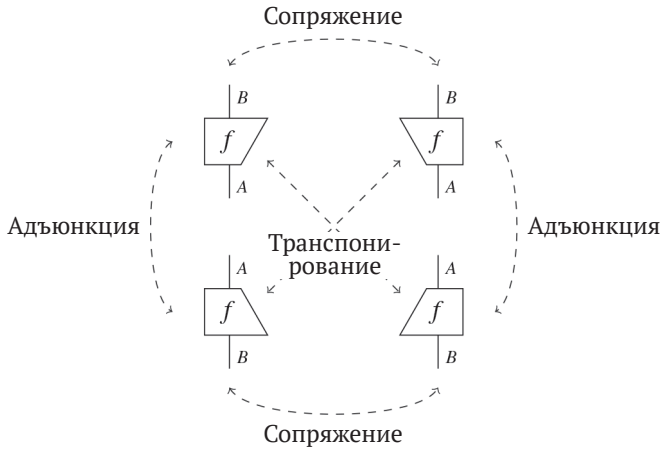
Это одно и то же, т. к. следующее преобразование является простой деформацией диаграмм:



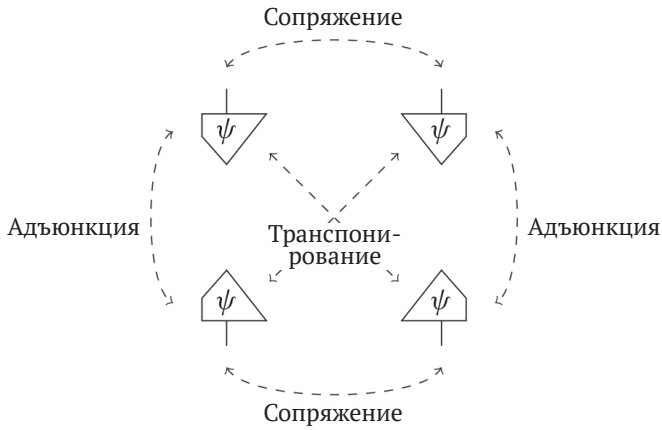
Определение 4.42. *Сопряженным (conjugate) процессом называется результат транспонирования его адьюнкта (или, что то же самое, адьюнкт транспонирования). Графически это выглядит так:*



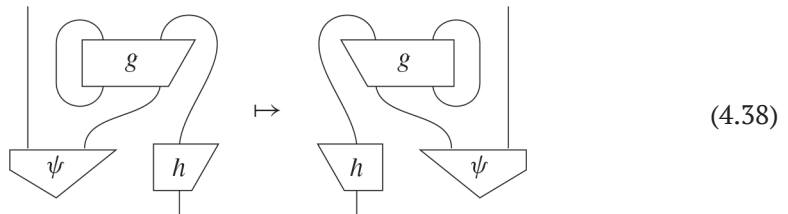
Как и в случае операций адьюнкции и транспонирования, повторное сопряжение приводит к исходному процессу. Собирая все вместе, получаем такой квартет блоков:



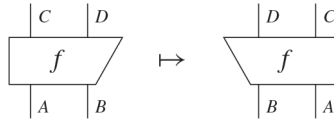
Заодно теперь должно быть понятно, почему мы отрезаем уголок в символах состояний и эффектов:



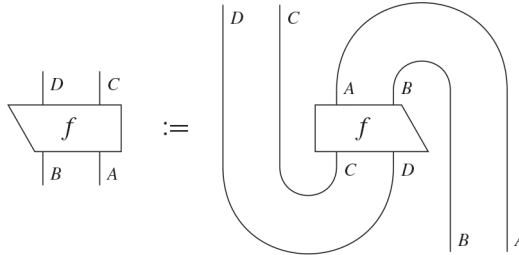
Как и адъюнкция, сопряжение отражает диаграмму целиком, только горизонтально, а не вертикально:



В частности, если блок имеет несколько входов и выходов, то их порядок изменяется на противоположный:



Это, конечно, следует из того факта, что транспонирование обращает порядок входов и выходов, как мы видели в разделе 4.2.2:



Как и в случае транспонирования, иногда желательно этого избежать. Тогда можно использовать *алгебраическое сопряжение*, определяемое в терминах алгебраического транспонирования:

$$\bar{f} := (f^T)^\dagger = (f^\dagger)^T.$$

Эта операция сохраняет порядок входов и выходов ценой перекрещивания проводов:

$$\overline{\left(\begin{array}{|c|c|} \hline C & D \\ \hline \text{\scriptsize } f \\ \hline A & B \\ \hline \end{array} \right)} = \begin{array}{|c|c|} \hline C & D \\ \hline \text{\scriptsize } f \\ \hline A & B \\ \hline \end{array} \quad (4.39)$$

Как и для транспонирования, в случае когда есть только один входной и выходной провода, обычное и алгебраическое сопряжения совпадают.

Замечание* 4.43. В главе 5 мы увидим, что для **линейных отображений** алгебраическое сопряжение делает ровно то, чего и следовало ожидать: заменяет все элементы матрицы комплексно-сопряженными. Поэтому адьюнкция, транспонирование и сопряжение в смысле линейной алгебры соответствуют адьюнкции, алгебраическому транспонированию и алгебраическому сопряжению.

Процессы, равные сопряженным с самими собой, будут играть важную роль в этой книге. Процесс называется *самосопряженным*, если

$$\begin{array}{|c|} \hline \text{\scriptsize } f \\ \hline \end{array} = \begin{array}{|c|} \hline \text{\scriptsize } f \\ \hline \end{array}$$

Для совместных систем это равенство принимает вид:

$$\begin{array}{|c|} \hline B \\ \hline \end{array} \begin{array}{|c|} \hline D \\ \hline \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|} \hline C \\ \hline \end{array} = \begin{array}{|c|} \hline D \\ \hline \end{array} \begin{array}{|c|} \hline B \\ \hline \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline C \\ \hline \end{array} \begin{array}{|c|} \hline A \\ \hline \end{array} \quad (4.40)$$

что, конечно, имеет смысл, только если $A = C$ и $B = D$ или, более общо, если входные и выходные типы – палиндромы, например $A \otimes B \otimes A$ или $B \otimes C \otimes C \otimes B$. С другой стороны, алгебраически самосопряженный процесс в совместной системе выглядит следующим образом:

$$\begin{array}{|c|} \hline B \\ \hline \end{array} \begin{array}{|c|} \hline D \\ \hline \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|} \hline C \\ \hline \end{array} = \begin{array}{|c|} \hline B \\ \hline \end{array} \begin{array}{|c|} \hline D \\ \hline \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|} \hline C \\ \hline \end{array} \quad (4.41)$$

Замечание* 4.44. Матрица является самосопряженной, если все ее элементы – вещественные числа.

Горизонтальное отражение чашки или крышки снова является чашкой или крышкой, поэтому следующий результат не должен вызывать удивления.

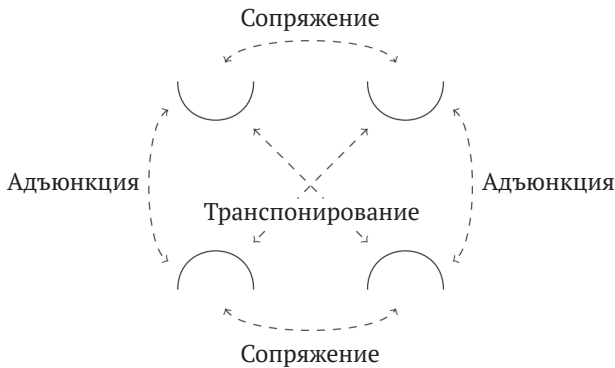
Предложение 4.45. Чашки и крышки являются самосопряженными (а также алгебраически самосопряженными).

Доказательство. Процесс, сопряженный чашке, имеет вид:

равно как и алгебраически сопряженный ей:

Для крышек доказательство аналогично. □

Таким образом, «квартет» для чашек и крышек выглядит так:



Упражнение 4.46. Докажите, что все **отношения** являются алгебраически самосопряженными. Какие из них будут самосопряженными в смысле равенства (4.40)?

Чтобы подчеркнуть, что состояние (или эффект) является самосопряженным, мы вернемся к исходной нотации с использованием треугольников:

$$\begin{array}{c} \downarrow \\ \psi \end{array} := \begin{array}{c} \downarrow \\ \psi \\ \downarrow \end{array} = \begin{array}{c} \downarrow \\ \psi \end{array}$$

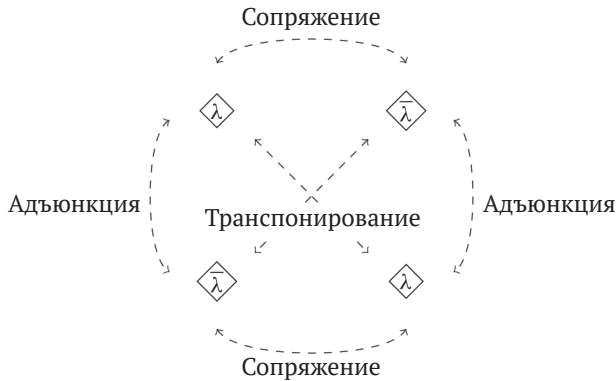
Но при работе с составными системами нужна аккуратность. Поскольку операция сопряжения отражает диаграммы, состояния, включающие несколько самосопряженных состояний, в общем случае не являются самосопряженными:

$$\begin{array}{c} \downarrow \\ \psi \end{array} := \begin{array}{c} \downarrow \\ 0 \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ 1 \\ \downarrow \end{array} \neq \begin{array}{c} \downarrow \\ 1 \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ 0 \\ \downarrow \end{array} =: \begin{array}{c} \downarrow \\ \psi \end{array}$$

Пример 4.47. Состояния и эффекты для одной системы в теории **отношений** всегда являются самосопряженными, поэтому мы будем изображать их, как показано выше. В частности, мы продолжим изображать состояния из примера 3.36 в виде:


$$\begin{array}{c} \downarrow \\ \emptyset \end{array} \quad \begin{array}{c} \downarrow \\ 0 \end{array} \quad \begin{array}{c} \downarrow \\ 1 \end{array} \quad \begin{array}{c} \downarrow \\ \mathbb{B} \end{array}$$


Для чисел операция транспонирования тривиальна (см. пример 4.31), поэтому сопряжение и адьюнкция – одно и то же. Следовательно, «квартет» для чисел превращается в «дуэт» числа и сопряженного к нему:



4.3.3. Внутреннее произведение

Вводя нотацию Дирака в разделе 3.4.4, мы упомянули, что диаграммному языку недостает возможности преобразовывать кет в бра и наоборот. Именно это и позволяет сделать адьюнкция, поэтому теперь можно изменить правила **D2** и **D3**, включив в них адьюнкты:

D2:  записывается в виде $\langle \phi |$ и называется «бра Дирака»;

D3:  записывается в виде $\langle \phi | \psi \rangle$ и называется «скобкой Дирака».

Композиция в **D3** настолько важна, что заслуживает специального названия.

Определение 4.48. *Внутренним произведением состояний ψ и ϕ одного типа называется:*



Состояния называются *ортогональными*, если

$$\langle \phi | \psi \rangle = 0$$

Квадратом нормы состояния ψ называется внутреннее произведение его с самим собой:



Состояние ψ называется *нормированным*, если

$$\langle \psi | \psi \rangle = \square$$

Замечание 4.49. Мы говорим «квадрат нормы», потому что в линейной алгебре нормой ψ обычно называется квадратный корень из этой величины.

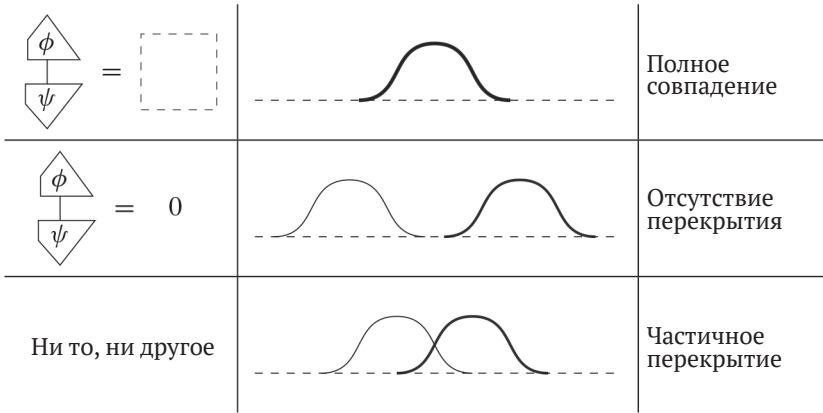
Смысл внутреннего произведения становится ясен, если вспомнить, для чего мы вводили операцию адьюнкции. Поскольку адьюнкт состояния – это эффект, проверяющий нахождение в этом состоянии, то имеем:

$$\langle \phi | \psi \rangle := \text{«проверка того, что состояние } \psi \text{ является состоянием } \phi \text{»}.$$

Иными словами, внутреннее произведение вычисляет «степень сходства» состояний, а ортогональность означает, что сходства нет вообще. С другой стороны,

когда мы проверяем, совпадает ли состояние само с собой, мы ожидаем получить 1 (т. е. пустую диаграмму). Это действительно так, когда состояние нормированно (что является достаточным основанием использовать нормированные состояния «по умолчанию»).

Еще одно полезное интуитивное соображение касательно «измерения общности» состоит в следующем. Если состояния – это некоторые распределения (например, распределения вероятностей), то внутреннее произведение показывает, насколько сильно эти распределения перекрываются:



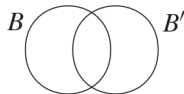
Пример 4.50. Для **отношений** имеем:

$$\begin{array}{c} \triangle \\ 0 \\ \hline \triangle \\ 0 \end{array} = \begin{array}{c} \triangle \\ 0 \\ \hline \triangle \\ B \end{array} = \begin{array}{c} \triangle \\ B \\ \hline \triangle \\ B \end{array} = \text{dashed box} \qquad \begin{array}{c} \triangle \\ 0 \\ \hline \triangle \\ 1 \end{array} = \begin{array}{c} \triangle \\ 0 \\ \hline \triangle \\ \emptyset \end{array} = \begin{array}{c} \triangle \\ B \\ \hline \triangle \\ \emptyset \end{array} = 0$$

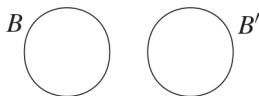
Первые три внутренних произведения включают как «полное совпадение», так и «частичное перекрытие», поскольку оба соответствуют одному и тому же числу. В теории **отношений** перекрытие можно воспринимать буквально, т. к.

$$\begin{array}{c} \triangle \\ B' \\ \hline \triangle \\ B \end{array} = \text{dashed box}$$

означает, что пересечение B и B' не пусто:



С другой стороны, подмножества в последних трех внутренних произведениях вообще не пересекаются:



Внутреннее произведение и соответствующий ему квадрат нормы – стандартные понятия линейной алгебры, и большая часть характерных свойств внутреннего произведения прямо следует из языка струнных диаграмм. Читателям, знакомым с внутренним произведением, будет проще узнать эти свойства, если мы будем обозначать сопряжение скобками $\overline{(\quad)}$ и использовать нотацию Дирака.

Предложение 4.51. Внутреннее произведение обладает следующими свойствами.

1. *Симметрия сопряжения:*

$$\overline{\langle \phi | \psi \rangle} = \langle \psi | \phi \rangle.$$

2. Сохранение внутреннего множителя во втором члене:

$$\langle \phi | \lambda \cdot \psi \rangle = \lambda \cdot \langle \phi | \psi \rangle.$$

3. Замена внутреннего множителя в первом члене сопряженным:

$$\langle \lambda \cdot \phi | \psi \rangle = \bar{\lambda} \cdot \langle \phi | \psi \rangle.$$

4. *Положительная определенность:*

$$\langle \psi | \psi \rangle = 0 \Leftrightarrow |\psi\rangle = 0.$$

Доказательство. Сначала докажем симметричность сопряжения:

$$\overline{\left(\begin{array}{c} \triangleup \phi \\ \triangle \psi \end{array} \right)} = \begin{array}{c} \triangle \phi \\ \triangleup \psi \end{array} \stackrel{(4.16)}{=} \begin{array}{c} \triangle \psi \\ \triangle \phi \end{array} \stackrel{(4.8)}{=} \begin{array}{c} \triangleup \psi \\ \triangle \phi \end{array}$$

Далее, полагая

$$\begin{array}{c} | \\ \triangle \lambda \cdot \psi \end{array} := \diamond \lambda \begin{array}{c} | \\ \triangle \psi \end{array}$$

мы сразу же получаем:

$$\begin{array}{c} \triangle \phi \\ | \\ \triangle \lambda \cdot \psi \end{array} = \diamond \lambda \begin{array}{c} \triangle \phi \\ | \\ \triangle \psi \end{array}$$

а также

$$\begin{array}{c} \triangle \lambda \cdot \phi \\ | \\ \triangle \psi \end{array} = \left(\diamond \lambda \begin{array}{c} | \\ \triangle \phi \end{array} \right)^\dagger \circ \begin{array}{c} | \\ \triangle \psi \end{array} = \diamond \bar{\lambda} \begin{array}{c} \triangle \phi \\ | \\ \triangle \psi \end{array}$$

А в конце раздела 4.3.1 мы дополнительно установили, что свойство

$$\begin{array}{c} \psi \\ \hline \psi \end{array} = 0 \iff \begin{array}{c} | \\ \hline \psi \end{array} = 0$$

как раз и определяет, какие адьюнкты считать хорошими.

Замечание 4.52. Возможно, у читателя возник вопрос, в чем смысл слова «положительная» во фразе «положительная определенность». Это станет ясно в разделе 4.3.5.

Замечание* 4.53. Читатели, знакомые с внутренними произведениями в линейной алгебре, вероятно, ждали, что условия 2 и 3 выше будут называться «линейность» и «сопряженная линейность». Но для этого необходимо, чтобы внутреннее произведение также сохраняло суммы. Это свойство появится естественно, когда мы определим суммы диаграмм в разделе 5.1.3.

4.3.4. Унитарность

Коль скоро внутреннее произведение измеряет общность (перекрытие), то следующий естественный шаг – выявить те процессы, которые сохраняют эту меру.

Определение 4.54. Процесс U называется *изометрией*, если имеет место равенство:

$$\begin{array}{c} | \\ \hline U \\ \hline B \\ \hline U \\ \hline A \end{array} = \begin{array}{c} | \\ \hline A \end{array} \quad (4.42)$$

Иными словами, U^\dagger удовлетворяет одному из двух условий обратимости из определения 4.24, т. е. U^\dagger – *одностороннее обращение* U .

Предложение 4.55. Изометрии сохраняют внутреннее произведение.

Доказательство. Имеем

$$\begin{array}{c} \psi \\ \hline U \circ \phi \\ \hline U \circ \psi \end{array} = \begin{array}{c} \phi \\ \hline U \\ \hline U \\ \hline \psi \end{array} \stackrel{(4.42)}{=} \begin{array}{c} \phi \\ \hline \psi \end{array}$$

□

Если U^\dagger удовлетворяет обоим условиям обратимости, то мы получаем другое понятие.

Определение 4.56. Процесс U называется *унитарным*, если имеет место равенство:

$$\begin{array}{c} A \\ | \\ \square U \triangle \\ | \\ B \\ | \\ \square U \triangle \\ | \\ A \end{array} = | A \qquad \begin{array}{c} B \\ | \\ \square U \triangle \\ | \\ A \\ | \\ \square U \triangle \\ | \\ B \end{array} = | B \qquad (4.43)$$

Из упражнения 4.25 мы знаем, что обратный процесс определен однозначно, откуда сразу следует, что для унитарного процесса U

$$\begin{array}{c} | \\ \square U^{-1} \triangle \\ | \end{array} = \begin{array}{c} | \\ \square U \triangle \\ | \end{array}$$

Из диаграммного определения унитарности получаем также следующее предложение.

Предложение 4.57. Тожественные процессы и перекоммутации унитарны, а последовательная и параллельная композиции унитарных процессов также унитарны.

Ниже приведены некоторые альтернативные характеристики унитарности.

Предложение 4.58. Для процесса f следующие утверждения эквивалентны:

- f унитарный;
- f – обратимая изометрия;
- f^\dagger – обратимая изометрия.

Упражнение 4.59. Докажите предложение 4.58.

В разделе 5.1.5 мы увидим еще несколько эквивалентных свойств изометричных и унитарных процессов.

4.3.5. Положительность

В замечании 4.52 мы обещали объяснить, к чему относится слово «положительная» во фразе «положительная определенность». Оказывается, что внутреннее произведение состояния с самим собой

$$\begin{array}{c} \triangle \psi \\ | \\ \triangle \psi \end{array} \qquad (4.44)$$

– частный случай более общего понятия положительности, имеющего смысл в любой процессной теории.

Определение 4.60. Процесс f называется *положительным*, если для некоторого g имеет место равенство:

$$\text{Diagram } f \text{ with two } A \text{ legs} = \text{Diagram } g \text{ with } A \text{ and } B \text{ legs} \text{ composed} \quad (4.45)$$

Таким образом, число на диаграмме (4.44) положительно по определению. На самом деле во многих процессных теориях

$$\langle \lambda \rangle = \text{Diagram } \psi \text{ with } B \text{ leg} \text{ simplifies to } \langle \lambda \rangle = \langle \mu \rangle \langle \mu \rangle$$

То есть мы всегда можем в качестве B взять «отсутствие провода». И, как мы увидим в следующей главе, тем самым мы фактически получаем аналог обычного понятия положительного числа (вещественного числа ≥ 0) для теории **линейных отображений**. Однако такое понятие положительности применимо уже не только к числам, но и к любым процессам с одной и той же системой на входе и выходе.

Из (4.45) с очевидностью следует, что положительные процессы инвариантны относительно вертикального отражения.

Предложение 4.61. Положительные процессы являются *самоадъюнктными*, т. е.

$$\text{Diagram } f \text{ with two legs} = \text{Diagram } f \text{ with two legs (reflected)} \quad (4.46)$$

В частности, самоадъюнктны положительные числа, а следовательно, поскольку транспонирование чисел – тривиальная операция, они являются и самосопряженными.

В силу положительной определенности ненулевые положительные процессы имеют ненулевой след. Иначе говоря, мы можем установить, является ли положительный процесс нулевым, вычислив его след.

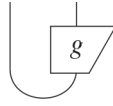
Предложение 4.62. Для положительных процессов имеет место импликация

$$\text{Diagram } f \text{ with a loop} = 0 \implies \text{Diagram } f \text{ with two legs} = 0$$

Доказательство. Если процесс f положительный, то имеем:

$$\text{Diagram } f \text{ with a loop} = \text{Diagram } g \text{ with } A \text{ and } B \text{ legs composed}$$

поэтому след f равен внутреннему произведению состояния



с самим собой. Если это внутреннее произведение равно нулю, то в силу положительной определенности равно нулю и это состояние. Следовательно, само g равно 0, а вместе с ним и f . □

Из общего определения положительного процесса вытекает также понятие положительности, знакомое из линейной алгебры. А именно если процесс f положительный, то число

$$\langle \psi | f | \psi \rangle =$$

положительно для всех ψ . В этом легко убедиться, продолжив определение 4.60:

4.3.6. \otimes -положительность

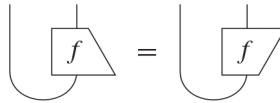
Мы начали эту главу с наблюдения, что посредством двойственности процессов и состояний мы можем связать \circ -разделимость процессов с \otimes -разделимостью двухкомпонентных состояний. Аналогично можно связать самоадьюнктные процессы с самосопряженными состояниями:

Предложение 4.63. Состояние ψ является самосопряженным тогда и только тогда, когда двойственный ему процесс f является самоадьюнктным:

Доказательство. Сопряженным к двухкомпонентному состоянию ψ является состояние:



и оно равно самому ψ тогда и только тогда, когда



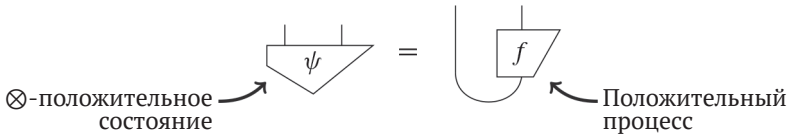
т. е. тогда и только тогда, когда процесс f является самоадьюнктным. □

Мы введем новое название для \otimes -аналога положительности.

Определение 4.64. Двухкомпонентное состояние ψ называется \otimes -положительным, если для некоторого процесса g имеет место равенство

(4.47)

Предложение 4.65. Состояние ψ \otimes -положительно тогда и только тогда, когда двойственный ему процесс f положителен:



Доказательство. Если выразить двухкомпонентное состояние ψ в терминах процесса f , то \otimes -положительность принимает вид условия:

для некоторого процесса g , что эквивалентно положительности f . □

Мы можем распространить определение \otimes -положительности состояний на процессы.

Определение 4.66. Процесс f называется \otimes -положительным, если для некоторого процесса g имеет место равенство

$$\begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline B \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline B \\ \hline \end{array} = \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad (4.48)$$

или, что эквивалентно, для некоторого процесса g' имеет место равенство

$$\begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline B \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline B \\ \hline \end{array} = \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad (4.49)$$

Полагая

$$\begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} := \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array}$$

мы действительно можем перейти от (4.48) к (4.49) и обратно:

$$\begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} = \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} = \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline C \\ \hline \end{array} \quad \begin{array}{|c|} \hline B \\ \hline \text{---} \\ \hline A \\ \hline \end{array}$$

Как следствие легко видеть, что \otimes -положительные состояния являются частным случаем \otimes -положительных процессов, в котором A – тривиальная система.

Упражнение 4.67. Покажите, что последовательная композиция двух \otimes -положительных процессов также является \otimes -положительным процессом.

Пример* 4.68. Некоторым читателям, возможно, знакомы *операторы плотности*, являющиеся примером положительных «процессов». Мы заключили слово «процессы» в кавычки, поскольку в квантовой теории операторы плотности используются для представления состояний. В главе 6 мы для представления квантовых состояний будем использовать не операторы плотности, а их \otimes -положительные аналоги. Мы также будем использовать \otimes -положительные процессы вместо *вполне положительных отображений* для представления квантовых процессов. Причина понятна: состояния должны представляться состояниями, а не «процессами», а процессы – процессами (а не «суперпроцессами», т. е. объектами, которые переводят один процесс в другой).

4.3.7. Проекторы

Еще немного расширим понятийный аппарат, связанный с процессами.

Определение 4.69. *Проектом* называется процесс P , который является положительным и *идемпотентным*:

$$\begin{array}{c} | \\ \hline P \\ \hline | \end{array} = \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array} \quad (4.50)$$

Предложение 4.70. Для процесса P следующие утверждения эквивалентны:

- (i) он является проектором;
- (ii) он самоадьюнктный и идемпотентный;
- (iii) он удовлетворяет условию

$$\begin{array}{c} | \\ \hline P \\ \hline | \end{array} = \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array} \quad (4.51)$$

Доказательство. Импликация (i \Rightarrow ii) следует из предложения 4.61. Импликация (ii \Rightarrow iii) вытекает из следующих равенств:

$$\begin{array}{c} | \\ \hline P \\ \hline | \end{array} \stackrel{(4.50)}{=} \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array} \stackrel{(4.46)}{=} \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array}$$

Что касается импликации (iii \Rightarrow i), то из (4.51) сразу следует, что P положительный. Поэтому он также самоадьюнктный, так что цепочка равенств

$$\begin{array}{c} | \\ \hline P \\ \hline | \end{array} \stackrel{(4.51)}{=} \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array} \stackrel{(4.46)}{=} \begin{array}{c} | \\ \hline P \\ \hline | \\ \hline P \\ \hline | \end{array}$$

устанавливает идемпотентность. □

Мы можем построить проектор по любому нормированному состоянию ψ следующим образом:

$$\begin{array}{c} | \\ \hline \psi \\ \hline | \\ \hline \psi \\ \hline | \end{array} \quad (4.52)$$

Этот процесс, очевидно, положителен, а идемпотентность легко доказывается:

$$\begin{array}{c} \psi \\ \psi \\ \psi \\ \psi \end{array} = \begin{array}{c} \psi \\ \square \\ \psi \end{array} = \begin{array}{c} \psi \\ \psi \end{array} \tag{4.53}$$

Будем называть такие проекторы *разделимыми*. На самом деле, при условии что $\psi \neq 0$, этот рецепт всегда дает проектор с точностью до числа (см. раздел 3.4.3):

$$\begin{array}{c} \psi \\ \psi \\ \psi \\ \psi \end{array} \approx \begin{array}{c} \psi \\ \psi \end{array}$$

Замечание* 4.71. В линейной алгебре разделимые проекторы – это в точности проекции на одномерные подпространства.

Теперь вспомним, что в силу двойственности процессов и состояний всякий процесс f дает следующее состояние:

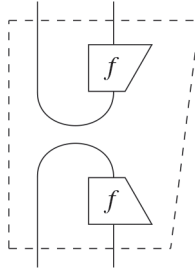
$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ f \end{array} := \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ f \end{array}$$

Если результирующее состояние нормированно, то мы получаем разделимый проектор:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ P_f \end{array} := \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ f \\ f \end{array}$$

Разумеется, в силу той же двойственности процессов и состояний любое двухкомпонентное состояние можно записать в терминах некоторого процесса f , откуда вытекает

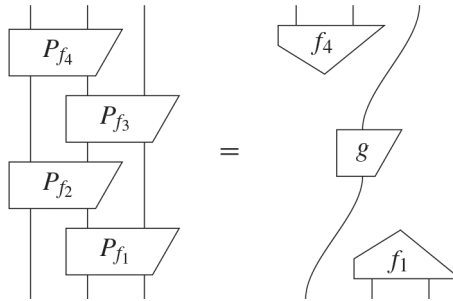
Следствие 4.72. В любой процессной теории, допускающей струнные диаграммы, всякий двухкомпонентный разделимый проектор имеет вид:



(4.54)

В следующем упражнении речь идет о композиции таких двухкомпонентных разделимых проекторов.

Упражнение 4.73. Покажите, что



(4.55)

где

$$g := f_3 \circ \bar{f}_4 \circ f_2^T \circ f_3^\dagger \circ f_1 \circ \bar{f}_2. \quad (4.56)$$

Сможете ли вы на основе этого конкретного вычисления получить более общее утверждение о диаграммах, включающих проекторы такого вида?

Заметим, в частности, что порядок процессов, составляющих g , на первый взгляд кажется совершенно несвязанным с порядком проекторов в левой части равенства (4.55). Получающееся в результате общее утверждение о том, как компонуются эти двухкомпонентные проекторы, на ранних порах диаграммных квантовых рассуждений называлось *логикой запутанности*.

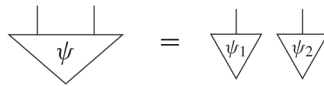
4.4. КВАНТОВЫЕ ОСОБЕННОСТИ, ВЫВОДИМЫЕ ИЗ СТРУННЫХ ДИАГРАММ

Не все процессные теории допускают струнные диаграммы, но те, что допускают, имеют несколько важных общих черт, которые на первый взгляд могут показаться странными. Мы уже видели, как двойственность позволяет сопоставить каждому процессу полностью отражающее его состояние, мы знаем, что операция транспонирования сопоставляет каждому процессу обратный к нему и, более общо, что можно смело менять местами входы и выходы процессов. Мы также видели, что двухкомпонентные проекторы демонстрируют довольно экстравагантное поведение при композиции. У всех этих особенностей нет аналогов в процессной

теории, не допускающей струнных диаграмм, например в теории **функций** (см. упражнение 4.10). Далее в этой главе мы обсудим и другие простые следствия природы струнных диаграмм, которые иногда (быть может, преждевременно) называют «квантовой странностью».

4.4.1. Теорема о невозможности универсальной делимости

Термин «теорема о невозможности», или «запрещающая теорема», означает результат, устанавливающий невозможность чего-то, что в свете нашего повседневного опыта может показаться истинным. Первая встретившаяся нам теорема о невозможности утверждает, что если нетривиальная теория допускает струнные диаграммы, то не может быть так, что все ее двухкомпонентные состояния делимы. Поскольку для описания \otimes -разделимого состояния



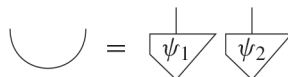
нужно описать состояния ψ_1 и ψ_2 соответствующих подсистем, то из этой теоремы следует, что должны существовать состояния составных систем, для описания которых недостаточно описать их части.

Чтобы перевести это в обыденную плоскость, предположим, что есть два объекта: удлинитель и додо. Тогда для описания системы, состоящей из этих двух объектов, достаточно описать объекты по отдельности. В \otimes -неразделимой теории это уже неверно: свойств частей недостаточно для описания свойств целого. Если бы дело обстояло так для системы додо–удлинитель, то свойства обоих объектов перемешались бы до полного хаоса. Например, цвет хохолка додо мог бы зависеть от того, на какую вилку рассчитан удлинитель: британскую или европейскую. Хотя эта конкретная ситуация кажется лишенной всякого смысла, в нашей повседневной жизни встречаются явления, которые по сути своей \otimes -неразделимы. Одно из них – близнецы: они характеризуются не тем, что у каждого близнеца есть определенное свойство, например светлые волосы или высокий рост, а тем, что каким бы свойством ни обладал один близнец, другой также будет обладать им. Такую концепцию можно было бы, к примеру, смоделировать чашками и крышками в теории **отношений**, как описано в упражнении 4.16.

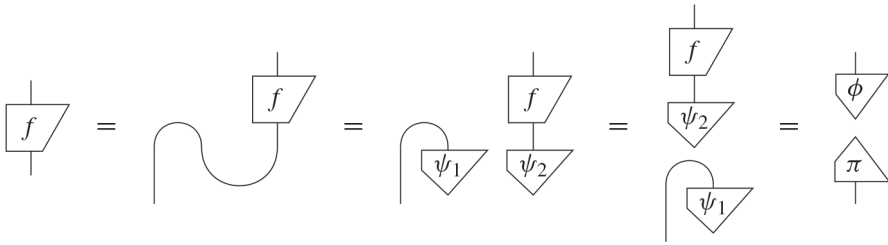
Способ доказательства теоремы о невозможности универсальной делимости уже был указан в замечании 4.7. Мы покажем, что если все двухкомпонентные состояния \otimes -разделимы, то все процессы \circ -разделимы, поэтому мы имеем дело с теорией, в которой все процессы постоянны, т. е. ничего не происходит. Но для любой «разумной» теории процессов это условие звучит абсурдно, а значит, все двухкомпонентные состояния не могут быть \otimes -разделимы.

Предложение 4.74. Если теория описывается струнными диаграммами и все двухкомпонентные состояния \otimes -разделимы, то все процессы \circ -разделимы.

Доказательство. По предположению, чашка – \otimes -разделимое состояние:

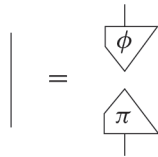


Поэтому для любого процесса f имеем:



для состояния $\phi := f \circ \psi_2$ и эффекта $\pi := \psi_1^T$. □

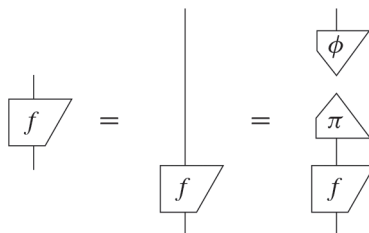
Если все процессы \circ -разделимы, значит, \circ -разделимы и тождественные процессы:



Поэтому, внимательно приглядевшись, можно обнаружить, что провода – это и не провода вовсе:



Обратно, мы могли бы с тем же успехом показать, что раз тождественные процессы \circ -разделимы, то и любой процесс \circ -разделим:



Доказательство. Полагая

$$\begin{array}{|c} \hline f^{-1} \\ \hline \end{array} := \begin{array}{|c} \hline \phi \\ \hline \end{array}$$

получаем:

$$\begin{array}{|c} \hline f^{-1} \\ \hline \end{array} = \begin{array}{|c} \hline \phi \\ \hline \end{array} = \begin{array}{|c} \hline \psi \\ \hline \end{array}$$

и

$$\begin{array}{|c} \hline f \\ \hline \end{array} = \begin{array}{|c} \hline \phi \\ \hline \end{array} = \begin{array}{|c} \hline \psi \\ \hline \end{array}$$

Из этих равенств с очевидностью следует, что f и f^{-1} удовлетворяют условиям обратимости (4.13) тогда и только тогда, когда ψ и ϕ удовлетворяют условиям невырожденности (4.57). \square

Пример* 4.79. Невырожденные эффекты наподобие ϕ часто встречаются в линейной алгебре, где называются *невырожденными билинейными формами*. В теории квантовой запутанности невырожденные состояния называются *состояниями полного ранга (Шмидта)*, или *SLOCC-максимальными состояниями*. Причины этого станут ясны в разделе 13.3.2.

Унитарные процессы – частный случай обратимых процессов, поэтому соответствующие им двухкомпонентные состояния являются специализацией чаше-подобных состояний.

Определение 4.80. Состояние ψ называется *максимально неразделимым*, если двойственный ему процесс U унитарный с точностью до числа:

$$\begin{array}{|c} \hline U \\ \hline \end{array} \approx \begin{array}{|c} \hline \psi \\ \hline \end{array} \tag{4.58}$$

Унитарный Максимально неразделимое

Обратите внимание, что мы используем знак \approx , чтобы ψ могло быть нормированным, несмотря на то что правая часть равенства (4.58) (почти) никогда нормированной не бывает.

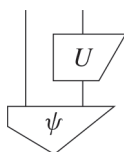
Упражнение 4.81. Чему равен квадрат нормы



когда процесс U унитарный? Когда это состояние нормированно?

Следующее упражнение показывает полезность унитарных процессов для взаимных преобразований максимально неразделимых состояний.

Упражнение 4.82. Покажите, что если применить унитарный процесс к одной стороне максимально неразделимого состояния:



то снова получится максимально неразделимое состояние, и что этот унитарный процесс всегда можно выбрать так, что результирующее состояние будет чашкой (с точностью до числа).

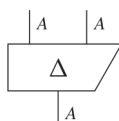
Пример* 4.83. В квантовой теории так определенные максимально неразделимые состояния называются *максимально запутанными состояниями*, или *LOCC-максимальными состояниями*, по причинам, которые мы объясним в разделе 13.3.1.

4.4.2. Две теоремы о невозможности клонирования

Одна из характерных особенностей классических вычислений – возможность копировать биты по своему усмотрению. Например, эта книга когда-то была PDF-файлом на наших компьютерах, а потом ее скопировали и разослали в разные места. Вроде бы вещь совершенно очевидная, однако «копирование» невозможно, когда мы имеем дело с состояниями и процессами в струнных диаграммах! И хотя поначалу это может показаться катастрофой, но полностью согласуется с тем, что происходит в квантовом мире и, как выясняется, дает неожиданные преимущества. Так, если мы хотим сохранить что-то в секрете, например ПИН-код банковской карты, то в мире, где нет копирования, украсть секрет без ведома владельца будет гораздо сложнее. Этот принцип лежит в основе квантовой криптографии, а также многих других квантовых протоколов безопасности, как мы увидим в разделе 9.2.6.

До сих пор наши вычисления были довольно тривиальными, а все доказанные факты на языке струнных диаграмм выглядели очевидно. Но следующие две теоремы, и особенно первая, потребуют более тонкой диаграммной эквилибристики.

Под *клоняющим процессом* для системы типа A мы понимаем процесс



который переводит входное состояние ψ в две копии ψ :

$$\text{Diagram} = \text{Diagram} \quad (4.59)$$

Мы ожидаем, что такой процесс будет обладать некоторыми естественными свойствами. Например, поскольку он порождает на выходе две идентичные копии состояния, их порядок не должен иметь значения:

$$\text{Diagram} = \text{Diagram} \quad (4.60)$$

Далее, если имеется два клонирующих процесса, один для типа A , другой для типа B , то для клонирования состояния типа $A \otimes B$ должно быть достаточно клонировать каждую систему по отдельности:

$$\text{Diagram} = \text{Diagram} \quad (4.61)$$

Наконец, мы будем предполагать, что наша процессная теория содержит хотя бы одно нормированное состояние, т. е. такое состояние ψ , что:

$$\text{Diagram} = \text{Diagram} \quad (4.62)$$

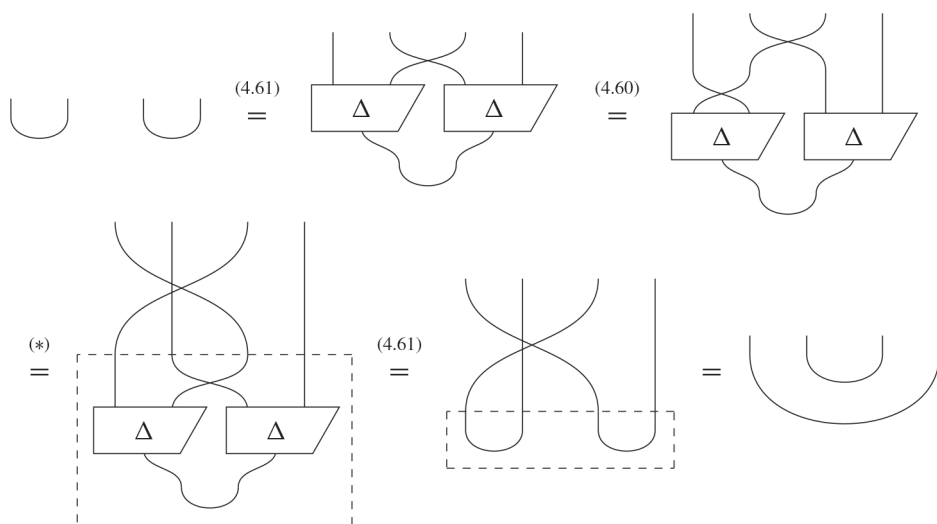
По существу, это тривиальное предположение, поскольку иначе просто нечего было бы клонировать!

Теорема 4.84. Рассмотрим процессную теорию, допускающую струнные диаграммы. Если существует клонирующий процесс типа A , который удовлетворяет условиям (4.60), (4.61) и (4.62), то любой процесс с системой типа A на входе обязан быть \circ -разделимым.

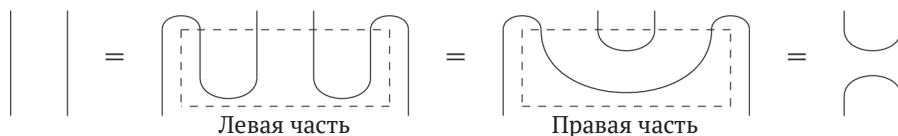
Доказательство. Применяя (4.61) к равенству

$$\text{Diagram} := \text{Diagram}$$

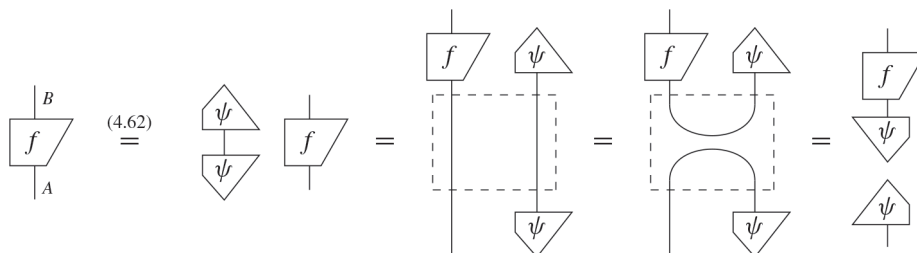
получаем



где все провода имеют тип A , а $(*)$ – просто деформация диаграммы. Теперь, если преобразовать внешние выходы левой и правой частей во входы:



то обнаружится, что тождественный процесс для пары систем разделим, что уже должно вызвать удивление. Подставляя это равенство в обведенные пунктиром области ниже:



мы действительно получаем, что всякий процесс f , получающий на входе систему типа A , \circ -разделим. □

Таким образом, в свете нашей концепции «тривиальности» из раздела 4.4.1, если существует клонирующий процесс для некоторого системного типа A , то процессная теория тривиальна относительно типа A , а если любой системный тип допускает клонирующий процесс, то и вся процессная теория тривиальна.

На самом деле все портит предположение (4.61). Если «думать» на языке струнных диаграмм, то довольно очевидно, что попытка скопировать неразделимое состояние, совершая какие-то действия с каждой подсистемой, заведомо обречена на провал.

Теорема 4.84 заметно отличается от той, что приводится в большинстве учебников. Во-первых, клонирующий процесс обычно определяется как процесс с двумя входами и двумя выходами, для которого второй вход находится в некотором фиксированном состоянии ϕ , которое перезаписывается скопированным состоянием ψ :

$$\begin{array}{c} \text{---} \\ \text{---} \\ \Delta' \\ \text{---} \\ \psi \quad \phi \end{array} = \begin{array}{c} \psi \\ \psi \end{array} \quad (4.63)$$

Понятно, что клонирующий процесс с одним входом и двумя выходами возникает следующим образом:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \Delta \\ \text{---} \end{array} := \begin{array}{c} \text{---} \\ \text{---} \\ \Delta' \\ \phi \end{array} \quad (4.64)$$

и мы легко могли бы использовать (4.64) для доказательства теоремы 4.84.

Во-вторых, обычно предполагается, что процесс Δ' в равенстве (4.63) унитарный, что, в свою очередь, означает, что предположения (4.60) и (4.61) не нужны.

Это отличие настолько существенно, что приводит, по существу, к другой теореме, несмотря на то что мы пытаемся установить одно и то же явление. Предположение об унитарности обосновано самой квантовой теорией (см. раздел 6.2.6). Но хотя эта теорема опирается на добавочные предположения, она все равно интересна, поскольку дополнительно точно показывает, какие наборы состояний *можно* совместно клонировать одним процессом, а именно *ортогональные*. Совместная клонируемость ортогональных состояний тесно связана с тем фактом, что они используются для кодирования классических данных в квантовых системах – эту тему мы будем изучать в главе 8, где дадим элегантное диаграммное представление классических данных.

Вместо Δ' мы будем использовать Δ , определенное, как в равенстве (4.64). В силу унитарности Δ' , если ϕ нормированное, Δ должно быть изометрией:

$$\begin{array}{c} \text{---} \\ \Delta \\ \text{---} \\ \text{---} \\ \Delta \\ \text{---} \end{array} \stackrel{(4.64)}{=} \begin{array}{c} \phi \\ \Delta' \\ \text{---} \\ \Delta' \\ \phi \end{array} \stackrel{(4.43)}{=} \left| \begin{array}{c} \phi \\ \phi \end{array} \right| \quad (4.43)$$

Таким образом, мы предполагаем существование изометрии, удовлетворяющей условию клонирования (4.59). Конечно, самым серьезным добавочным предположением в традиционной теореме о невозможности клонирования является то, что мы имеем дело с конкретной теорией **квантовых процессов** (которую мы пока еще даже не определили!). Однако это предположение избыточно. На самом деле нам только и нужны два допущения о числах в нашей теории:

(а) все ненулевые числа допускают *сокращение*, т. е. если $\lambda \neq 0$, то

$$\lambda \begin{array}{|c|} \hline \diagup \\ \hline f \\ \hline \diagdown \\ \hline \end{array} = \lambda \begin{array}{|c|} \hline \diagdown \\ \hline g \\ \hline \diagup \\ \hline \end{array} \implies \begin{array}{|c|} \hline \diagup \\ \hline f \\ \hline \diagdown \\ \hline \end{array} = \begin{array}{|c|} \hline \diagdown \\ \hline g \\ \hline \diagup \\ \hline \end{array}$$

что, очевидно, справедливо для чисел, представляющих возможность (см. теорию **отношений**) или вероятность;

(б) число 1 означает «достоверно», как в разделе 4.3.1. То есть для нормированных состояний ψ_1, ψ_2 имеем:

$$\begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array} = \begin{array}{|c|} \hline \\ \hline \\ \hline \\ \hline \\ \hline \end{array} \implies \begin{array}{|c|} \hline \psi_1 \\ \hline \diagdown \\ \hline \end{array} = \begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \end{array}$$

Теорема 4.85. В любой процессной теории, допускающей струнные диаграммы и удовлетворяющей условиям (а) и (б) выше, если два нормированных состояния ψ_1 и ψ_2 можно клонировать изометрическим процессом Δ , то они либо равны, либо ортогональны, т. е.

$$\begin{array}{|c|} \hline \psi_1 \\ \hline \diagdown \\ \hline \end{array} = \begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \end{array} \quad \text{или} \quad \begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array} = 0$$

Доказательство. Сначала заметим, что

$$\begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array} \stackrel{(4.43)}{=} \begin{array}{|c|} \hline \psi_2 \\ \hline \Delta \\ \hline \Delta \\ \hline \psi_1 \\ \hline \end{array} \stackrel{(4.59)}{=} \begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array} \begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array}$$

Далее рассмотрим два случая. Если

$$\begin{array}{|c|} \hline \psi_2 \\ \hline \diagdown \\ \hline \psi_1 \\ \hline \diagup \\ \hline \end{array} \neq 0$$

то, по предположению (a), мы можем сократить это число в обеих частях и получить

$$\square = \begin{array}{c} \triangle \psi_2 \\ | \\ \triangle \psi_1 \end{array}$$

Поэтому, в силу предположения (b), состояния ψ_1 и ψ_2 равны. С другой стороны, если

$$\begin{array}{c} \triangle \psi_2 \\ | \\ \triangle \psi_1 \end{array} = 0$$

то ψ_1 и ψ_2 ортогональны. □

Из теоремы 4.85 сразу же вытекает вторая теорема о невозможности клонирования.

Следствие 4.86. В предположениях теоремы 4.85, если в процессной теории имеется, по крайней мере, два состояния типа A , которые не являются ни равными, ни ортогональными, то не существует клонирующего процесса типа A .

Замечание 4.87. Отметим, что первая теорема о невозможности клонирования применима к **отношениям**, тогда как вторая к ним неприменима, поскольку опирается на предположение (b). На самом деле доказательство первой теоремы вообще не зависит от адьюнктов, так что в этом смысле она более общая. Однако во второй теореме нет никаких дополнительных предположений о механизме клонирования (и прежде всего ограничения (4.61) на клонирование совместных состояний), поэтому она не является непосредственным следствием теоремы 4.84.

Замечание 4.88. Во фразе «возможность копировать биты по своему усмотрению» есть одна тонкость: предполагается, что биты *детерминированы*, т. е. имеют определенные значения. Мы не будем сейчас вдаваться в этот вопрос, а обсудим его в разделе 6.2.8 вместе с уточненной теоремой о невозможности, в которой это ограничение снято.

4.4.3. Как будто время вспять течет

Рассмотрим следующие струнные диаграммы:

$$\begin{array}{c} \text{---} \\ | \\ \square f \\ | \\ \square g \\ | \\ \text{---} \end{array} \quad = \quad \begin{array}{c} \text{---} \\ | \\ \square g \\ | \\ \square f \\ | \\ \text{---} \end{array} \tag{4.65}$$

Будем интерпретировать левую и правую части как процессы, имеющие место в моменты времени t_1, \dots, t_4 :

(4.66)

Тогда получается странная вещь. Рассматривая левую часть, мы имеем:

- t_2 : происходит что-то, в чем участвует g ;
- t_3 : происходит что-то, в чем участвует f .

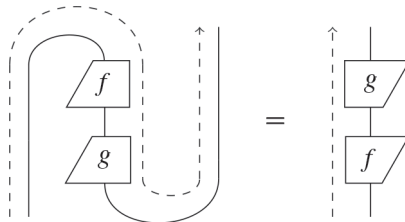
С другой стороны, при рассмотрении правой части мы видим:

- t_2 : происходит что-то, в чем участвует f ;
- t_3 : происходит что-то, в чем участвует g .

В левой части выход процесса, помеченного как g , является входом процесса, помеченного как f , а в правой части все наоборот – выход процесса, помеченного как f , является входом процесса, помеченного как g . То есть порядок протекания процессов поменялся на противоположный!

Причина, по которой такое может случиться, заключается в том, что две равные диаграммы могут относиться к совершенно разным *операционным сценариям*. Операционный сценарий – это способ фактической реализации диаграммы, например путем соединения каких-то устройств проводами в лаборатории. Левая и правая части приведенного выше равенства в операционном смысле различны, поскольку в левой части в моменты t_2 и t_3 участвуют три системы, а в правой части в любой момент времени – только одна. Чашки соответствуют созданию двух систем, а крышки – уничтожению двух систем. В результате левая часть описывает более сложный операционный сценарий, который в правой части упрощен.

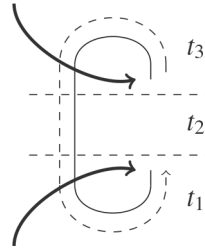
Несмотря на различия операционных прочтений, конечный результат, согласно нашей теории, один и тот же. Можно было бы назвать его *логическим прочтением* струнной диаграммы. В данном случае, чтобы убедиться в том, что логические прочтения обеих диаграмм совпадают, достаточно проследить за логическим потоком диаграммы:



который проходит сначала через блок f , а затем через блок g .

При логическом прочтении чашка и крышка создают видимость того, что системы движутся назад во времени! Это навело нескольких исследователей на мысль предложить чашку и крышку как модель путешествий во времени:

Здесь входим в машину времени



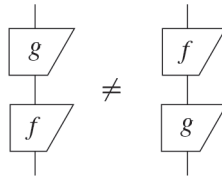
Выходим из машины времени в прошлом

Означает ли это, что чашки и крышки открывают путь к созданию настоящей машины времени? Нет, конечно! Основная проблема здесь в том, что, как мы увидим позже, крышки невозможно реализовать достоверно, а можно лишь с некоторой вероятностью. А причина этого – в так называемом *принципе причинности* (см. раздел 6.4). В общем, если кто-то предложит вам совершить путешествие в такой машине, настоятельно рекомендуем отказаться, поскольку, как мы увидим в разделе 6.4.4, обратно вы выйдете в несколько перепутанном виде!

Упражнение 4.89. Обозначим $\mathbb{T} := \{0, 1, 2\}$ множество из трех элементов (множество «тритов»). Определим отношения $f, g : \mathbb{T} \mapsto \mathbb{T}$ следующим образом:

- $f :: \{0 \mapsto 1, 1 \mapsto 0, 2 \mapsto 2\}$;
- $g :: \{0 \mapsto 0, 1 \mapsto 2, 2 \mapsto 1\}$.

Отметим, кстати, что эти отношения не коммутативны:



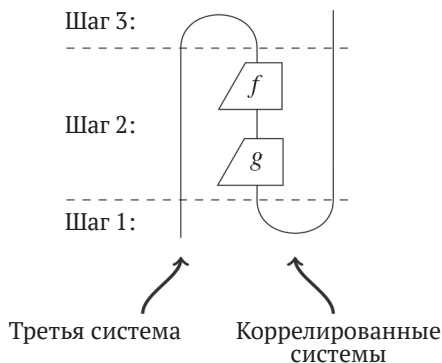
Пусть чашка и крышка определены, как в упражнении 4.16. Проверьте уравнение «обращения времени» (4.65), явно вычислив композицию отношений.

Упражнение 4.89 демонстрирует, как можно реализовать «обращение времени» с помощью недетерминированных процессов.

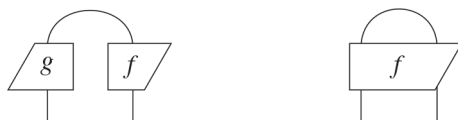
Шаг 1: создать недетерминированные прямолинейные корреляции двух систем.

Шаг 2: применить две последовательные операции к одной из систем.

Шаг 3: предписать, что выход совпадает с состоянием третьей системы.



Помимо струнных диаграмм, просто имеющих странных логические прочтения, могут быть диаграммы, допускающие несколько прочтений или вообще ни одного, например:

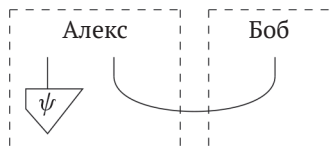


Куда направлен «поток» на левой диаграмме: от g к f или от f к g ? И кто знает, что на самом деле происходит на правой диаграмме? Однако мы все же можем придать смысл таким диаграммам, если будем интерпретировать провода не как «поток», имеющий определенное направление, а как «требование одинаковости значений на обеих сторонах» – тогда концепция обретает симметрию.

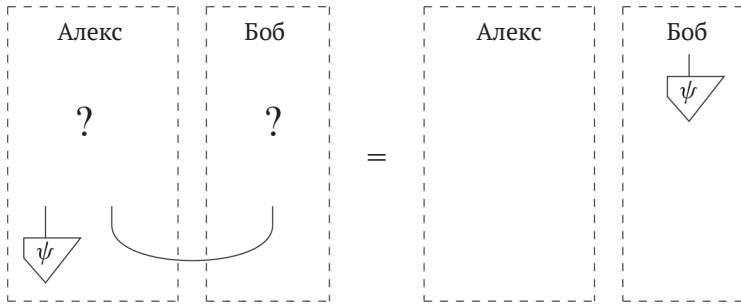
4.4.4. Телепортация

Вот мы и подошли к одному из «сногшибательных приложений» квантовой теории: квантовой телепортации. Удивительно, но для описания самой сути квантовой телепортации достаточно тех диаграммных средств, с которыми мы уже знакомы. В главе 6 мы вернемся к этому протоколу и восполним детали, в частности дадим аккуратное определение *квантовых состояний и измерений*.

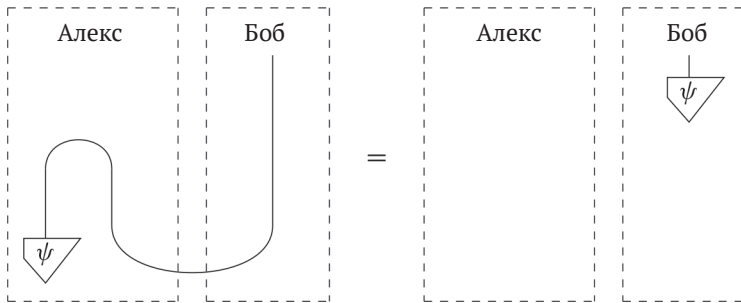
Итак, в чем состоит проблема? Алекс и Боб находятся далеко друг от друга, Алекс располагает системой в состоянии ψ , а Бобу нужно это состояние. Предположим также, что оба они разделяют еще одно состояние: чашку. То есть мы имеем такую ситуацию:



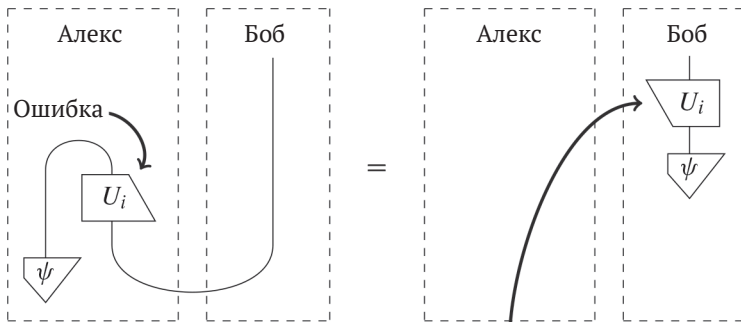
При подобном начальном положении могут ли Алекс и Боб сделать в областях, помеченных знаком вопроса, нечто такое, в результате чего Боб получит ψ ?



Вот простое решение:



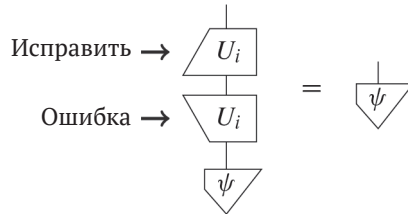
Но является ли крышка (т. е. эффект) процессом, который Алекс может «сделать»? Не совсем. В главе 6 мы увидим, что эффекты возникают в результате квантовых измерений. А у измерения есть такая особенность, что Алекс может получить не тот эффект, что хочет (т. е. крышку), а крышку с некоторой (недетерминированной) ошибкой, которую мы можем представить в виде блока:



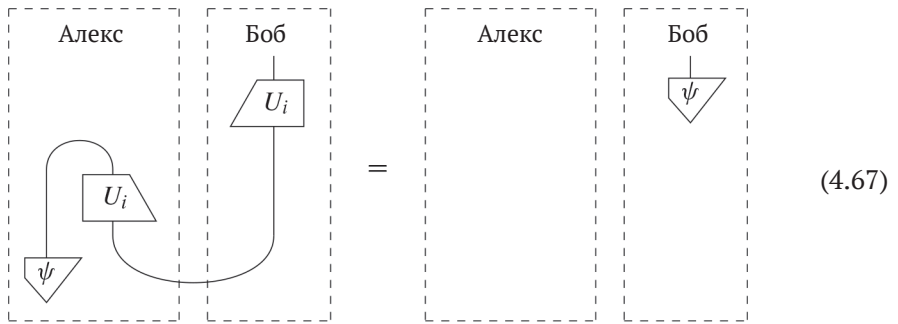
Теперь эта проблема и у Боба!

Алекс заранее не знает, какую ошибку получит, известно лишь, что она принадлежит множеству $\{U_0, U_1, \dots, U_{n-1}\}$. Может случиться так, что U_0 – тождественный процесс, т. е. ошибки нет вообще. Если он считает себя счастливым, то будет надеяться, что так и произойдет, а если не произойдет, то он попробует еще

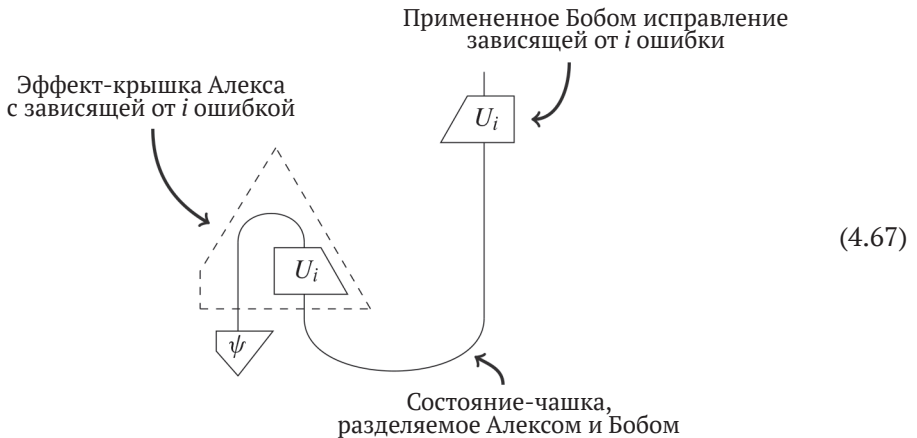
раз с новым ψ и новым состоянием-чашкой. Это называется *поствыборкой* (post-selection). Поразмыслив, Алекс понимает, что такая тактика несколько расточительна. Более того, если он располагает только одной системой в состоянии ψ , то это состояние будет навсегда потеряно. Поэтому Алекс принимает решение позвонить Бобу и сказать ему, чтобы тот исправил ошибку. В частном случае, когда процесс U_i унитарный, Боб может сделать это следующим образом:



То есть Алекс должен только сообщить Бобу значение $i \in \{0, \dots, n-1\}$, чтобы тот знал, какое исправление применить. И вуаля – у Боба теперь есть система в состоянии ψ :



Вот это она и есть: квантовая телепортация. Вкратце:



Важно здесь то, что Алекс должен отправить Бобу значение i , иначе Боб не сможет исправить ошибку. В таком случае Боб получит только шум, как мы уви-

дим в разделе 6.4.4. Вот почему квантовая телепортация совместима, например, с теорией относительности, которая запрещает передавать сигнал быстрее, чем скорость света. Следовательно, употребляя термин «телепортация», мы на самом деле не имеем в виду волшебное перемещение по какому-то лучу сквозь пространство. Просто в протоколе телепортации один вид информации используется для передачи другого вида информации. Алекс передает некоторые *классические данные* Бобу, и в результате Боб получает *квантовые данные* (т. е. квантовое состояние). Это и вправду удивительно, поскольку, как мы увидим в главе 7, пространство возможных квантовых состояний бесконечно больше количества возможных классических значений.

Упражнение 4.90. Запишите протокол телепортации (4.67):

- 1) в виде диаграммной формулы и
- 2) в алгебраической форме с использованием операций \otimes и \circ .

Мы еще не совсем готовы к тому, чтобы полностью описать квантовую телепортацию. Однако существует вполне классический аналог квантовой телепортации, который можно описать с помощью **отношений**.

Пример 4.91 («классическая» телепортация). Предположим, что у Алекса и Боба есть конверты с карточками, на которых написано 0 или 1. Они не знают, что именно написано, но знают, что их карточки одинаковы. Это недетерминированное состояние можно представить в виде отношения «чашка»:

$$U :: \begin{cases} * \mapsto (0, 0) \\ * \mapsto (1, 1) \end{cases}.$$

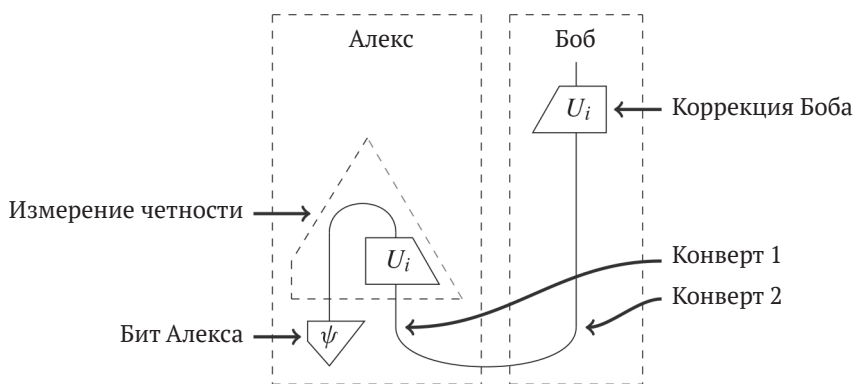
Теперь предположим, что у Алекса имеется бит ψ , который он хочет передать Бобу. Как и прежде, у них есть телефон, но только теперь Алекс располагает классическим битом, поэтому может просто сообщить его значение. С другой стороны, Алекс – немного параноик и не хочет, чтобы потенциальные противники подслушали его и узнали, чему равен ψ . Поэтому вместо того чтобы просто сообщить значение ψ Бобу, он сравнивает четность ψ с четностью бита в своем конверте и сообщает Бобу, совпадают они или нет. Первый случай соответствует эффекту M_0 , второй – эффекту M_1 :

$$M_0 :: \begin{cases} (0, 0) \mapsto * \\ (1, 1) \mapsto * \end{cases}; \quad M_1 :: \begin{cases} (0, 1) \mapsto * \\ (1, 0) \mapsto * \end{cases}.$$

Если биты совпадают, то Боб знает, что бит на карточке в его конверте и есть ψ . Если различны, то ψ – отрицание бита на карточке в конверте. Иными словами, зная результаты измерения, проведенного Алексом, Боб решает, как скорректировать бит в своем конверте:

$$U_0 :: \begin{cases} 0 \mapsto 0; \\ 1 \mapsto 1; \end{cases} \quad U_1 :: \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0. \end{cases}$$

Заметив, что эффект M_i можно переписать в терминах крышки и U_i , мы можем собрать все вместе – получится такая картина:



А это не что иное, как телепортация!

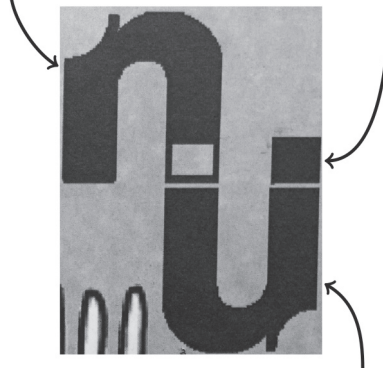
Замечание 4.92. В области компьютерной безопасности пример 4.91 называется *шифрованием по блокноту одноразового использования*. Биты в конвертах соответствуют общему ключу, или «блокноту», измерение четности *шифрует* бит Алекса, а коррекция Боба *дешифрирует* его. Выше мы отметили, что в протоколе телепортации информация одного вида используется для передачи информации другого вида. Эта интерпретация применима и здесь. В этом случае Алекс отправляет *открытые* (т. е. незашифрованные) данные Бобу, а Боб на своей стороне получает *закрытые* (т. е. зашифрованные) данные. Таким образом, аналогия между классической и квантовой телепортациями выглядит следующим образом:

| | Алекс отправляет | Боб принимает | Используемый общий объект |
|---|---------------------|------------------|---------------------------|
| Шифрование по блокноту одноразового использования | открытые данные | закрытые данные | ключ шифрования |
| Квантовая телепортация | классические данные | квантовые данные | квантовое состояние |



Исправление ошибки, выполненное Бобом
(дополняет белый квадратик)

Эффект-крышка Алекса с ошибкой
(см. белый квадратик)



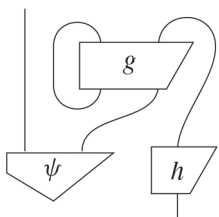
Состояние-чашка, общее для Алекса и Боба

Рис. 4.1 ❖ Телепортация есть всюду, надо только знать, как ее обнаружить. На рисунке показано кафе Cantine в районе площади Таксим в Стамбуле – всячески рекомендуем

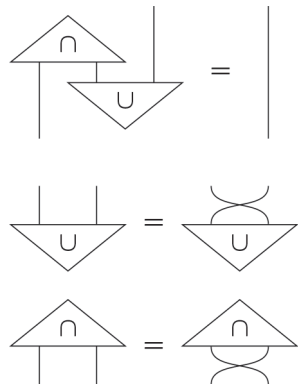
4.5. Итоги: что следует запомнить

1. В *струнных диаграммах* реализовано то, что Шрёдингер считал характерной особенностью квантовой теории: неразделимость. Их можно охарактеризовать двумя эквивалентными способами:

диаграммы, на которых входы могут быть соединены с входами, а выходы с выходами, так что образуются чаше-подобные и крышкоподобные провода:



схемы, в которых каждому типу соответствует специальное *состояние-чашка* и специальный *эффект-крышка*, удовлетворяющие таким условиям:



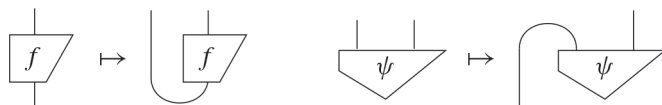
Чтобы установить эквивалентность этих двух характеристик, полагаем



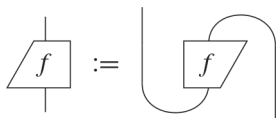
и тогда условия, определяющие состояние-чашку и эффект-крышку, принимают вид *уравнений разгибания*:



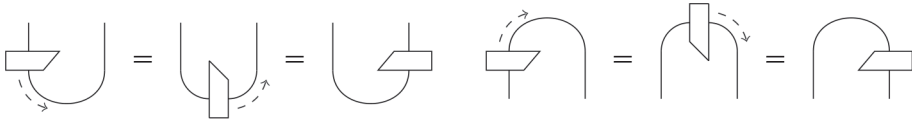
- Для струнных диаграмм существует взаимно однозначное соответствие между процессами и двухкомпонентными состояниями – *двойственность процессов и состояний*, которая устанавливается следующим образом:



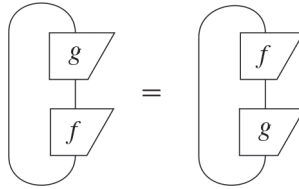
- Язык струнных диаграмм позволяет определить *транспонирование*, которое мы представляем как поворот на 180°:



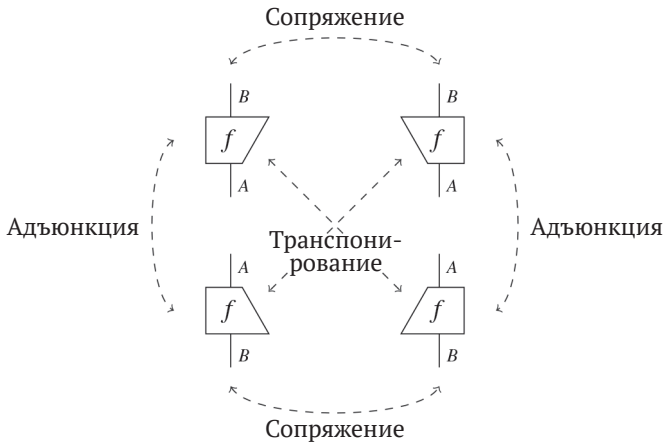
Как следствие получаем, что блоки могут скользить вдоль чашек и крышек:



4. Он также позволяет определить операцию следа (см. ниже), которая дает возможность сопоставлять процессам числа и сохраняет цикличность:

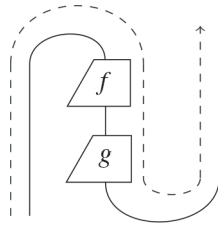


5. Мы также ввели вертикальное отражение диаграмм. Операция *адьюнкции* предлагает интерпретацию вертикального отражения в рамках теории процессов и ассоциирует с каждым состоянием эффект, который проверяет нахождение в этом состоянии. Она позволяет также определить *внутреннее произведение*, *изометрию*, *унитарные процессы*, *положительные процессы* и *проекторы* (см. ниже).
6. Комбинируя вертикальное отражение с транспонированием и поворотом, мы получаем еще одно, горизонтальное отражение, которое называется также *сопряжением*:

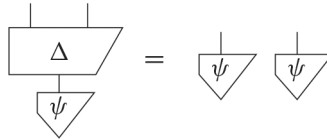


Сопряжение позволяет определить \otimes -положительные двухкомпонентные состояния (см. ниже).

7. Мы выявили несколько «физических» особенностей струнных диаграмм.
- В любой нетривиальной теории всегда существуют неразделимые состояния и прежде всего состояние-чашка. Это состояние устанавливает прямолинейную корреляцию и может создать иллюзию систем, перемещающихся назад во времени:

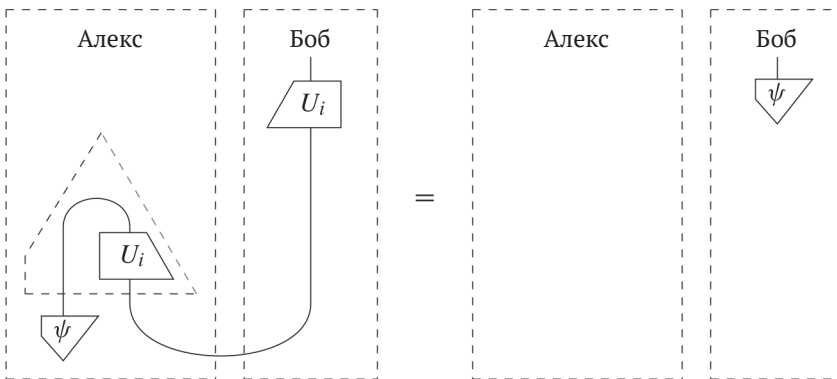


- Не существует операции



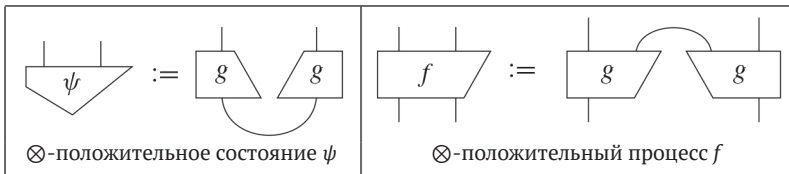
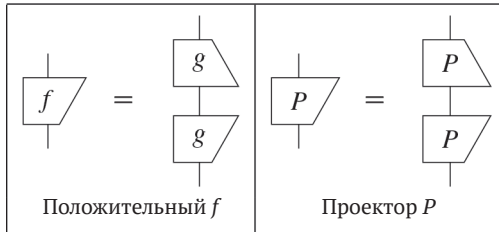
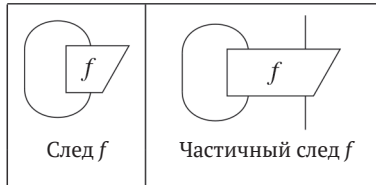
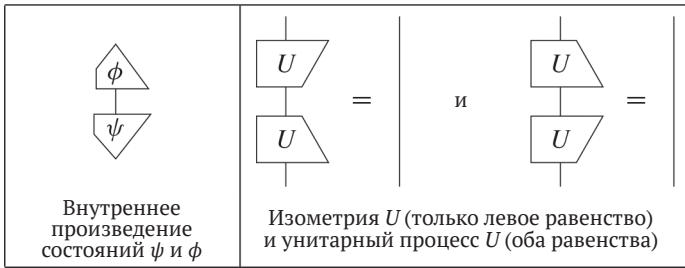
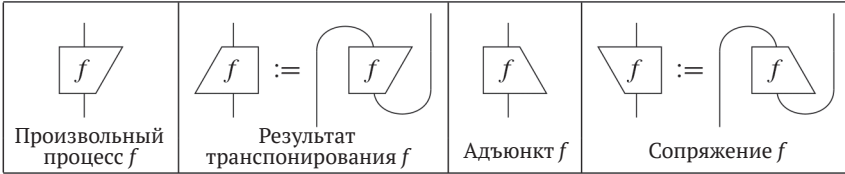
которая копирует все состояния ψ . В частности, состояния, допускающие совместное клонирование изометрическим процессом, должны быть ортогональны.

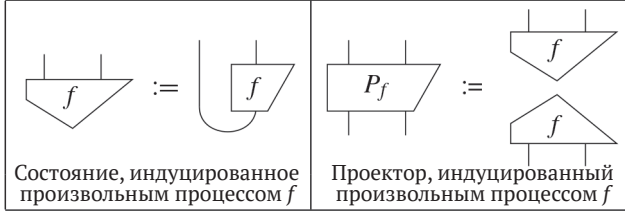
- Мы можем описать телепортацию, что сводится к такому равенству:



8. Мы определили на диаграммах целый ряд понятий и для удобства читателя приведем их сводку:

| | | | |
|-------------------------------|-----------------------------------|------------------------------|------------------------------|
| | | | |
| Состояние-чашка | Эффект-крышка | Произвольное число λ | Число, сопряженное λ |
| | | | |
| Произвольное состояние ψ | Результат транспонирования ψ | Адьюнкт ψ | Сопряженное ψ |





4.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

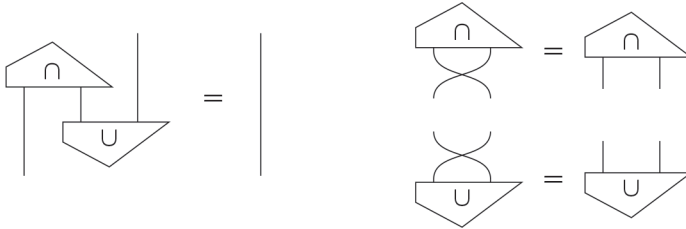
Вслед за дополнительным материалом к предыдущей главе мы теперь рассмотрим, как введенная структура струнных диаграмм определяется в терминах абстрактных тензорных систем, с одной стороны, и симметричных моноидальных категорий – с другой. Во втором случае нам предварительно придется уточнить порядок обращения с чашками и крышками.

4.6.1. Струнные диаграммы в абстрактных тензорных системах*

В абстрактных тензорных системах струнные диаграммы возникают просто путем соединения тензоров U_{AB} и \cap_{AB} , удовлетворяющих условиям:

$$\begin{aligned} \cap_{AB} U^{BC} &= \delta_A^C; & \cap_{BA} &= \cap_{AB}; \\ U^{BA} &= U^{AB}. \end{aligned}$$

Будучи изображены в виде картинок, эти равенства оказываются обычными тождествами для чашек и крышек:



На языке тензоров чашки и крышки иногда называются операциями *поднятия* и *опускания индекса*, поскольку композиция с ними других тензоров приводит к поднятию и опусканию индекса соответственно (т. е. меняет вход на выход или наоборот). Это прием нам уже встречался в разделе 4.2:

$$f_A^{IBC} = f_{AC'}^B U^{C'C}; \quad f_{AC}^{IB} = f_A^{BC'} \cap_{C'C}.$$

Тензор \cap_{AB} играет ключевую роль в *дифференциальной геометрии*, разделе математики, в котором изучаются геометрические свойства кривых поверхностей. Крышка называется *метрикой* пространства. В этом контексте более привычная нотация чашек и крышек выглядит так:

$$g^{\mu\nu} := U^{AB}; \quad g_{\mu\nu} := \cap_{AB}$$

где $\mu := A$ и $\nu := B$. Если внутреннее произведение применяется для вычисления длин векторов в обычном декартовом пространстве, то метрика – для вычисления длин путей в более общих пространствах, которые могут быть искривлены и деформированы. Такие пространства играют центральную роль в общей теории относительности, где гравитационные эффекты приводят к искажениям пространства-времени (отсюда и буква «g» – gravity).

4.6.2. Двойственные типы и самодвойственность*

Чтобы упростить представление чашек и крышек, мы в этой книге предполагаем, что те и другие обладают свойством *самодвойственности*:



или, иными словами, что все наши типы являются *самодвойственными*. Требование о том, что оба типа совпадают, можно ослабить. Вместо того чтобы рассматривать чашки и крышки как основные объекты в определении, мы переместим фокус на «другой тип», участвующий в чашках и крышках, тогда фраза «обладающий чашками и крышками» принимает вид «обладающий двойственными объектами».

Определение 4.93. Для любого типа A тип A^* называется *двойственным* к A , если существуют *состояние-чашка* и *эффект-крышка*:



удовлетворяющие уравнениям разгибания:

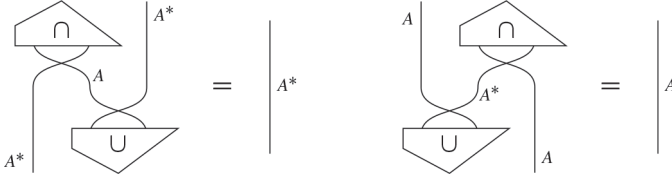
$$\begin{array}{c} \cap \\ | \\ A \end{array} \begin{array}{c} | \\ A^* \\ \cup \end{array} = | \begin{array}{c} A \end{array} \qquad \begin{array}{c} | \\ A^* \\ \cup \end{array} \begin{array}{c} \cap \\ | \\ A \end{array} = | \begin{array}{c} A^* \end{array} \qquad (4.69)$$

Тип A называется *самодвойственным*, если $A = A^*$.

Вспомнив предложение 4.13, в котором мы дали два эквивалентных представления уравнений разгибания, легко видеть, что приведенные выше равенства являются обобщением варианта (ii). Если тип A самодвойственный и дополнительно удовлетворяет условию

$$\begin{array}{c} \cap \\ | \\ \cup \end{array} = \begin{array}{c} | \\ | \\ \cup \end{array} \qquad (4.70)$$

то говорят, что *когерентно самодвойственный*. Если $A \neq A^*$, то это равенство вообще не имеет смысла, потому что типы левой и правой частей не совпадают. Однако простое деформирование равенств (4.69) показывает, что левая часть дает чашку для A^* . В паре с подходящей крышкой это дает



Таким образом, A фактически является двойственным типом для A^* . Следовательно, мы можем положить

$$(A^*)^* := A,$$

и тогда (4.70) принимает вид:

(4.71)

Если $A = A^*$, то у нас есть два способа построить чашку с таким же типом (либо U_A , либо U_{A^*}), поэтому (4.70) говорит, что они должны быть равны.

В математике есть много ситуаций, когда более естественно считать, что сам тип и двойственный ему различаются. Важный пример дают **линейные отображения**, представленные в главе 5. Тем, кто незнаком с векторными пространствами, линейными отображениями и тензорным произведением, имеет смысл сначала прочитать главу 5, а только потом переходить к следующему примеру.

Пример 4.94. Для конечномерного векторного пространства A обозначим A^* пространство, *двойственное* A . Это значит, что элементами $\xi \in A^*$ являются линейные отображения из A в \mathbb{C} . Они образуют векторное пространство, если определить «поточечные» операции сложения и умножения на скаляр:

$$(\xi + \eta)(v) := \xi(v) + \eta(v); \quad (\lambda \cdot \xi)(v) := \lambda \xi(v).$$

Далее любому базису $\{\phi_{ij}\}$ в A соответствует *двойственный базис* $\{\tilde{\phi}_{ij}\}$:

$$\tilde{\phi}_i(\phi_j) := \delta_i^j.$$

Теперь мы можем показать, что тип A^* является двойственным к A , определив состояние-чашку и эффект-крышку. Выбор эффекта-крышки вполне естественный: мы просто берем эффект, который вычисляет $\xi \in A^*$ в векторе $v \in A$:

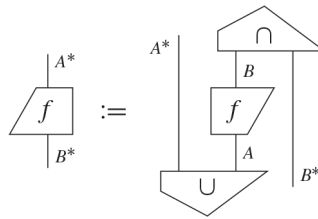
$$\cap_{A, A^*} :: (v \otimes \xi) \mapsto \xi(v)$$

Состояние-чашка получается путем суммирования по базису:

$$\begin{array}{c} | A^* \\ | A \\ \cup \end{array} :: 1 \mapsto \sum_i \tilde{\phi}_i \otimes \phi_i$$

Можно проверить, что эти чашка и крышка удовлетворяют условию (4.69), а также что, в отличие от самодвойственных вариаций, эти чашка и крышка не зависят от выбора базиса $\{\phi_{ij}\}$.

Если транспонировать $f : A \rightarrow B$ относительно этих новых чашек и крышек, то получится новое отображение $f^* : B^* \rightarrow A^*$:

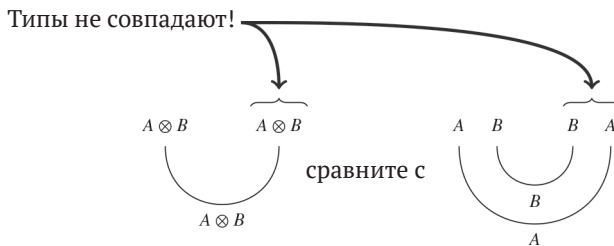


которое иногда называют *линейным оператором транспонирования*. Точнее, f^* переводит элемент B^* в элемент A^* путем композиции его с f :

$$f^*(\xi) := \xi \circ f.$$

Это отображение также не зависит от выбора базиса (в отличие от обычного транспонирования).

Даже если можно выбрать самодвойственный тип A , свобода выбирать A^* иногда бывает полезной. Рассмотрим, к примеру, проблему «вложенных крышек» из раздела 4.2.2.



Эта проблема исчезает, если положить:

$$(A \otimes B)^* := B^* \otimes A^*.$$

Но мы, похоже, частично утрачиваем изящество нотации, если $A \neq A^*$. Вместо того чтобы представлять чашки и крышки отрезками проводов, мы, кажется, вынуждены использовать явные блоки для \cap и \cup , в противном случае образуются провода с разными типами на обоих концах:



Это как-то неправильно! Однако существует элегантный способ наглядно изобразить двойственность. Сначала снабдим провода *направлением*:

$$\begin{array}{c} | \\ \uparrow \\ A \end{array} := \begin{array}{c} | \\ A \end{array} \qquad \begin{array}{c} | \\ \downarrow \\ A^* \end{array} := \begin{array}{c} | \\ A^* \end{array}$$

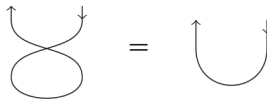
Провода «нормального» типа A рисуются направленными вверх (т. е. «время течет вперед»), а провода двойственного типа A^* – направленными вниз («время течет назад»). В обоих случаях провод помечается просто буквой A , а о том, что это – A или A^* , – мы судим по направлению. Это небольшое изменение нотации снова позволяет представлять чашки и крышки отрезками проводов, только теперь они ориентированные:



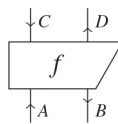
Равенства (4.69) принимают вид:



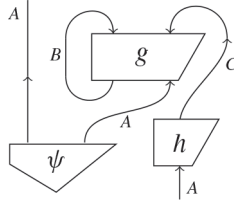
а равенство (4.71) выглядит так:



Отображения с двойственными типами на входе или на выходе изображаются в виде блоков, к которым подходят провода противоположного направления. Например, блок с входным типом $A \otimes B^*$ и выходным типом $C^* \otimes D$ будет выглядеть так:



Точно так же, как раньше нам удалось определить струнные диаграммы, не прибегая к чашкам и крышкам (см. определение 4.18), мы теперь можем определить *ориентированные струнные диаграммы* как диаграммы, в которых разрешено соединять любые два провода, при условии что их типы и направления совместимы:



Таким образом, если мы соединяем вход с выходом, то типы должны быть одинаковы. А если соединяется вход с входом (или выход с выходом), то типы должны быть двойственными. Например, выход h типа C^* соединяется с выходом g типа C .

4.6.3. Инволютивные компактные замкнутые категории*

Компактная замкнутая категория – это симметричная моноидальная категория, в которой для каждого объекта имеется двойственный. На языке категорий это формулируется следующим образом.

Определение 4.95. *Компактной замкнутой категорией* называется такая симметричная моноидальная категория \mathcal{C} , что для любого объекта $A \in \text{ob}(\mathcal{C})$ существует другой объект $A^* \in \text{ob}(\mathcal{C})$ и морфизмы:

$$\epsilon_A : A \otimes A^* \mapsto I \qquad \eta_A : I \mapsto A^* \otimes A$$

такие, что:

$$(\epsilon_A \otimes 1_A) \circ (1_A \otimes \eta_A) = 1_A (1_{A^*} \otimes \epsilon_A) \circ (\eta_A \otimes 1_{A^*}) = 1_{A^*}. \tag{4.72}$$

Замечание 4.96. Прилагательное «замкнутый» означает, что для любых двух объектов A и B существует специальный объект $[A \mapsto B]$, состояния которого $\psi : I \mapsto [A \mapsto B]$ кодируют морфизмы в $\mathcal{C}(A, B)$. Например, в категории, объектами которой являются множества, а морфизмами – функции, $[A \mapsto B]$ – это множество всех функций из A в B , тогда как в категории, объектами которой являются векторные пространства, а морфизмами – линейные отображения, $[A \mapsto B]$ – это векторное пространство линейных отображений из A в B . Словосочетание «компактные замкнутые» означает, что эти специальные объекты имеют вид

$$[A \mapsto B] := A^* \otimes B,$$

т. е. что в этой категории имеет место двойственность процессов и состояний.

Адьюнкты тоже можно определить в терминах теории категорий.

Определение 4.97. *Инволютивным функтором (dagger functor)* для симметричной моноидальной категории называется операция \dagger , которая не изменяет объектов:

$$A^\dagger := A,$$

инвертирует морфизмы:

$$(f : A \mapsto B)^\dagger := f^\dagger : B \mapsto A,$$

является инволютивной:

$$(f^\dagger)^\dagger = f$$

и сохраняет структуру симметричной моноидальной категории:

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger; \quad (f \otimes g)^\dagger = f^\dagger \otimes g^\dagger; \quad \sigma_{A,B}^\dagger = \sigma_{B,A}.$$

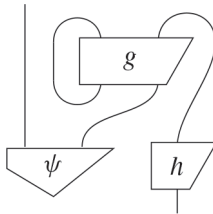
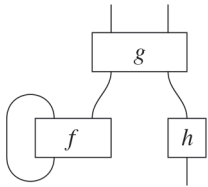
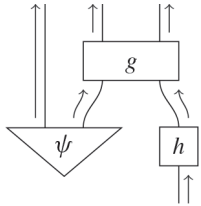
Инволютивной компактной замкнутой категорией называется компактная замкнутая категория \mathcal{C} с инволютивным функтором, удовлетворяющая условию

$$\epsilon_A^\dagger = \eta_{A^*}.$$

Теорема 3.49 устанавливала корректность и полноту для схемных диаграмм относительно симметричных моноидальных категорий. То же самое справедливо для струнных диаграмм и инволютивных компактных замкнутых категорий.

Теорема 4.98. Струнные диаграммы корректны и полны относительно инволютивных компактных замкнутых категорий. Иначе говоря, доказать, что два морфизма f и g равны, используя определение инволютивной компактной замкнутой категории, можно тогда и только тогда, когда они выражаются одной и той же струнной диаграммой.

Теперь мы можем расширить таблицу из раздела * 3.6.3.

| | | |
|---|--|--|
| <p>Струнные диаграммы</p>  <p>т. е. все на все</p> | <p>Диаграмма «общего вида»</p>  <p>т. е. выход подается на вход</p> | <p>Схемная диаграмма</p>  <p>т. е. имеет причинно-следственную структуру</p> |
| <p>АТС с g-метрикой</p> | <p>АТС</p> | <p>АТС без циклов</p> |
| <p>инволютивная компактная замкнутая</p> | <p>СМК со следом</p> | <p>СМК</p> |

4.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Способ композиции двухкомпонентных проекторов, обсуждавшийся в разделе 4.3.7, заимствован из работы Соеске (2003) и стал формальной основой для первого формального графического представления квантовой телепортации. И хотя будет справедливо сказать, что эта работа положила начало диаграммному подходу к изображению квантовых процессов, редактор журнала *Physical Review Letters*

отказался ее публиковать (даже без консультаций с рецензентами) на том основании, что она слишком «умозрительная». Идея о том, что эти двухкомпонентные проекторы следует интерпретировать в терминах чашек, крышек и блоков, как на рис. 4.54, впервые появилась в работах Abramsky and Coecke (2005, 2014a). Независимый топологический анализ квантовой телепортации приведен в работе Kauffman (2005).

Но на самом деле чашки и крышки появились гораздо раньше, в диаграммном исчислении Пенроуза для абстрактных тензорных систем (Penrose, 1971), где представляли метрические тензоры в геометрии пространства-времени. Однако последующее развитие струнных диаграмм и их интерпретация в терминах математических моделей происходили в основном в недрах сообщества, занимающегося теорией категорий. Примерно в то же время, когда была написана работа Пенроуза, струнные диаграммы появились в работе Келли, где было введено понятие компактных замкнутых категорий (Kelly, 1972), которое, как сказано в разделе* 4.6.3, является вариантом изложения процессной теории, допускающей струнные диаграммы, в терминах теории категорий. Использованием дополнительных блоков, помимо чашек и крышек, в контексте категорий мы обязаны Йеттеру (см., например, Freyd and Yetter, 1989), который употреблял название «цветные клубки» (coloured tangles).

Двойственность процессов и состояний в контексте квантовой теории известна под названием изоморфизма Чоя–Жамиолковского (Jamiołkowski, 1972; Choi, 1975). На самом деле изоморфизмы, предложенные Жамиолковским и Чоем, не эквивалентны. В этой книге мы в основном пользуемся изоморфизмом Чоя, который зависит от базиса. Изоморфизм же Жамиолковского от базиса не зависит и происходит от чашек и крышек в примере* 4.94.

Инволютивные компактные замкнутые категории были определены в работе Abramsky and Coecke (2004, 2005), чтобы аксиоматизировать способ композиции двухкомпонентных проекторов, что привело к изложению основ квантовой теории в терминах теории категорий. Примерно в то же время аналогичные идеи были высказаны в работе Baez (2006). Идея асимметричных блоков для представления операций транспонирования и адьюнкции заимствована из работы Selinger (2007). Как математические сущности инволютивные компактные замкнутые категории уже встречались в работе Baez and Dolan (1995) в качестве частного случая более общей конструкции n -категорий. Теорема 4.98 считается фольклором, а ее строгая формулировка приведена в работе (2007), где сказано, что «неявное доказательство» впервые было дано в работе (Kelly and Laplaza, 1980).

Понятие \otimes -положительности было введено в работе Selinger (2007) под названием (абстрактной) полной положительности. Вариант теоремы о невозможности клонирования, который представлен в теореме 4.85 и предшествовал появлению понятия квантовой информации, был независимо доказан в работах Dieks (1982) и Wootters and Zurek (1982). Вариант, представленный в теореме 4.84, который опирается на существование чашек, а не на использование унитарности, взят из работы Abramsky (2010).

Слово «телепортация» впервые употребил в 1931 году американский исследователь «непознанного» Чарльз Форт в книге *Lo!*¹, состоящей из двух частей, первая

¹ В русском переводе вышла под названием «Вулканы небес». – Прим. перев.

из которых целиком посвящена телепортации. Однако по-настоящему эта идея заиграла, когда нашла применение в качестве средства транспортировки в саге Джина Родденберри «Звездный путь» о приключениях корабля «Энтерпрайз». Квантовая телепортация впервые была описана в работе Bennett et al. (1993), а ее первая экспериментальная реализация – в работе Bouwmeester et al. (1997). Диаграммное представление квантовой телепортации приведено в работе Coecke et al. (2008b), а более детальное изложение можно найти в работе Stay and Vicary (2013).

Наблюдение по поводу обращения хода времени в разделе 4.4.3 взято из работы Coecke (2003, 2014a), а экспериментальное моделирование полученных в ней результатов описано в работе Laforest et al. (2006). Идея о том, что чашки и крышки можно использовать для моделирования путешествий во времени, заимствована из той же работы и впервые сформулирована в таком виде в работе Svetlichny (2009). Позже она была подхвачена в работе Lloyd et al. (2011), которая получила много внимания от СМИ, причем некоторые заголовки кричали о том, что путешествие во времени уже осуществилось. Гораздо раньше другая теория квантовых путешествий во времени появилась в работе Deutsch (1991).

Лучший обзор различных вариантов моноидальных категорий и связанных с ними диаграммных понятий – работа Selinger (2011b). Тем, кого интересует дополнительная информация об использовании струнных диаграмм в контексте физики, математической логики и топологии, мы рекомендуем работу Baez and Stay (2011), а в контексте физики и лингвистики – работу Heunen et al. (2012a). Обо всем спектре (преимущественно) диаграммных конструкций, используемых в многомерной теории категорий, см. работу Leinster (2004).

Цитата, приведенная в начале этой главы, взята из работы Schrödinger (1935).

Глава 5

От диаграмм к гильбертову пространству

Я хочу сделать признание, которое может показаться аморальным: «Я больше абсолютно не верю в гильбертово пространство».

– Джон фон Нейман,
письмо Гаррету Биркгофу, 1935

Мы уже видели, что процессы, описываемые струнными диаграммами, демонстрируют некоторые особенности, напоминающие квантовые. Естественно задать вопрос, сколько дополнительной работы нужно проделать, чтобы перейти от струнных диаграмм к гильбертовым пространствам и линейным отображениям – тому математическому инструментарию, который использовал фон Нейман для формулировки квантовой теории в конце 1920-х годов. Ответ: не так уж много.

Начнем с рассмотрения такого вопроса: что означает, что два процесса равны? Во многих процессных теориях достаточно, чтобы они были согласованы на относительно небольшом множестве состояний. Это естественно приводит нас к понятию *базиса*, а для выделения особенно удобных базисов – *ортонормированных* – мы можем воспользоваться адьюнкцией. Если все типы допускают базис, то любой процесс можно полностью описать набором чисел, который называется его *матрицей*.

Такая матрица однозначно определяет конкретный процесс, но чтобы любая матрица представляла некоторый процесс, необходима дополнительная структура. Поэтому мы разрешим объединять процессы с одинаковыми входными и выходными проводами в один процесс – их *сумму*. Если процессная теория допускает струнные диаграммы, если для каждого типа имеется ортонормированный базис (ОНБ) и если определена операция сложения процессов, то можно описать суммы, последовательную и параллельную композиции, транспонирование, сопряжение и адьюнкцию в терминах операций над матрицами. Мы будем называть это *матричным исчислением* процессной теории.

Таким образом, добавив ОНБ и суммы, мы почти воспроизвели всю мощь *линейной алгебры*, обобщив ее в том смысле, что на числа λ по-прежнему налагается очень мало ограничений (в частности, не требуется, чтобы они были элементами некоторого поля, как, например, вещественные или комплексные числа). На са-

мом деле вполне можно определить матричное исчисление для теории отношений, числами в нем будут булевы величины.

Последний шаг на пути к гильбертовым пространствам и линейным отображениям – потребовать, чтобы числа в процессной теории были *комплексными числами*. То есть мы определяем **линейные отображения** как процессную теорию, допускающую струнные диаграммы и такую, что:

- 1) для каждого типа существует конечный ОНБ;
- 2) для любого $n \in \mathbb{N}$ существует тип с ОНБ размера n ;
- 3) процессы одного и того же типа можно складывать;
- 4) числами являются комплексные числа.

Системные типы в этой процессной теории называются *гильбертовыми пространствами*. Знакомым с формализмом гильбертовых пространств в квантовой теории сразу бросится в глаза отсутствие какого-либо упоминания *тензорного произведения* гильбертовых пространств и *(мульти)линейности* отображения. Причина в том, что язык струнных диаграмм дает нам это задаром!

Наше изложение гильбертовых пространств и линейных отображений сильно отличается от общепринятого «восходящего» подхода. Обычно начинают с малых объектов, а именно векторов, затем определяют множества векторов со специальными свойствами – векторные пространства, а уже потом их частный случай – гильбертовы пространства. Для превращения всего этого добра в процессную теорию нужно еще немало потрудиться: определить линейные и билинейные отображения, композицию и тензорное произведение, пользуясь всем арсеналом теории множеств и алгебры. Эти теоретико-множественные определения по духу своему являются *сведением*: они определяют большее в терминах меньшего. Этим они очень напоминают мечту специалиста по физике элементарных частиц: построить «теорию всего», которая объясняла бы мир исключительно в терминах его мельчайших частей. Мы же стремимся понять сущность в терминах ее взаимодействия с другими сущностями. Поэтому имеет смысл принять «нисходящий» подход, при котором определение процессной теории **линейных отображений** начинается с того, как устроена композиция объектов, а потом уже восполняются детали.

Но ведь это книга о применении диаграмм для рассуждений о квантовых процессах, так причем же здесь гильбертовы пространства? На самом деле в главе 8 такие вещи, как существование ОНБ и суммы, будут учтены в определении нового диаграммного примитива, а в главе 9 нечто похожее будет сделано, чтобы учесть тот факт, что в одной системе может быть несколько ОНБ. Тем не менее есть три веские причины включить в книгу введение в гильбертовы пространства.

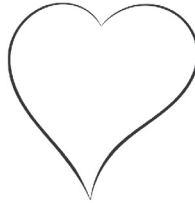
1. Читателям, знакомым с описанием квантовой теории с помощью гильбертовых пространств, будет полезно посмотреть, как диаграммные концепции представляются на языке гильбертовых пространств, поскольку этот язык они знают.
2. Читатели, незнакомые с описанием квантовой теории с помощью гильбертовых пространств, смогут перевести то, что узнают из этой книги, на язык, используемый в большинстве других учебников по квантовой теории.
3. Иногда описанный в этом разделе смешанный подход – сочетание диаграммных рассуждений с суммами – удобен для вычислений. Такой гибрид уже доказал свою полезность в некоторых областях чистой математики, например в теории узлов, где встречаются равенства вида:

$$\times = \lambda \left| \right| + \lambda^{-1} \cup$$

И это еще не все. Даже если читателя вообще не интересует формулировка квантовой теории в терминах гильбертовых пространств, он все равно может спросить: «Что все-таки можно доказать с помощью струнных диаграмм?» И если говорить о процессных равенствах, то ответ на этот вопрос прозвучит неожиданно: «Все, что можно доказать с помощью гильбертовых пространств!»

В терминах математической логики это означает, что существует *теорема о полноте* гильбертовых пространств относительно струнных диаграмм. Что это значит, мы подробно объясним в разделе 5.4.1.

С другой стороны, струнные диаграммы обременены куда меньшим багажом, чем гильбертовы пространства, поэтому оставляют больше места для поиска альтернативы гильбертовым пространствам в роли формальной основы квантовой теории. Таким образом, два, на первый взгляд, не связанных между собой события – отказ от формализма квантовой теории на основе гильбертовых пространств (как того хотел фон Нейман) и принятие неразделимости в качестве критически важной особенности квантовой теории (как настаивал Шрёдингер) – идут в нашей истории рука об руку:



5.1. БАЗИСЫ И МАТРИЦЫ

Теперь мы покажем, как стандартные понятия линейной алгебры, прежде всего базисы и матрицы, возникают в некоторых процессных теориях и как специальные процессы и операции, определенные в предыдущих главах для диаграмм, трансформируются в стандартные концепции линейной алгебры.

В этом разделе предполагается, что процессные теории допускают струнные диаграммы и что для каждого системного типа имеется нулевой процесс.

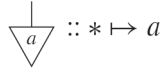
5.1.1. Базис для типа

Многие изученные до сих пор процессы обладают следующим свойством:

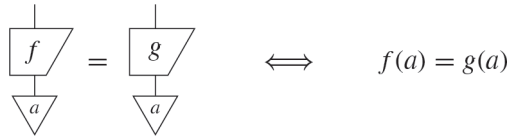
$$\left(\text{для всех } \psi \downarrow : \begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \psi \downarrow \end{array} = \begin{array}{c} \downarrow \\ \boxed{g} \\ \downarrow \\ \psi \downarrow \end{array} \right) \Rightarrow \begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} = \begin{array}{c} \downarrow \\ \boxed{g} \\ \downarrow \end{array} \quad (5.1)$$

т. е. если два процесса делают одно и то же для любого состояния, то они равны. Иными словами, процесс однозначно определяется тем, что он делает с состояниями.

Примеры 5.1. Теории **функций** и **отношений** обладают свойством (5.1). Для **функций** мы в примере 3.35 видели, что состояния типа A



находятся во взаимно однозначном соответствии с элементами $a \in A$, которое устанавливается следующим образом:

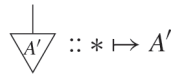


Следовательно, мы можем переписать (5.1) в виде:

$$(\text{для всех } a \in A : f(a) = g(a)) \Rightarrow f = g,$$

что, конечно, правильно для любых функций f и g .

Для **отношений** мы в примере 3.36 видели, что состояния типа A



находятся во взаимно однозначном соответствии с подмножествами $A' \subseteq A$. Однако в свете (5.1) рассматривать все состояния $A' \subseteq A$ излишне. Если ограничиться только одноэлементными подмножествами, то уже будем иметь:

$$(\text{для всех } a \in A : R(a) = S(a)) \Rightarrow R = S.$$

То есть отношение однозначно определяется тем, что оно делает с одноэлементными подмножествами.

Как мы только что видели на примере **отношений**, для однозначного определения процесса не всегда необходимо знать, что он делает с каждым состоянием. Иногда достаточно знать, как он воздействует только на некоторое подмножество всех состояний.

Определение 5.2. *Базисом* типа A называется минимальное множество состояний

$$\mathcal{B} := \left\{ \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array}, \dots, \begin{array}{c} \downarrow \\ \triangle \\ n \end{array} \right\}$$

такое, что для любых процессов f и g

$$\left(\text{для всех } \downarrow i \in \mathcal{B} : \begin{array}{c} \downarrow \\ \text{---} \\ \text{f} \\ \text{---} \\ \downarrow \\ \text{---} \\ \text{i} \end{array} = \begin{array}{c} \downarrow \\ \text{---} \\ \text{g} \\ \text{---} \\ \downarrow \\ \text{---} \\ \text{i} \end{array} \right) \Rightarrow \begin{array}{c} \downarrow \\ \text{---} \\ \text{f} \\ \text{---} \\ \downarrow \\ \text{---} \end{array} = \begin{array}{c} \downarrow \\ \text{---} \\ \text{g} \\ \text{---} \\ \downarrow \\ \text{---} \end{array} \quad (5.2)$$

где слово «минимальное» означает, что из \mathcal{B} невозможно удалить ни одного состояния без нарушения условия (5.2). *Размерностью* $\dim(A)$ типа A называется минимальный размер базиса A .

Замечание* 5.3. В любой процессной теории без аномалий, например в теории **отношений**, все базисы для конкретной системы имеют одинаковый размер. В таком случае мы можем просто определить $\dim(A)$ как размер произвольного базиса. В теории **линейных отображений** этот результат часто называют *теоремой о размерности*.

Упражнение 5.4. Докажите, что для множества A в теории **отношений** одноэлементные множества

$$\mathcal{B}_A := \left\{ \downarrow a \mid a \in A \right\}$$

образуют базис, т. е. при удалении из \mathcal{B}_A любого элемента оно перестает быть базисом. Также докажите, что все базисы имеют такой вид и, следовательно, размерность множества A в теории **отношений** равна числу элементов в нем.

Далее мы будем использовать обозначение

$$\left\{ \downarrow i \right\}_i$$

как сокращенную форму записи

$$\left\{ \downarrow 1, \dots, \downarrow n \right\}$$

Лучшими базисами являются те, чьи состояния идеально различимы с помощью испытаний. То есть при проверке того, находится ли i -е состояние в j -м состоянии, утвердительный ответ будет получен тогда и только тогда, когда $i = j$. Мы будем использовать для таких множеств состояний (i , в частности, базисов) специальное название.

Определение 5.5. Множество состояний

$$\mathcal{A} := \left\{ \downarrow i \right\}_i$$

называется *ортонормированным*, если для любых i, j имеет место равенство

$$\begin{array}{c} \triangleup j \\ | \\ \triangleleft i \end{array} = \delta_i^j \tag{5.3}$$

где δ_i^j – символ Кронекера:

$$\delta_i^j = \begin{cases} \text{пустая диаграмма} & \text{если } i = j \\ 0 & \text{в противном случае} \end{cases}$$

Если \mathcal{A} образует базис, то он называется *ортонормированным базисом (ОНБ)*.

Напомним (см. раздел 4.3.3), что внутреннее произведение в равенстве (5.3) можно интерпретировать как меру «перекрывания» состояний. В таком случае ОНБ можно интерпретировать как базис, элементы которого не перекрываются, как в следующем примере.

Пример 5.6. В примере 4.50 мы видели, что внутреннее произведение двух состояний в теории **отношений** равно 1 тогда и только тогда, когда они пересекаются. Поскольку пересечение любых двух (различных) одноэлементных множеств пусто, то однозначно определенные базисы из упражнения 5.4 ортонормированные:

$$\begin{array}{c} \triangleup b \\ | \\ \triangleleft a \end{array} = \begin{cases} \text{пустая диаграмма} & \text{если } a = b \\ \emptyset & \text{если } a \neq b \end{cases}$$

Не всегда ОНБ определен однозначно.

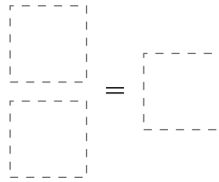
Пример 5.7. В разделе 5.3 мы увидим, что **линейные отображения** допускают много различных ОНБ для одного системного типа и нет никакого специального «предпочтительного» ОНБ. Этот факт очень важен для многих квантовых явлений.

Некоторые ОНБ даже невидимы.

Пример 5.8. Поскольку для любых состояний ψ и ϕ системы A имеет место импликация:

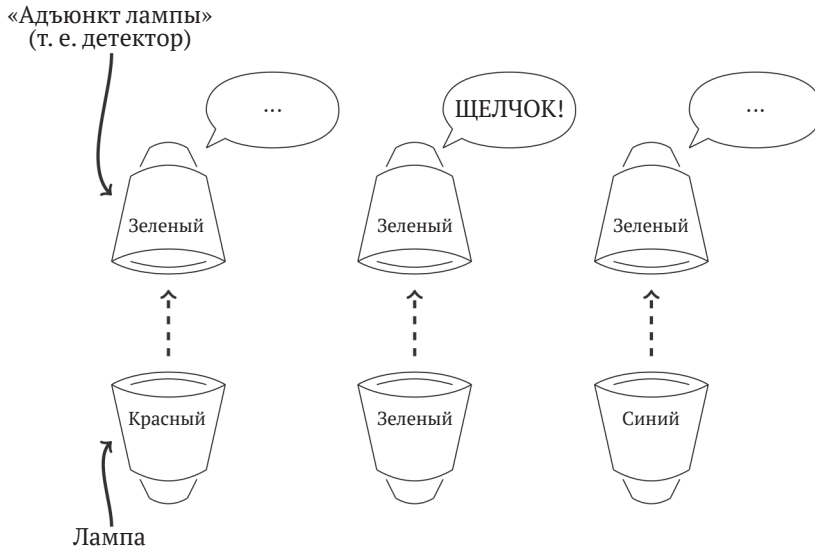
$$\begin{array}{c} \triangleup \psi \\ | \\ \text{пустая диаграмма} \end{array} = \begin{array}{c} \triangleup \phi \\ | \\ \text{пустая диаграмма} \end{array} \implies \begin{array}{c} \triangleup \psi \\ | \\ \text{пустая диаграмма} \end{array} = \begin{array}{c} \triangleup \phi \\ | \\ \text{пустая диаграмма} \end{array}$$

то пустые диаграммы образуют ОНБ для типа «без проводов», поскольку в этом случае ортонормированность означает просто:

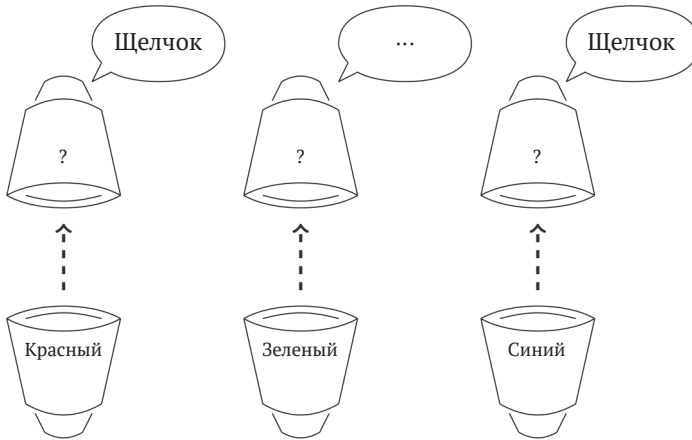


А бывают разноцветные ОНБ.

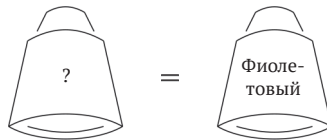
Пример 5.9. Рассмотрим процессную **теорию лампы и детекторов**, в которой состояниями являются лампы, дающие свет определенного цвета, а эффектами – детекторы, которые щелкают, обнаруживая свет определенного цвета. Числа возникают при композиции лампы с детектором. Число 0 означает «щелчка нет», т. е. ничего не обнаружено, а 1 – «самый громкий щелчок», т. е. обнаружена максимальная яркость. При нашей интерпретации адъюнкции адъюнктом лампы является детектор света того же цвета. В таком случае красная, зеленая и синяя лампы «ортонормированны», потому что никогда не обнаружат свет друг друга:



и при этом они образуют базис. Например, предположим, что имеется некоторый неизвестный детектор и происходит следующее:



Тогда мы можем заключить, что



Для базиса общего вида проверка условия минимальности из определения 5.2 может оказаться нетривиальной. По счастью, в случае ОНБ это условие выполняется автоматически.

Предложение 5.10. Если ортонормированное множество состояний типа \mathcal{A} удовлетворяет условию (5.2) для любой пары процессов, то оно должно быть минимальным и, следовательно, является ОНБ.

Доказательство. Пусть

$$\mathcal{A} = \left\{ \begin{array}{c} \downarrow \\ i \end{array} \right\}_i$$

– ортонормированное множество состояний, удовлетворяющее условию (5.2). Предположим, что оно не минимально, т. е. существует такое состояние i , что множество

$$\mathcal{A}' := \mathcal{A} - \left\{ \begin{array}{c} \downarrow \\ i \end{array} \right\}$$

все еще удовлетворяет условию (5.2). Прежде всего отметим, что эффект i не может быть равен нулевому (во избежание путаницы он изображен здесь как $\boxed{0}$), потому что

$$\begin{array}{c} \triangle \\ | \\ i \\ | \\ \triangle \\ | \\ i \end{array} = 1 \neq 0 = \begin{array}{c} \square \\ | \\ 0 \\ | \\ \triangle \\ | \\ i \end{array}$$

Однако поскольку состояния в \mathcal{A} ортонормированные, то для любого $j \neq i$ имеем:

$$\begin{array}{c} \triangle \\ | \\ i \\ | \\ \triangle \\ | \\ j \end{array} = 0 = \begin{array}{c} \square \\ | \\ 0 \\ | \\ \triangle \\ | \\ j \end{array}$$

Но тогда из (5.2) следует, что

$$\begin{array}{c} \triangle \\ | \\ i \\ | \\ \square \end{array} = \begin{array}{c} \square \\ | \\ 0 \\ | \\ \square \end{array}$$

И мы пришли к противоречию. □

Теперь самое время сделать одно предупреждение, касающееся ОНБ.

▲ Предупреждение 5.11. В разделе 3.4.3 мы ввели понятие равенства процессов «с точностью до числа» и показали, что отношение \approx хорошо согласуется с диаграммами. А вот с ОНБ оно уживается плохо. Даже если мы докажем, что для всех i

$$\begin{array}{c} | \\ \square \\ | \\ f \\ | \\ \triangle \\ | \\ i \end{array} \approx \begin{array}{c} | \\ \square \\ | \\ g \\ | \\ \triangle \\ | \\ i \end{array} \tag{5.4}$$

это не будет означать, что

$$\begin{array}{c} | \\ \square \\ | \\ f \\ | \\ \square \end{array} \approx \begin{array}{c} | \\ \square \\ | \\ g \\ | \\ \square \end{array}$$

Чтобы это утверждение было истинным, каждый экземпляр равенства (5.4) должен выполняться с точностью до одного и того же числа, иначе мы можем и не найти такую одну пару чисел λ, μ , для которой $\lambda f = \mu g$. Например, если f и g – эффекты, то это просто означает, что f и g ненулевые на одном и том же множестве ортонормированных состояний.

Как правило, все базисы в этой книге будут ортонормированными, но есть одно важное исключение: *томография* (см. раздел 7.4). Чтобы учесть и его, мы в последующих разделах докажем ряд результатов для базисов общего вида, не обязательно ортонормированных. Будет также удобно (а иногда и необходимо) выбирать базис, состоящий из самосопряженных состояний. Если базис самосопряженный, то соответствующие эффекты также самосопряженные. Мы будем обозначать самосопряженные состояния и эффекты следующим образом:

$$\begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} := \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} = \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} \quad \text{и} \quad \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ i \end{array} := \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ i \end{array} = \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ i \end{array}$$

Пример* 5.12. В линейной алгебре самосопряженными являются ОНБ, матрица которых содержит только вещественные числа. Канонический пример:

$$\begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \\ & & & & 1 \end{pmatrix}, \dots, \begin{pmatrix} 0 & & & \\ & \vdots & & \\ & & 0 & \\ & & & 1 \end{pmatrix}$$

В разделе 5.2.3 мы увидим, что любой ОНБ можно преобразовать в самосопряженный, просто правильно выбрав чашки и крышки (в общем случае это можно сделать не единственным способом). Пример, когда приходится иметь дело с несамосопряженным базисом, – изучение нескольких различных базисов одной и той же системы. В общем случае не всегда возможно выбрать чашку и крышку так, чтобы все базисы одновременно оказались самосопряженными.

Пример* 5.13. В квантовых вычислениях X -базис, Y -базис и Z -базис для кубитов обладают тем свойством, что только два из трех можно одновременно сделать самосопряженными.

5.1.2. Матрица процесса

Имея базисные состояния, мы часто можем доказать некоторые утверждения о процессах, доказав что-то для состояний. Однако при наличии адьюнктов мы также имеем ассоциированные базисные эффекты, так что есть возможность получить лучше. Чтобы доказать равенство процессов, достаточно просто взглянуть на числа.

Теорема 5.14. Предположим, что \mathcal{B} – базис A , а \mathcal{B}' – базис B . Тогда для любых процессов f и g с входным типом A и выходным типом B имеем:

$$\left(\text{для всех } \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} \in \mathcal{B}, \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ j \end{array} \in \mathcal{B}' : \begin{array}{c} \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} \\ f \\ \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} \end{array} = \begin{array}{c} \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} \\ g \\ \begin{array}{c} \downarrow \\ \triangle \\ \downarrow \\ i \end{array} \end{array} \right) \Rightarrow \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} f = \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} g \quad (5.5)$$

Доказательство. Будем доказывать утверждение отдельно для каждого базиса. Сначала возьмем произвольное состояние j из \mathcal{B}' . Тогда для всех состояний i из \mathcal{B} , если взять:

$$\begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} f = \begin{array}{c} \triangle \\ \uparrow \\ \triangle \\ \uparrow \\ j \end{array} g$$

то, поскольку \mathcal{B} – базис, отсюда следует, что

$$\begin{array}{c} \triangle j \\ | \\ \square f \\ | \end{array} = \begin{array}{c} \triangle j \\ | \\ \square g \\ | \end{array}$$

и, применив к обеим частям адъюнкцию, получаем:

$$\begin{array}{c} | \\ \square f \\ | \\ \triangle j \end{array} = \begin{array}{c} | \\ \square g \\ | \\ \triangle j \end{array}$$

Это равенство имеет место для всех $j \in \mathcal{B}'$, поэтому, т. к. \mathcal{B}' – базис, имеем:

$$\begin{array}{c} | \\ \square f \\ | \end{array} = \begin{array}{c} | \\ \square g \\ | \end{array}$$

Снова применив адъюнкцию к обеим частям, заключаем, что $f = g$. □

Упражнение 5.15. Покажите, что если потребовать еще, чтобы \mathcal{B} и \mathcal{B}' были минимальны, т. е. если при выполнении условия (5.5) имеет место (5.2) для \mathcal{B} и \mathcal{B}' , то верна и теорема, обратная теореме 5.14.

Если базисы в теореме 5.14 ортонормированные, то числа, однозначно определяющие процесс, имеют хорошо знакомое название.

Определение 5.16. Числа

$$\mathbf{f} := \left(f_i^j \mid \begin{array}{c} | \\ \triangle i \\ | \end{array} \in \mathcal{B}, \begin{array}{c} \triangle j \\ | \end{array} \in \mathcal{B}' \right)$$

где \mathcal{B} и \mathcal{B}' – ортонормированные базисы и

$$f_i^j := \begin{array}{c} \triangle j \\ | \\ \square f \\ | \\ \triangle i \end{array} \tag{5.6}$$

называются *матрицей* f . Числа f_i^j называются *элементами матрицы*.

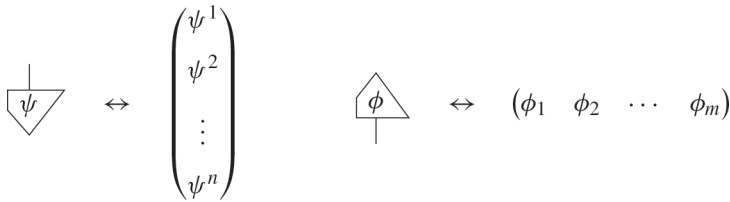
Обычно мы будем одинаково обозначать процесс f и его матрицу, но если потребуется провести различие между тем и другим, то матрица будет обозначаться полужирным шрифтом – \mathbf{f} .

В школе вы, наверное, встречались с такой записью матрицы:

$$\begin{pmatrix} f_1^1 & f_2^1 & \cdots & f_m^1 \\ f_1^2 & f_2^2 & \cdots & f_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ f_1^n & f_2^n & \cdots & f_m^n \end{pmatrix}$$

Обратите внимание, что у каждого элемента матрицы имеется верхний индекс строки (который берется из элемента выходного базиса) и нижний индекс столбца (который берется из элемента входного базиса). Такая «тензорная» нотация (см. раздел* 3.6.1) окажется удобной при наличии нескольких входных или выходных проводов.

Матрица процесса с входом A и выходом B имеет $\dim(A)$ столбцов и $\dim(B)$ строк. В примере 5.8 мы видели, что у типа «без проводов» базис состоит из одного элемента. Поэтому состояниям соответствуют матрицы размера $n \times 1$ – *векторы-столбцы*, а эффектам – матрицы размера $1 \times m$ – *векторы-строки*:



Понятно, что числам соответствуют матрицы размера 1×1 :

$$(\lambda)$$

но так мы их обычно не записываем.

Хотя, как правило, матрицы ассоциируются с линейными отображениями, в действительности они представляют собой более общий объект. Например, это удобное альтернативное представление отношений.

Пример 5.17. Ранее мы видели, что с каждым типом в теории **отношений** связан однозначно определенный ОНБ, образованный одноэлементными множествами, а в примере 3.36 мы показали, что существует только два числа:

$$0 := \emptyset \text{ («невозможно»)} \quad 1 := \boxed{} \text{ («возможно»)}$$

Тогда имеем

$$\begin{array}{c} \triangle b \\ | \\ \square R \\ | \\ \triangle a \end{array} = \begin{cases} 1 & \text{если } R :: a \mapsto b \\ 0 & \text{в противном случае} \end{cases}$$

Очевидно, что эти числа полностью характеризуют R , поскольку они точно определяют пары (a, b) такие, что $R :: a \mapsto b$, соотнося с ними число 1. Мы можем пометить столбцы матрицы R элементами A , а ее строки – элементами B . Тогда 1 будет находиться в элементах на пересечении строк и столбцов, которые связаны данным отношением, а остальные элементы будут равны 0.

Эту матрицу иногда называют *матрицей смежности* R .

Мало того что матрицами можно представлять процессы, так еще и диаграммные операции транспонирования, сопряжения и адьюнкции соответствуют знакомым операциям над матрицами.

Теорема 5.18. Пусть f – процесс, с которым ассоциирована матрица \mathbf{f} . Матрицей процесса f^\dagger является *эрмитово-сопряженная матрица* \mathbf{f}^\dagger , определенная следующим образом:

$$R :: \begin{cases} a_1 \mapsto b_4 \\ a_2 \mapsto b_2 \\ a_2 \mapsto b_3 \\ a_3 \mapsto b_4 \end{cases} \quad \Leftrightarrow \quad \begin{matrix} a_1 & a_2 & a_3 \\ b_1 & \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{matrix}$$

Доказательство. Элементы матрицы f^\dagger вычисляются так:

$$(f^\dagger)_i^j = \begin{array}{c} \triangle_j \\ | \\ \square_f \\ | \\ \triangle_i \end{array} \stackrel{(4.18)}{=} \begin{array}{c} \triangle_i \\ | \\ \square_f \\ | \\ \triangle_j \end{array} = \overline{\left(\begin{array}{c} \triangle_i \\ | \\ \square_f \\ | \\ \triangle_j \end{array} \right)} = \overline{(f_j^i)}$$

где (4.18) выражает тот факт, что числа самотранспонированные. □

Отметим, что эта теорема справедлива для любых ОНБ, а не только самосопряженных. Напротив, чтобы операции транспонирования и сопряжения правильно работали с матрицами, необходимо, чтобы ОНБ были самосопряженными.

Теорема 5.19. Пусть f – процесс, с которым ассоциирована матрица \mathbf{f} с самосопряженными ОНБ \mathcal{B} и \mathcal{B}' . Матрицей процесса f^T является *транспонированная матрица* \mathbf{f}^T , определенная следующим образом:

$$(\mathbf{f}^T)_i^j := \mathbf{f}_i^j.$$

Матрицей процесса \bar{f} является *сопряженная матрица* $\bar{\mathbf{f}}$, определенная следующим образом:

$$\bar{\mathbf{f}}_i^j := \overline{(\mathbf{f}_i^j)}.$$

Доказательство. Элементы матрицы, транспонированной к f^\dagger , вычисляются так:

$$\begin{array}{c} \triangleup_j \\ \square f \\ \triangleleft_i \end{array} = \begin{array}{c} \triangleup_j \\ \square f \\ \triangleleft_i \end{array} \stackrel{(*)}{=} \begin{array}{c} \triangleleft_i \\ \square f \\ \triangleup_j \end{array} \quad (5.7)$$

а для элементов матрицы сопряженного процесса имеем:

$$\begin{array}{c} \triangleup_j \\ \square f \\ \triangleleft_i \end{array} \stackrel{(*)}{=} \begin{array}{c} \triangleleft_j \\ \square f \\ \triangleup_i \end{array}$$

где равенство, помеченное знаком (*), вытекает из того, что базисы \mathcal{B} и \mathcal{B}' само-сопряженные. Если бы это было не так, то результирующие матрицы выражались бы не в терминах \mathcal{B} и \mathcal{B}' , а в терминах сопряженных с ними базисов. \square

Таким образом, транспонированная матрица \mathbf{f}^T получается перестановкой индексов строк и столбцов, сопряженная матрица $\bar{\mathbf{f}}$ – заменой каждого элемента комплексно-сопряженным ему, а эрмитово-сопряженная матрица \mathbf{f}^\dagger – применением обеих операций. Поэтому эрмитово-сопряженную матрицу иногда называют сопряженно-транспонированной. Как и для диаграмм, порядок операций не имеет значения:

$$\mathbf{f}^\dagger = \overline{(\mathbf{f}^T)} = (\bar{\mathbf{f}})^T.$$

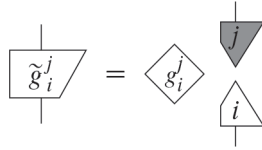
Упражнение 5.20. Охарактеризуйте матрицу самоадьюнктного процесса.

Итак, мы уже можем рассматривать несколько операций над процессами как операции над матрицами. Но мы еще не разработали *матричное исчисление* в полной мере. Теорема 5.14 утверждает, что $f = g$ тогда и только тогда, когда матрицы процессов f и g совпадают. Иными словами, если существует процесс f с заданной матрицей, то он единственный. Но если дана произвольная матрица, то нет никакой гарантии (пока), что существует процесс f , ассоциированный с этой матрицей.

Возьмем несколько чисел и организуем их в матрицу размера $n \times m$:

$$\begin{pmatrix} g_1^1 & g_2^1 & \cdots & g_m^1 \\ g_1^2 & g_2^2 & \cdots & g_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ g_1^n & g_2^n & \cdots & g_m^n \end{pmatrix} \quad (5.8)$$

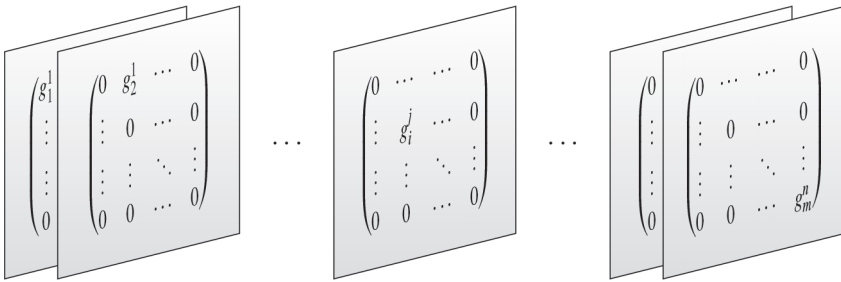
Как получить процесс g , имеющий такую матрицу? Сначала выберем ОНБ \mathcal{B} и \mathcal{B}' . Тогда для любых i, j можно построить процесс \tilde{g}_i^j , который согласован с g на i -м входном элементе \mathcal{B} и j -м выходном элементе \mathcal{B}' и равен 0 во всех остальных местах:



Если вычислить матрицу \tilde{g}_i^j , то у нее будет в точности один ненулевой элемент g_i^j в позиции (i, j) :

$$\begin{array}{c} \diagup \\ \tilde{g}_i^j \\ \diagdown \end{array} \leftrightarrow \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & g_i^j & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Мы можем определить целую стопку таких процессов \tilde{g}_i^j для всех i, j :



Тогда, если бы нам удалось «наложить» их друг на друга, мы получили бы g .

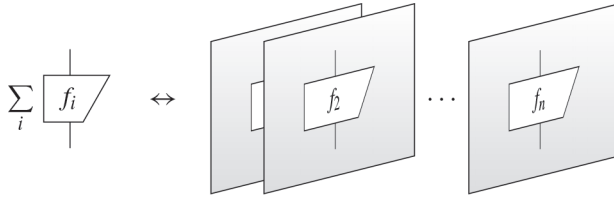
Оказывается, что для некоторых процессных теорий «наложение» процессов – вполне осмысленное действие. Если обозначить процедуру «наложения» как сумму процессов, то g можно выразить следующим образом:

$$\begin{array}{c} \diagup \\ g \\ \diagdown \end{array} := \sum_{ij} \begin{array}{c} \diagup \\ g_i^j \\ \diagdown \end{array} \begin{array}{c} \triangle \\ j \\ \triangle \\ i \end{array} \quad (5.9)$$

Таким образом, осталось только точно определить, что такое «сумма процессов».

5.1.3. Суммы процессов

Что такое суммирование старых процессов, не вполне понятно; например, как определить сумму двух младенцев? Но во многих процессных теориях эта операция имеет точно определенный математический смысл, прямо вытекающий из интуитивного представления о наложении диаграмм:



Определение 5.21. Говорят, что процессная теория *обладает суммами*, если выполнены три условия.

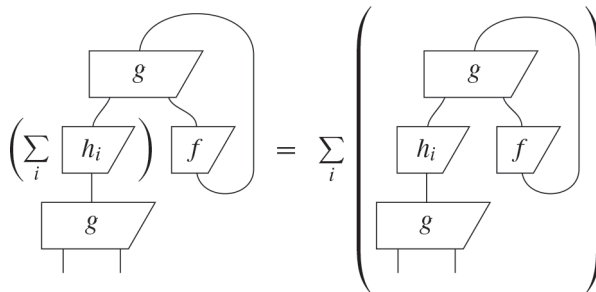
- **Условие 1:** для любых двух процессов f, g с одинаковыми входными и выходными типами $f + g$ является процессом. Мы всегда предполагаем, что операция «+» ассоциативна, коммутативна и имеет нейтральный элемент, совпадающий с нулевым процессом:

$$(f + g) + h = f + (g + h), \quad f + g = g + f, \quad f + 0 = f = 0 + f, -$$

и для множества $\{f_i\}_i$ процессов пишем:

$$\sum_i f_i := f_1 + f_2 + \dots + f_N$$

- **Условие 2:** сумма *дистрибутивна относительно диаграмм*, т. е. суммирование можно вынести из диаграммы наружу:



- **Условие 3:** суммирование сохраняет адьюнкты:

$$\left(\sum_i f_i \right)^\dagger = \sum_i f_i$$

Заметим, что **условие 2** включает в себя дистрибутивность суммы относительно параллельной и последовательной композиций:

$$\left(\sum_i f_i \right) \square g = \sum_i \left(f_i \square g \right)$$

и

$$\left(\sum_i \begin{array}{c} \text{---} \\ \boxed{g} \\ \text{---} \\ \boxed{f_i} \\ \text{---} \end{array} \right) = \sum_i \left(\begin{array}{c} \text{---} \\ \boxed{g} \\ \text{---} \\ \boxed{f_i} \\ \text{---} \end{array} \right)$$

Важный пример – *линейность* отображений относительно состояний:

$$\left(\sum_i \begin{array}{c} \text{---} \\ \diamond \lambda_i \\ \text{---} \\ \boxed{f} \\ \text{---} \\ \boxed{\psi_i} \\ \text{---} \end{array} \right) = \sum_i \left(\begin{array}{c} \text{---} \\ \diamond \lambda_i \\ \text{---} \\ \boxed{f} \\ \text{---} \\ \boxed{\psi_i} \\ \text{---} \end{array} \right)$$

Другой пример – внутреннее произведение. Имеет место истинная линейность для состояний:

$$\left(\sum_i \begin{array}{c} \text{---} \\ \diamond \lambda_i \\ \text{---} \\ \boxed{\phi} \\ \text{---} \\ \boxed{\psi_i} \\ \text{---} \end{array} \right) = \sum_i \left(\begin{array}{c} \text{---} \\ \diamond \lambda_i \\ \text{---} \\ \boxed{\phi} \\ \text{---} \\ \boxed{\psi_i} \\ \text{---} \end{array} \right) \tag{5.10}$$

и сопряженная линейность для эффектов:

$$\left(\sum_i \begin{array}{c} \text{---} \\ \diamond \bar{\lambda}_i \\ \text{---} \\ \boxed{\phi_i} \\ \text{---} \\ \boxed{\psi} \\ \text{---} \end{array} \right) = \sum_i \left(\begin{array}{c} \text{---} \\ \diamond \bar{\lambda}_i \\ \text{---} \\ \boxed{\phi_i} \\ \text{---} \\ \boxed{\psi} \\ \text{---} \end{array} \right) \tag{5.11}$$

Дистрибутивность также позволяет вывести матричный аналог сумм. Неудивительно, что мы получаем нечто похожее на сумму матриц в линейной алгебре.

Теорема 5.22. Пусть $\{f_k\}_k$ – процессы с ассоциированными матрицами $\{\mathbf{f}_k\}_k$. Матрицей процесса $\sum_k f_k$ является сумма матриц $\sum_k \mathbf{f}_k$, где

$$\left(\sum_k \mathbf{f}_k \right)_i^j := \sum_k (\mathbf{f}_k)_i^j.$$

Доказательство. Мы можем воспользоваться **условием 2** для вычисления матрицы процесса $\sum_k f_k$:

$$\left(\sum_k \begin{array}{c} \text{---} \\ \blacktriangle j \\ \text{---} \\ \boxed{f_k} \\ \text{---} \\ \blacktriangledown i \\ \text{---} \end{array} \right) = \sum_k \left(\begin{array}{c} \text{---} \\ \blacktriangle j \\ \text{---} \\ \boxed{f_k} \\ \text{---} \\ \blacktriangledown i \\ \text{---} \end{array} \right) = \sum_k (\mathbf{f}_k)_i^j$$

□

$$\sum_i \begin{array}{|c|} \hline \diagup \\ \hline f_i \\ \hline \diagdown \\ \hline \end{array} \approx \sum_i \begin{array}{|c|} \hline \diagdown \\ \hline g_i \\ \hline \diagup \\ \hline \end{array}$$

Чтобы это было правдой, во всех экземплярах равенства (5.12) должно фигурировать одно и то же число.

Хотя суммирование не распространяется на младенцев, с отношениями все хорошо.

Пример 5.25. В теории **отношений** в роли суммы выступает объединение. Если положить

$$\sum_i R_i := \bigcup_i R_i,$$

то можно без труда показать, что **условия 1–3** выполняются. Применяя это определение к числам 0 и 1, получаем:

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 1.$$

Таким образом, «+» для чисел в **теории отношений** – это логическая операция «или». Если обозначить «·» (параллельную или последовательную) композицию чисел, то также получим:

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Следовательно, мы имеем логическую операцию «и», и **условие 2** теперь оказывается обычным *правилом дистрибутивности* для «или» и «и»:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

Итак, в процессной теории с суммами для чисел всегда определены операции «плюс» и «умножить» (т. е. композиция), и вторая дистрибутивна относительно первой. Так что они начинают обретать сходство с настоящими числами.

Пример 5.26. Мы можем рассматривать любое натуральное число n как число в нашей процессной теории. Нужно просто просуммировать n единиц (т. е. пустых диаграмм):

$$\diamond n := \underbrace{1 + \dots + 1}_{n \text{ раз}}. \tag{5.13}$$

Если числа процессной теории – вещественные или комплексные числа, то они точно соответствуют натуральным числам (рассматриваемым как подмножество \mathbb{R} или \mathbb{C}). Однако это необязательно. Например, если числа – это булевы величины, как в примере 5.25, то все n – одно и то же:

$$\underbrace{1 + \dots + 1}_{n \text{ раз}} = 1.$$

Можно даже рассмотреть процессные теории с *вычитанием*, в которых для каждого процесса f существует процесс $-f$ такой, что $f + (-f) = 0$. Как обычно, $f + (-g)$

Доказательство. Достаточно показать, что для любых i, j следующие числа равны:

$$\begin{array}{c} \triangleup j \\ \square g \\ \triangle i \end{array} = \diamond g_i^j \tag{5.15}$$

В этом легко убедиться, подставив (5.14) в (5.15):

$$\begin{array}{c} \triangleup j \\ \square g \\ \triangle i \end{array} = \sum_{kl} \diamond g_k^l \begin{array}{c} \triangleup j \\ \triangle i \\ \square k \\ \triangle i \end{array} = \sum_{kl} \delta_i^k \delta_l^j \diamond g_k^l = \diamond g_i^j \quad \square$$

Говорят, что процесс в правой части равенства (5.14) представлен в *матричной форме*, т. е. записан в виде слагаемых, состоящих из:

- (1) числа,
- (2) состояния ОНБ и
- (3) эффекта ОНБ.

Матричной эта форма называется, потому что в сумму явно входят все элементы матрицы g . Для частного случая состояний матричная форма – это просто состояние, записанное в виде суммы базисных состояний с коэффициентами:

$$\downarrow \psi = \sum_i \diamond \psi^i \downarrow i$$

Мы можем подойти к этому с другой стороны и дать еще одну характеристику ОНБ.

Теорема 5.30. Предположим, что существует базис \mathcal{B} для типа A . Тогда еще одно ортонормированное множество состояний

$$\mathcal{A} := \left\{ \downarrow i \right\}_i$$

образует ОНБ для A тогда и только тогда, когда оно *стягивает* A , т. е. если любое состояние ψ типа A можно записать в виде линейной комбинации, где λ_i – числа:

$$\downarrow \psi = \sum_i \diamond \lambda_i \downarrow i \tag{5.16}$$

Доказательство. Чтобы доказать импликацию \Rightarrow , предположим, что \mathcal{A} является ОНБ. Тогда равенство (5.16) следует из матричной формы состояния ψ . Обратно, предположим, что \mathcal{A} стягивает A и

для всех $\downarrow_i \in \mathcal{A}$:

$$\begin{array}{c} \downarrow \\ | \\ \text{f} \\ \diagdown \\ | \\ \text{i} \end{array} = \begin{array}{c} \downarrow \\ | \\ \text{g} \\ \diagdown \\ | \\ \text{i} \end{array}$$

Поскольку \mathcal{A} стягивает \mathcal{A} , мы можем выразить любое состояние ψ в виде:

$$\downarrow_{\psi} = \sum_i \diamond_{\lambda_i} \downarrow_i$$

Поэтому

$$\begin{array}{c} \downarrow \\ | \\ \text{f} \\ \diagdown \\ | \\ \downarrow_{\psi} \end{array} = \sum_i \diamond_{\lambda_i} \begin{array}{c} \downarrow \\ | \\ \text{f} \\ \diagdown \\ | \\ \text{i} \end{array} = \sum_i \diamond_{\lambda_i} \begin{array}{c} \downarrow \\ | \\ \text{g} \\ \diagdown \\ | \\ \text{i} \end{array} = \begin{array}{c} \downarrow \\ | \\ \text{g} \\ \diagdown \\ | \\ \downarrow_{\psi} \end{array}$$

В частности, f и g совпадают на всех состояниях из базиса \mathcal{B} , и значит, $f = g$. \square

Еще один исключительно полезный частный случай – матричная форма тождественного процесса. Если задан ОНБ, то элементы матрицы тождественного процесса равны

$$\begin{array}{c} \uparrow_j \\ | \\ \boxed{} \\ | \\ \downarrow_i \end{array} = \delta_i^j$$

Если записать их в виде матрицы, то мы получим единицы на главной диагонали (там, где $i = j$) и нули во всех остальных местах:

$$\left| \right. \leftrightarrow \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

т. е. *единичную матрицу*. Переводя это в матричную форму, получаем:

$$\left| \right. = \sum_i \delta_i^j \begin{array}{c} \uparrow_j \\ | \\ \downarrow_i \end{array} = \sum_i \begin{array}{c} \uparrow_i \\ | \\ \downarrow_i \end{array}$$

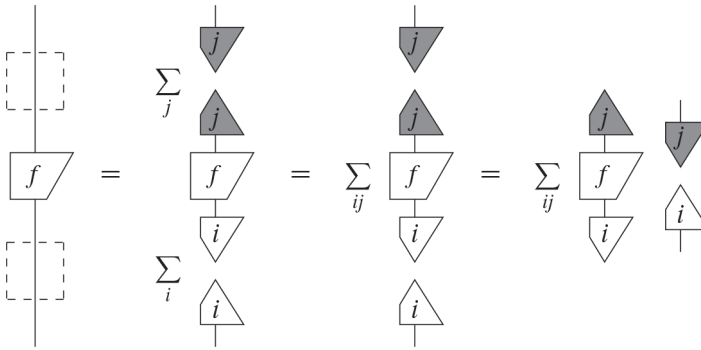
Таким образом, мы доказали следующую теорему.

Теорема 5.31. Для любого ОНБ имеет место равенство

$$| = \sum_i \begin{array}{c} \downarrow i \\ \uparrow i \end{array} \quad (5.17)$$

Такую декомпозицию мы будем называть *разложением единицы*.

Матричная форма тождественного процесса дает удобный способ вычисления матричной формы произвольного процесса:



Обращение теоремы 5.31 также верно и дает еще одну, очень лаконичную характеристику ОНБ:

Теорема 5.32. Множество состояний

$$\mathcal{A} := \left\{ \begin{array}{c} \downarrow i \\ \uparrow i \end{array} \right\}_i$$

является ОНБ тогда и только тогда, когда

$$\begin{array}{c} \downarrow j \\ \uparrow i \end{array} = \delta_i^j \quad | = \sum_i \begin{array}{c} \downarrow i \\ \uparrow i \end{array} \quad (5.18)$$

Доказательство. Из теоремы 5.31 мы знаем, что любой ОНБ удовлетворяет условию (5.18). Обратно, пусть \mathcal{A} удовлетворяет (5.18), и предположим, что для процессов f и g справедливо утверждение

$$\text{для всех } \begin{array}{c} \downarrow i \\ \uparrow i \end{array} \in \mathcal{A} : \begin{array}{c} \downarrow \\ \uparrow i \end{array} f = \begin{array}{c} \downarrow \\ \uparrow i \end{array} g$$

Тогда

$$\begin{array}{c} \diagup \\ f \\ \diagdown \end{array} \stackrel{(5.17)}{=} \sum_i \begin{array}{c} \diagup \\ f \\ \diagdown \\ \diagup \\ i \\ \diagdown \\ \diagup \\ i \\ \diagdown \end{array} = \sum_i \begin{array}{c} \diagup \\ g \\ \diagdown \\ \diagup \\ i \\ \diagdown \\ \diagup \\ i \\ \diagdown \end{array} \stackrel{(5.17)}{=} \begin{array}{c} \diagup \\ g \\ \diagdown \end{array}$$

поэтому \mathcal{A} действительно образует базис и, значит, является ОНБ. □

Еще одно интересное следствие теоремы 5.31 касается числа, обозначенного «кружочком». Имеем:

$$\bigcirc = \sum_i \begin{array}{c} \diagup \\ i \\ \diagdown \\ \diagup \\ i \\ \diagdown \end{array} = \sum_i \begin{array}{c} \diagup \\ i \\ \diagdown \\ \diagup \\ i \\ \diagdown \end{array} = \begin{array}{c} \diagup \\ 1 \\ \diagdown \\ \diagup \\ 1 \\ \diagdown \end{array} + \dots + \begin{array}{c} \diagup \\ D \\ \diagdown \\ \diagup \\ D \\ \diagdown \end{array} = \langle D \rangle$$

где согласно примеру 5.26:

$$\langle D \rangle := \underbrace{1 + \dots + 1}_{D \text{ раз}} \tag{5.19}$$

Таким образом, кружочек подсчитывает количество векторов в базисе, т. е. дает размерность! Ну, по крайней мере, чаще всего. Напомним (см. пример 5.26), что $\langle D \rangle$ не всегда совпадает с фактическим натуральным числом D ; например, в теории **отношений** возможно значение 0 (для нуля базисных векторов) или 1 (для одного и более базисных векторов). Но в случае **линейных отображений** $\langle D \rangle$ обязательно равно $\dim(A)$.

Следствие 5.33. Для размерности D системного типа A имеет место равенство

$${}_A \bigcirc = \langle D \rangle$$

где $\langle D \rangle$ определено, как в (5.19).

Замечание 5.34. На самом деле нам суммы не нравятся! И причина очевидна:

$$\begin{array}{c} \text{Есть провод} \longrightarrow \\ \hline \\ \longleftarrow \text{Нет провода} \end{array} = \sum_i \begin{array}{c} \diagup \\ i \\ \diagdown \\ \diagup \\ i \\ \diagdown \end{array}$$

Суммы совершенно не согласуются с тем фактом, что диаграммы – это про то, как «одно соединено с другим», и именно в этом состоит их прелесть. Поэтому мы

всегда избавляемся от сумм, если удастся найти более свойственную диаграммам альтернативу.

Мы завершим этот раздел определением (классического) распределения вероятностей с помощью матриц. Распределение вероятностей сопоставляет каждому элементу набора взаимоисключающих событий вещественное число от 0 до 1, причем сумма всех этих чисел равна 1. Распределения вероятностей и особенно их матричные представления будут играть в этой книге важную роль.

Определение 5.35. Предположим, что множество чисел в некоторой процессной теории содержит положительные вещественные числа. *Распределением вероятностей* называется матрица вида

$$\begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} \tag{5.20}$$

элементами которой являются положительные вещественные числа p^i , дающие в сумме 1:

$$\sum_i p^i = \boxed{}$$

Распределения вероятностей можно также представить в виде состояний такого вида:

$$\downarrow p \quad := \quad \sum_i p^i \downarrow_i$$

где p^i те же, что и выше. Распределения вероятностей, соответствующие базисным состояниям

$$\downarrow_1 \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \dots \quad \downarrow_i \leftrightarrow \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad \downarrow_n \leftrightarrow \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

называются *точечными распределениями*.

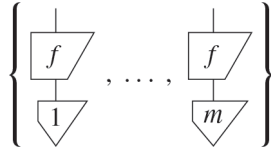
Поскольку распределение вероятностей – это матрица (или состояние в матричной форме), то ему всегда сопутствует выбор ОНБ. Мы будем выбирать самосопряженный ОНБ по той простой причине, что сопряжение не играет никакой роли в теории вероятностей.

5.1.5. Матрицы изометрических и унитарных процессов

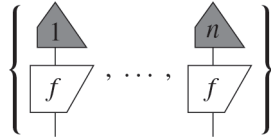
В этом и следующем разделе мы охарактеризуем изометрические, унитарные и положительные процессы, проекторы и \otimes -положительные состояния в терминах их матриц.

В первых двух случаях, которые мы рассмотрим в этом разделе, будет полезно взглянуть на строки и столбцы матриц.

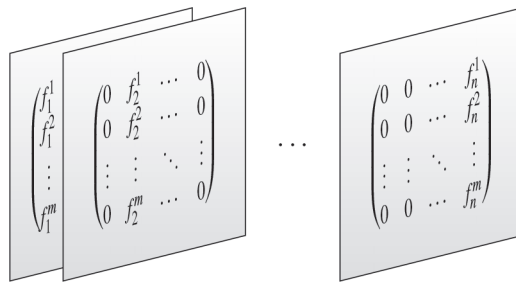
Определение 5.36. Если заданы ОНБ для входного и выходного типов процесса f , то *столбцами* f называются матрицы следующего множества состояний:



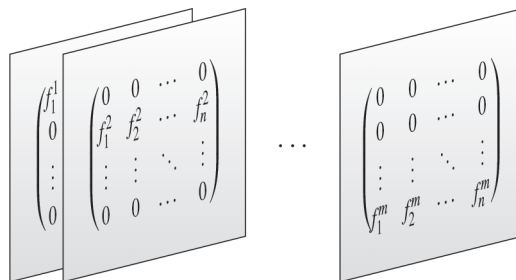
а *строками* – матрицы следующего множества эффектов:



Как можно предположить по названию, стопка столбцов f образует полную матрицу f :



и аналогично для строк:



Мы говорим, что векторы-столбцы образуют ОНБ, если это справедливо для ассоциированных с ними состояний. Аналогично векторы-строки образуют ОНБ, если это справедливо для (адьюнктов) ассоциированных с ними эффектов. Теперь у нас есть способ распознать матрицы изометрических процессов.

Предложение 5.37. Для любого процесса f следующие утверждения эквивалентны:

- (1) f – изометрия;
- (2) f переводит ортонормированное множество состояний в ортонормированное множество состояний;
- (3) столбцы f ортонормированны;
- (4) строки f^\dagger ортонормированны.

Доказательство. Сначала докажем импликацию $(1 \Rightarrow 2)$. Пусть дано произвольное ортонормированное множество состояний

$$\mathcal{A} := \left\{ \begin{array}{c} \downarrow \\ i \end{array} \right\}_i$$

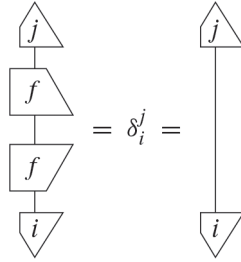
Мы должны показать, что следующее множество тоже ортонормированно:

$$\left\{ \begin{array}{c} \downarrow \\ f \\ i \end{array} \right\}_i$$

Это следует из того, что f – изометрия:

$$\begin{array}{c} \begin{array}{c} \uparrow j \\ \downarrow f \\ \downarrow f \\ \downarrow i \end{array} \quad (4.42) \quad = \quad \begin{array}{c} \uparrow j \\ \downarrow i \end{array} = \delta_i^j \end{array}$$

Импликация $(2 \Rightarrow 3)$ очевидна, потому что столбцы f получаются применением процесса f к конкретному ортонормированному множеству, а именно фиксированному ОНБ в его входной системе. Импликация $(3 \Rightarrow 4)$ следует из того факта, что строки f^\dagger – это просто адьюнкты столбцов f . Чтобы доказать импликацию $(4 \Rightarrow 1)$, предположим, что строки f^\dagger ортонормированны. Тогда, в силу ортонормированности, $f^\dagger \circ f$ имеет такую же матрицу, как тождественный процесс:



Таким образом, f – изометрия. □

Это предложение позволяет легко распознать унитарные процессы по их матрицам. Нужно просто заменить ортонормированные множества ортонормированными базисами.

Предложение 5.38. Следующие утверждения эквивалентны:

- (1) f – унитарный процесс;
- (2) f переводит ОНБ в ОНБ;
- (3) столбцы f образуют ОНБ;
- (4) строки f образуют ОНБ.

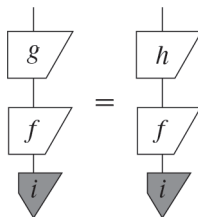
Доказательство. (1 \Rightarrow 2) Если процесс f унитарный, то он является изометрией. Поэтому для любого ОНБ

$$\mathcal{B} := \left\{ \begin{array}{c} \downarrow \\ \text{и} \\ \downarrow \end{array} \right\}_i$$

мы из предложения 5.37 знаем, что состояния

$$\left\{ \begin{array}{c} \downarrow \\ \text{f} \\ \downarrow \\ \text{и} \\ \downarrow \end{array} \right\}_i$$

ортонормированны. Осталось показать, что эти состояния образуют базис. Для этого мы покажем, что $g = h$ в точности тогда, когда g и h совпадают на всех этих состояниях. Предположим, что для всех i



Так как \mathcal{B} – базис, то

$$\begin{array}{c} \diagup \\ g \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} = \begin{array}{c} \diagup \\ h \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \tag{5.21}$$

В сочетании с унитарностью f это дает:

$$\begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \stackrel{(4.43)}{=} \begin{array}{c} \diagup \\ g \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \stackrel{(5.21)}{=} \begin{array}{c} \diagup \\ h \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \stackrel{(4.43)}{=} \begin{array}{c} \diagdown \\ h \\ \diagup \end{array}$$

Импликация $(2 \Rightarrow 3)$ очевидна. Чтобы доказать импликацию $(3 \Rightarrow 1)$, заметим, что, согласно предыдущему предложению, f является изометрией, поэтому достаточно показать, что и f^\dagger – тоже изометрия. В силу (5.17)

$$\begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} = \sum_i \begin{array}{c} \diagup \\ f \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ i \\ \diagup \end{array} \begin{array}{c} \diagdown \\ i \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array}$$

Поскольку столбцы f образуют ОНБ, то по теореме 5.31 правая часть этого равенства также является разрешением единицы:

$$\sum_i \begin{array}{c} \diagup \\ f \\ \diagdown \end{array} \begin{array}{c} \diagdown \\ i \\ \diagup \end{array} \begin{array}{c} \diagdown \\ i \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} = \left| \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \right|, \quad \text{поэтому} \quad \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} = \left| \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \right|$$

Наконец, эквиваленция $(3 \Leftrightarrow 4)$ следует из того, что процесс f унитарный тогда и только тогда, когда f^\dagger унитарный.

Доказанная теорема дает характеристику унитарных процессов как отображений, переводящих ОНБ в ОНБ. Из нее сразу вытекает

Следствие 5.39. Унитарными являются те и только те процессы, которые можно представить в виде:



для некоторой пары ОНБ (с одинаковым числом элементов).

Замечание 5.40. Предложение 5.37 говорит, что изометрия переводит ортонормированные множества состояний в ортонормированные. В частности, она переводит ОНБ в некоторое *подмножество* другого ОНБ. Поэтому мы по-прежнему можем пользоваться представлением (5.39) для изометрий, при условии что ослабим требование на множество



– оно должно быть ортонормированным множеством, а необязательно ОНБ. Иными словами, мы можем рассматривать изометрии как унитарные процессы, «про-долженные» на более широкую выходную систему.

5.1.6. Матрицы самоаdjюнктных и положительных процессов

В теореме 5.18 мы охарактеризовали матрицу адьюнкта процесса:

$$(f^\dagger)_i = \overline{(f^i)}.$$

Отсюда сразу следует, что матрица самоаdjюнктного процесса имеет вид:

$$\begin{pmatrix} f_1^1 & f_2^1 & \cdots & f_n^1 \\ \overline{f_2^1} & f_2^2 & \cdots & f_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \overline{f_n^1} & \overline{f_n^2} & \cdots & f_n^n \end{pmatrix},$$

причем элементы на главной диагонали самосопряженные:

$$f_i^i \stackrel{(5.25)}{=} \begin{array}{c} \triangleup i \\ \square f \\ \triangle i \end{array} \stackrel{(4.46)}{=} \begin{array}{c} \triangleup i \\ \square f \\ \triangle i \end{array} \stackrel{(5.25)}{=} (f_i^i)^\dagger = \overline{f_i^i}$$

К сожалению, матрицы положительных процессов охарактеризовать не так просто, но мы, по крайней мере, знаем, как выглядят числа на диагонали:

$$f_i^i \stackrel{(5.25)}{=} \begin{array}{c} \triangle i \\ \square f \\ \triangle i \end{array} \stackrel{(4.45)}{=} \begin{array}{c} \triangle i \\ \square g \\ \square g \\ \triangle i \end{array} = \begin{array}{c} \triangle i \\ \square g \\ \square g \\ \triangle i \end{array} \quad (5.22)$$

т. е. это положительные числа. Тогда в силу двойственности процессов и состояний имеет место

Следствие 5.41. Для любого \otimes -положительного состояния ψ числа

$$\psi^{ii} := \begin{array}{c} \triangle i \quad \triangle i \\ \square \psi \end{array}$$

положительны.

По счастью, для так называемых *диагонализуемых* процессов характеристики чисел на главной диагонали вполне достаточно.

Определение 5.42. *Собственным состоянием* процесса f называется ненулевое состояние ψ такое, что для некоторого числа λ имеет место равенство

$$\begin{array}{c} \square f \\ \triangle \psi \end{array} = \lambda \begin{array}{c} \triangle \psi \end{array}$$

а f называется *диагонализуемым*, если существует такой ОНБ \mathcal{B} , что все базисные состояния являются собственными состояниями f , т. е.

$$\text{для любого } \begin{array}{c} \triangle i \end{array} \in \mathcal{B} \text{ существует } \lambda_i : \begin{array}{c} \square f \\ \triangle i \end{array} = \lambda_i \begin{array}{c} \triangle i \end{array} \quad (5.23)$$

Следующий результат оправдывает принятую терминологию.

Предложение 5.43. Если процесс f диагонализуемый, то его матрица в базе собственных состояний *диагональна*:

$$\begin{array}{c} \diagup \\ f \\ \diagdown \end{array} = \sum_i \lambda_i \begin{array}{c} \diagdown \\ i \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} \leftrightarrow \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} \quad (5.24)$$

Доказательство. Для элементов матрицы диагоналируемого процесса f имеем:

$$\begin{array}{c} \diagdown \\ j \\ \diagup \\ \diagdown \\ f \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} \stackrel{(5.23)}{=} \lambda_i \begin{array}{c} \diagdown \\ j \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} = \lambda_i \delta_i^j \quad (5.25)$$

откуда следует (5.24). □

Если процесс диагоналируемый, то мы можем охарактеризовать его самоадьюнктность, положительность и свойство быть проектором в терминах чисел на диагонали.

Предложение 5.44. Для любого диагоналируемого процесса f справедливы следующие утверждения:

- (i) f самоадьюнктивный тогда и только тогда, когда все числа λ_i самосопряженные;
- (ii) f положительный тогда и только тогда, когда все числа λ_i положительные;
- (iii) f является проектором тогда и только тогда, когда все числа λ_i положительные и удовлетворяют условию $(\lambda_i)^2 = \lambda_i$.

Доказательство. Часть (i) следует из характеристики самоадьюнктных матриц, приведенной в начале этого раздела. Для доказательства (ii) сначала предположим, что f – положительный процесс. Тогда, в силу (5.22), все λ_i положительные. Обратное, предположим, что все λ_i положительные. Тогда существуют такие μ_i , что $\lambda_i = \mu_i^\dagger \circ \mu_i$. Для всех процессных теорий в этой книге можно предполагать, что каждое μ_i – тоже число (а не более общее состояние), поэтому сначала рассмотрим этот случай. Если положить

$$\begin{array}{c} \diagup \\ g \\ \diagdown \end{array} := \sum_i \mu_i \begin{array}{c} \diagdown \\ i \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array}$$

то легко проверить, что $f = g^\dagger \circ g$. Для более общей процессной теории μ_i необязательно является числом, и в таком случае g нужно конструировать аккуратнее (см. упражнение* 5.45). Для доказательства (iii) предположим, что f – проектор. Из (i) мы знаем, что λ_i должны быть положительными. Далее имеем:

$$\lambda_i \stackrel{(5.25)}{=} \begin{array}{c} \triangleup i \\ | \\ \square f \\ | \\ \triangle i \end{array} \stackrel{(4.50)}{=} \begin{array}{c} \triangleup i \\ | \\ \square f \\ | \\ \square f \\ | \\ \triangle i \end{array} \stackrel{(5.23)}{=} \begin{array}{c} \triangleup i \\ | \\ \square f \\ | \\ \triangle i \end{array} \stackrel{(5.25)}{=} (\lambda_i)^2$$

Обратно, если все λ_i положительны, положительным будет и процесс f , и очевидно, что f является проектором в точности тогда, когда $(\lambda_i)^2 = \lambda_i$.

Эквивалентно можно сказать, что диагоналируемый процесс f является самоадьюнктным, положительным или проектором тогда и только тогда, когда сами числа λ_i соответственно самоадьюнктные, положительные или являются проекторами.

Упражнение* 5.45. Докажите часть (ii) предложения 5.44 в случае, когда каждый процесс μ_i является состоянием типа A_i , т. е.

$$\lambda_i = \begin{array}{c} \triangleup \mu_i \\ | \\ A_i \\ | \\ \triangle i \end{array}$$

Во всех процессных теориях, рассматриваемых в этой книге, единственными числами, удовлетворяющими условию $\lambda^2 = \lambda$, являются 0 и 1, поэтому на главной диагонали диагоналируемых проекторов могут находиться только нули и единицы.

А почему мы вообще уделили столько внимания диагоналируемым процессам? На первый взгляд кажется, что это очень ограничительное условие. Так, в некоторых процессных теориях диагоналируемость вообще не представляет интереса.

Пример 5.46. В теории **отношений** любой ортонормированный базис содержит всего один элемент. Поэтому диагоналируемыми будут только те процессы, матрицы которых уже диагональны.

Однако в разделе 5.3.3.1 мы увидим, что все самоадьюнктные процессы в теории **линейных отображений** диагоналируемы. Поскольку положительные процессы и проекторы являются самоадьюнктными, предложение 5.44 в этом контексте дает исчерпывающую характеристику.

С другой стороны, существует много несамоадьюнктных процессов, которые невозможно диагонализировать практически ни в какой процессной теории.

Упражнение 5.47. Покажите, что в любой процессной теории, в которой ненулевые числа сокращаются (см. раздел 4.4.2), для любых ненулевых состояний ψ , ϕ , удовлетворяющих условию

$$\begin{array}{c} \triangleup \phi \\ | \\ \triangle \psi \end{array} = 0$$

процесс



не является диагонализируемым ни в каком ОНБ.

5.1.7. Следы матриц

В разделе 4.2.3 мы определили след процесса:

$$\text{tr}(f) := \text{loop}(f)$$

Матричную форму следа f можно вывести, воспользовавшись разложением единицы:

$$\text{loop}(f) = \sum_i \text{loop}(f \circ \text{triangle}_i) = \sum_i \text{triangle}_i \circ f \circ \text{triangle}_i \tag{5.26}$$

В терминах матрицы f это сумма всех элементов вида f_i^i . Иными словами, след матрицы равен сумме ее диагональных элементов:

$$\text{tr} \begin{pmatrix} f_1^1 & \dots & \dots & \cdot \\ \vdots & f_2^2 & \dots & \cdot \\ \vdots & \vdots & \ddots & \vdots \\ \cdot & \cdot & \dots & f_D^D \end{pmatrix} = \sum_i f_i^i$$

Отметим, что диагональные элементы матрицы зависят от того, в каком базисе записана матрица. Поэтому может показаться, что след зависит от базиса. Но это, очевидно, не так, потому что изначально мы определяли след без всякого упоминания ОНБ. Принципиальна здесь диаграмма (5.26): мы можем разложить тождественный процесс, используя любой ОНБ, и результат получится тем же самым.

Аналогично можно охарактеризовать частичный след. Сначала заметим, что след, как и раньше, можно представить в виде суммы:

5.2. МАТРИЧНОЕ ИСЧИСЛЕНИЕ

Теперь мы можем представить каждый процесс матрицей, и наоборот, каждая матрица представляет процесс. Мы умеем идентифицировать специальные процессы в терминах их матриц и определили матричные аналоги транспонирования, сопряжения и адьюнкции. Но нас интересуют не столько отдельные процессы, сколько формирование из них диаграмм. Поэтому нужно понять, как устроено соответствие между диаграммами и композицией матриц.

Перед нами открываются два пути. Один, навеянный теоремой 4.19, – рассматривать струнные диаграммы как схемные, пополненные чашками и крышками для каждого типа, и определить матричные аналоги последовательной и параллельной композиций, а также чашек и крышек. Мы сделаем это в следующих трех разделах. Затем в разделе 5.2.4 мы продемонстрируем более прямой способ вычисления матрицы струнной диаграммы с помощью формул, введенных в определении 4.21.

Расставив все по местам, мы покажем, что матрицы дают не только способ представления процессных теорий, но и простой путь построения «абстрактных» процессных теорий, когда нужно только задать числа, выступающие в роли элементов матриц.

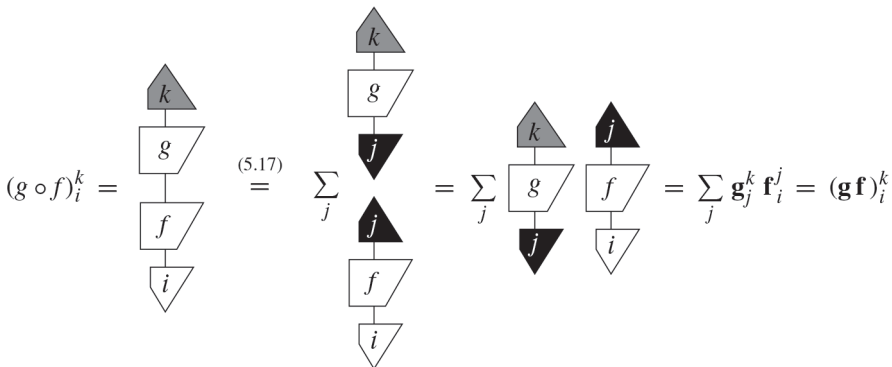
5.2.1. Последовательная композиция матриц

Сначала изучим, как последовательную композицию процессов можно интерпретировать в виде операции над матрицами этих процессов.

Теорема 5.48. Пусть f и g – процессы, с которыми ассоциированы матрицы \mathbf{f} и \mathbf{g} . Матрицей процесса $g \circ f$ является произведение матриц $\mathbf{g f}$, определяемое формулой:

$$(\mathbf{g f})_i^k := \sum_j \mathbf{g}_j^k \mathbf{f}_i^j \tag{5.27}$$

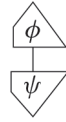
Доказательство. Элементы матриц $g \circ f$ равны



□

Существует простой способ вычислить произведение матриц (5.27), используя строки и столбцы. Сначала заметим, что матрица состояния состоит из одного

столбца, а матрица эффекта – из одной строки. Применяя формулу композиции (5.27) к случаю состояния ψ и эффекта ϕ



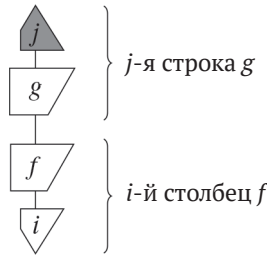
получаем:

$$(\phi_1 \quad \phi_2 \quad \cdots \quad \phi_n) \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = \phi_1 \psi^1 + \cdots + \phi_n \psi^n.$$

Иногда эту величину называют *скалярным произведением* ψ и ϕ , хотя в действительности это всего лишь последовательная композиция. Внимательно приглядевшись к элементам матрицы в формуле композиции (5.27) для процессов общего вида f и g :

$$(g \circ f)_i^j = g^j f_i^1 + \cdots + g_n^j f_i^n,$$

мы увидим, что можем получить элемент в i -м столбце и j -й строке матрицы $g \circ f$, вычислив скалярное произведение i -го столбца f на j -ю строку g :



в результате чего получается

$$\begin{pmatrix} \vdots \\ g_1^j \quad \cdots \quad g_n^j \\ \vdots \end{pmatrix} \begin{pmatrix} f_i^1 \\ \vdots \\ f_i^m \end{pmatrix} = \begin{pmatrix} \vdots \\ g_1^j f_i^1 + \cdots + g_n^j f_i^m \\ \vdots \end{pmatrix}.$$

Именно так большинство читателей училось умножать матрицы в школе.

5.2.2. Параллельная композиция матриц

Перейдем теперь к параллельной композиции. Мы вычислим матрицу, соответствующую $f \otimes g$, зная матрицы f и g . Для этого мы сначала должны понять, как получить ОНБ типа совместной системы:



при условии что известны ОНБ типов A и B .

Теорема 5.49. Обозначим

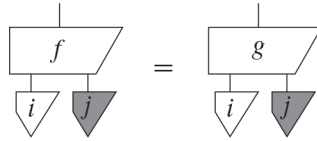
$$\mathcal{B} := \left\{ \begin{array}{c} \downarrow \\ i \end{array} \right\}_i \quad \text{и} \quad \mathcal{B}' := \left\{ \begin{array}{c} \downarrow \\ j \end{array} \right\}_j$$

ОНБ типов A и B соответственно. Тогда множество состояний

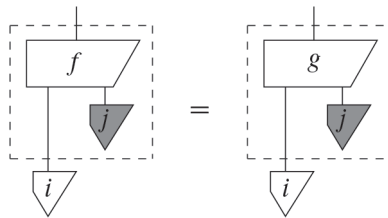
$$\left\{ \begin{array}{c} \downarrow \quad \downarrow \\ i \quad j \end{array} \right\}_{ij} \tag{5.28}$$

образует ОНБ типа $A \otimes B$, который называется *базисом произведения*.

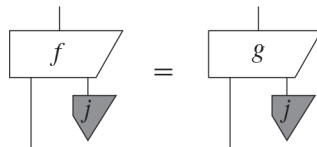
Доказательство. Мы можем показать, что условие (5.2) выполняется, рассматривая по одному базису, как при доказательстве теоремы 5.14. Предположим, что любая пара процессов f, g с входным типом $A \otimes B$ совпадает на всех состояниях из множества (5.28):



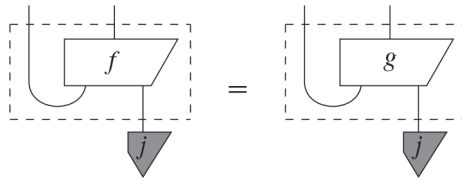
что можно переписать в виде:



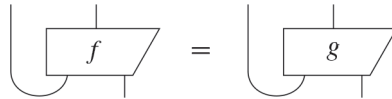
Из того, что \mathcal{B} – базис, следует:



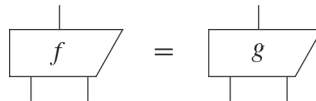
поэтому для всех состояний j , принадлежащих \mathcal{B}' , имеем также:



а поскольку \mathcal{B}' – базис, то:



и стало быть:



Ортонормированность состояний (5.28) означает, что:

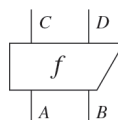
$$\begin{array}{c} \triangleleft i' \\ \triangleleft i \end{array} = \delta_i^{i'} \delta_j^{j'}$$

что следует из ортонормированности \mathcal{B} и \mathcal{B}' . Поэтому, в силу предложения 5.10, мы имеем ОНБ. □

Если A имеет базис размера D , то $A \otimes A$ имеет D^2 базисных состояний. Обобщая, приходим к выводу, что система, состоящая из n копий A , имеет D^n базисных состояний. Поэтому размерность экспоненциально растет с увеличением количества систем!

Замечание* 5.50. Отметим, что доказательство теоремы 5.49 существенно зависит от чашек и крышек. Поэтому струнные диаграммы заставляют нас использовать *тензорное произведение* при описании составных систем. Другого варианта просто нет. Это интересно в свете того факта, что физики уже давно задаются вопросом, почему для описания составных систем используется тензорное произведение, а не *прямая сумма*. Оставляем в качестве упражнения интересующемуся читателю попытку построить процессную теорию, в которой линейные отображения комбинировались бы с помощью прямой суммы. Что в ней не так?

Предположим теперь, что мы хотим записать матрицу для процесса вида:



До сих пор при записи матриц процессов мы неявно предполагали, что на базисных состояниях определен какой-то порядок. А иначе откуда бы мы знали, в какую позицию матрицы помещать каждое число? Если состояния помечены числами $i \in \{1, \dots, D\}$, то, очевидно, так оно и есть. Таким образом, чтобы записать матрицу f в терминах базисов произведения, мы должны зафиксировать порядок состояний в базисе произведения. Для начала немного упростим себе жизнь, прономеровав элементы базиса, начиная с 0. Тогда для базисов

$$\left\{ \begin{array}{c} \downarrow \\ i \end{array} \right\}_{0 \leq i < D} \quad \text{и} \quad \left\{ \begin{array}{c} \downarrow \\ j \end{array} \right\}_{0 \leq j < D'}$$

мы можем воспользоваться тем фактом, что любое целое число k в диапазоне $0 \leq k < DD'$ можно единственным образом представить в виде $iD' + j$. Поэтому элементы базиса произведения можно занумеровать следующим образом:

$$\begin{array}{c} \downarrow \downarrow \\ iD' + j \end{array} := \begin{array}{c} \downarrow \downarrow \\ i \quad j \end{array} \quad (5.29)$$

Такое соглашение естественно обобщается на любое количество систем, и если все системы имеют одинаковую размерность D , то (5.29) можно рассматривать как представление некоторого числа по основанию D . Например, если все системные типы имеют размерность $D = 2$, то:

$$\begin{array}{c} \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \\ 117 \end{array} := \begin{array}{c} \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \downarrow \\ 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \end{array} \quad (5.30)$$

т. к. число 117 в двоичной системе записывается в виде 1110101.

Замечание 5.51. Тот факт, что базисные состояния N систем можно закодировать битовыми строками, очень важен для квантовых вычислений. Мы уже встречались с похожим кодированием в примере 3.27, когда представляли битовые строки как декартово произведение N экземпляров множества \mathbb{B} .

При работе с базисами произведения почти всегда удобнее индексировать элементы матрицы отдельными цифрами, избегая тем самым дополнительного жонглирования числами в соответствии с равенством (5.29). Если дана строка индивидуальных базисных состояний, как в правой части (5.30), то будем называть крайнее слева состояние *старшим* базисным состоянием, поскольку его изменение приводит к наибольшему изменению «закодированного» числа, а крайнее справа состояние – *младшим* базисным состоянием. Это согласуется с терминологией, применяемой в информатике, где говорят о «старшем» и «младшем» битах в битовой строке. Разумеется, это всего лишь соглашение. Но важно один раз выбрать соглашение и затем придерживаться его.

Для двумерной системы Q размерность $Q \otimes Q$ равна четырем, поэтому матрица состояния типа $Q \otimes Q$ – это вектор-столбец с четырьмя элементами:

$$\begin{array}{c} | \\ \text{---} \\ \psi \\ \text{---} \\ | \end{array} \leftrightarrow \begin{pmatrix} \psi^{00} \\ \psi^{01} \\ \psi^{10} \\ \psi^{11} \end{pmatrix}, \quad \text{где} \quad \psi^{ij} := \begin{array}{c} \triangleup \quad \triangleup \\ | \quad | \\ \psi \\ \text{---} \\ | \end{array}$$

Благодаря использованию нижних и верхних индексов формулы становятся опрятнее, даже если индексов несколько:

$$\begin{array}{c} | \\ \text{---} \\ g \\ \text{---} \\ | \end{array} \leftrightarrow \begin{pmatrix} g_{00}^0 & g_{01}^0 & g_{10}^0 & g_{11}^0 \\ g_{00}^1 & g_{01}^1 & g_{10}^1 & g_{11}^1 \end{pmatrix}, \quad \text{где} \quad g_{ij}^k := \begin{array}{c} \triangleup \quad k \\ | \\ \text{---} \\ g \\ \text{---} \\ | \quad | \\ \triangleleft \quad i \quad \triangleleft \quad j \end{array}$$

Таким образом, в общем случае мы встречаем матрицы с большим количеством верхних и нижних индексов:

$$\left(g_{i_1 i_2 \dots i_M}^{j_1 j_2 \dots j_N} \mid 0 \leq i_k < D_k, 0 \leq j_k < D'_k \right). \quad (5.31)$$

Замечание* 5.52. Иногда такая запись называется *тензорной нотацией*, где под тензором понимается просто матрица с большим количеством индексов. Это предтеча *абстрактной тензорной нотации* (см. раздел* 3.6.1), а стало быть, также диаграммных формул. Правда, ни то, ни другое не зависит от фиксированных базисов.

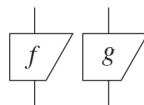
Рассмотрим теперь разделимое состояние $\psi \otimes \phi$ типа $\mathbb{Q} \otimes \mathbb{Q}$. Поскольку оно образовано из состояний ψ и ϕ , можно ожидать, что существует связь между его матрицей и матрицами ψ и ϕ . Легко проверить, что это действительно так:

$$\begin{array}{c} | \\ \text{---} \\ \psi \\ \text{---} \\ | \end{array} \leftrightarrow \begin{pmatrix} \psi^0 \\ \psi^1 \end{pmatrix} \quad \begin{array}{c} | \\ \text{---} \\ \phi \\ \text{---} \\ | \end{array} \leftrightarrow \begin{pmatrix} \phi^0 \\ \phi^1 \end{pmatrix} \quad \begin{array}{c} | \quad | \\ \text{---} \quad \text{---} \\ \psi \quad \phi \\ \text{---} \quad \text{---} \\ | \quad | \end{array} \leftrightarrow \begin{pmatrix} \psi^0 \phi^0 \\ \psi^0 \phi^1 \\ \psi^1 \phi^0 \\ \psi^1 \phi^1 \end{pmatrix}$$

Последняя матрица содержит все способы образовать произведение числа из первой матрицы на число из второй матрицы. Она называется *кронекеровским произведением* матриц. Обозначим ϕ матрицу состояния ϕ . Тогда кронекеровское произведение можно записать более кратко в виде *блочной матрицы*:

$$\begin{array}{c} | \quad | \\ \text{---} \quad \text{---} \\ \psi \quad \phi \\ \text{---} \quad \text{---} \\ | \quad | \end{array} \leftrightarrow \begin{pmatrix} \psi^0 \phi \\ \psi^1 \phi \end{pmatrix}$$

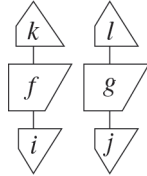
где $\psi_i \phi$ означает «умножить все элементы ϕ на ψ_i ». Кронекеровское произведение годится не только для матриц состояний, но и для произвольных процессов вида:



Теорема 5.53. Пусть f и g – процессы с матрицами \mathbf{f} и \mathbf{g} . Матрицей процесса $f \otimes g$ является кронекеровское произведение $\mathbf{f} \otimes \mathbf{g}$, определяемое формулой:

$$(\mathbf{f} \otimes \mathbf{g})_{ij}^{kl} := \mathbf{f}_i^k \mathbf{g}_j^l. \tag{5.32}$$

Доказательство. Элементы матрицы $f \otimes g$ имеют вид:



а это в точности соответствует определению (5.32). □

Если

$$\mathbf{f} := \begin{pmatrix} f_1^1 & \cdots & f_m^1 \\ \vdots & \ddots & \vdots \\ f_1^n & \cdots & f_m^n \end{pmatrix} \quad \mathbf{g} := \begin{pmatrix} g_1^1 & \cdots & g_{m'}^1 \\ \vdots & \ddots & \vdots \\ g_1^{n'} & \cdots & g_{m'}^{n'} \end{pmatrix},$$

то в терминах блочных матриц кронекеровское произведение является матрицей размера $(nn') \times (mm')$:

Это справедливо для матриц любого размера, поэтому мы можем вычислять кронекеровское произведение матриц состояний, эффектов и более общих процессов. Например, кронекеровское произведение матрицы состояний ψ размера 2×1 и матрицы процесса f размера 2×2 вычисляется следующим образом:

$$\begin{pmatrix} \psi^0 \\ \psi^1 \end{pmatrix} \otimes \begin{pmatrix} f_0^0 & f_1^0 \\ f_0^1 & f_1^1 \end{pmatrix} = \begin{pmatrix} \psi^0 \mathbf{f} \\ \psi^1 \mathbf{f} \end{pmatrix} = \begin{pmatrix} \psi^0 f_0^0 & \psi^0 f_1^0 \\ \psi^0 f_0^1 & \psi^0 f_1^1 \\ \psi^1 f_0^0 & \psi^1 f_1^0 \\ \psi^1 f_0^1 & \psi^1 f_1^1 \end{pmatrix}.$$

Упражнение 5.54. Выпишите матрицы следующих процессов:



в предположении, что все системы двумерные.

В заключение этого раздела рассмотрим транспонирование матриц составных систем. Как и раньше, при вычислении транспонированных матриц в теореме 5.19, до конца этого раздела будем предполагать, что все ОНБ самосопряженные.

В разделе 4.2.2 мы говорили, что существует два способа транспонирования процессов с составными системами на входе и выходе: обычное транспонирование, которое является просто поворотом, и алгебраическое транспонирование, в котором используются «перекрещенные» чашки и крышки. Для обычного транспонирования имеем:

$$\begin{array}{c} \triangle k \quad \triangle l \\ | \quad | \\ \text{---} f \text{---} \\ | \quad | \\ \triangle i \quad \triangle j \end{array} = \begin{array}{c} \triangle k \quad \triangle l \\ | \quad | \\ \text{---} f \text{---} \\ | \quad | \\ \triangle i \quad \triangle j \end{array} = \begin{array}{c} \triangle j \quad \triangle i \\ | \quad | \\ \text{---} f \text{---} \\ | \quad | \\ \triangle l \quad \triangle k \end{array} \quad (5.33)$$

а для алгебраического:

$$\begin{array}{c} \triangle k \quad \triangle l \\ | \quad | \\ \text{---} f^T \text{---} \\ | \quad | \\ \triangle i \quad \triangle j \end{array} = \begin{array}{c} \triangle k \quad \triangle l \\ | \quad | \\ \text{---} f \text{---} \\ | \quad | \\ \triangle i \quad \triangle j \end{array} = \begin{array}{c} \triangle i \quad \triangle j \\ | \quad | \\ \text{---} f \text{---} \\ | \quad | \\ \triangle k \quad \triangle l \end{array} \quad (5.34)$$

Как видим, транспонирование меняет местами верхние и нижние индексы и обращает порядок входов и выходов, тогда как алгебраическое транспонирование только меняет местами верхние и нижние индексы:

$$f_{ij}^{kl} \stackrel{(5.33)}{\sim} f_{lk}^{ji} \qquad f_{ij}^{kl} \stackrel{(5.34)}{\sim} f_{kl}^{ji}$$

Поэтому именно алгебраическое транспонирование соответствует обычному транспонированию матрицы, принятому в линейной алгебре:

$$\begin{pmatrix} f_{00}^{00} & f_{01}^{00} & f_{10}^{00} & f_{11}^{00} \\ f_{00}^{01} & f_{01}^{01} & f_{10}^{01} & f_{11}^{01} \\ f_{00}^{10} & f_{01}^{10} & f_{10}^{10} & f_{11}^{10} \\ f_{00}^{11} & f_{01}^{11} & f_{10}^{11} & f_{11}^{11} \end{pmatrix} \stackrel{(5.34)}{\sim} \begin{pmatrix} f_{00}^{00} & f_{01}^{01} & f_{10}^{10} & f_{11}^{11} \\ f_{01}^{00} & f_{01}^{01} & f_{10}^{10} & f_{11}^{11} \\ f_{10}^{00} & f_{10}^{01} & f_{10}^{10} & f_{11}^{11} \\ f_{11}^{00} & f_{11}^{01} & f_{11}^{10} & f_{11}^{11} \end{pmatrix}$$

Алгебраическое транспонирование также сохраняет старшее (левое) и младшее (правое) базисные состояния:

$$\begin{array}{c} \text{---} 6 \text{---} \\ | \quad | \quad | \end{array} = \begin{array}{c} \triangle 1 \quad \triangle 1 \quad \triangle 0 \\ | \quad | \quad | \end{array} = \begin{array}{c} \triangle 1 \quad \triangle 1 \quad \triangle 0 \\ | \quad | \quad | \end{array} = \begin{array}{c} \text{---} 6 \text{---} \\ | \quad | \quad | \end{array}$$

Сравним это с обычным, «поворотным» транспонированием. Оно удобно с диаграммной точки зрения, но плохо приспособлено для вычислений:



Поскольку сопряжение определяется через транспонирование, это различие проявляется и здесь тоже.

Упражнение 5.55. Покажите, что сопряжение обращает порядок индексов входов и выходов, а алгебраическое сопряжение – нет:

$$f_{ij}^{kl} \rightsquigarrow \overline{f_{ji}^{lk}} \quad \text{и} \quad f_{ij}^{kl} \rightsquigarrow \overline{f_{ij}^{kl}}$$

5.2.3. Матричная форма чашек и крышек

В настоящий момент у нас есть матричные аналоги последовательной и параллельной композиций, т. е. матричное представление схем. Чтобы получить матричное представление струнных диаграмм, нам еще нужны матричные аналоги чашек и крышек. Начнем с вычисления их матричной формы.

Предложение 5.56. Для любого ОНБ имеет место равенство

$$\cup = \sum_i \downarrow_i \downarrow_i \quad \text{и} \quad \cap = \sum_i \uparrow_i \uparrow_i \quad (5.35)$$

Доказательство. Разложение чашки по базису сразу вытекает из матричной формы тождественного процесса (5.17):

$$\cup = \sum_i \downarrow_i \downarrow_i$$

Для разложения крышки по базису нужно применить адъюнкцию. □

Таким образом, (5.35) дает матричную форму чашек и крышек в базисе произведения. Но этот базис произведения состоит не из двух копий одного и того же ОНБ, а из ОНБ и сопряженного с ним. На первый взгляд может даже показаться, что это нарушает законы разгибания, т. е.

$$\infty = \cup$$

Но это не так. В предложении 5.56 ключевым моментом является то, что оно справедливо для любого ОНБ. В частности, мы можем применить его к базису,

сопряженному с нашим исходным ОНБ, и получить следующую эквивалентную характеристику чашек и крышек:

$$\cup = \sum_i \downarrow_i \downarrow_i \quad \smile = \sum_i \uparrow_i \uparrow_i \quad (5.36)$$

Из этих двух эквивалентных форм сразу же следуют законы разгибания. Но этого осложнения можно избежать, если использовать самосопряженные ОНБ, поскольку в таком случае (5.35) принимает вид:

$$\cup = \sum_i \downarrow_i \downarrow_i \quad \smile = \sum_i \uparrow_i \uparrow_i \quad (5.37)$$

Замечание 5.57. Преобразуя равенства (5.37) в нотацию Дирака, мы получаем обычное определение состояния и эффекта Белла, встречающееся в литературе по квантовым вычислениям:

$$\sum_i \downarrow_i \downarrow_i = \sum_i |ii\rangle \quad \sum_i \uparrow_i \uparrow_i = \sum_i \langle ii|$$

Матрицы чашек и крышек в двумерном случае имеют вид:

$$\cup \leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \smile \leftrightarrow (1 \ 0 \ 0 \ 1)$$

Упражнение 5.58. Выпишите матрицы чашек и крышек в трех- и четырехмерном случае. Какая связь имеется между матрицей чашки (крышки) и единичной матрицей?

На самом деле мы могли бы принять (5.37) за определение чашек и крышек для системы типа A , а затем проверить уравнения разгибания непосредственно:

$$\begin{array}{c} \text{---} \\ \cup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \downarrow_i \quad \downarrow_i \\ \text{---} \end{array} = \sum_j \begin{array}{c} \text{---} \\ \uparrow_j \quad \uparrow_j \\ \text{---} \end{array} = \sum_{ij} \delta_{ij} \begin{array}{c} \text{---} \\ \downarrow_i \\ \text{---} \\ \uparrow_j \\ \text{---} \end{array} = \sum_i \begin{array}{c} \text{---} \\ \downarrow_i \\ \text{---} \\ \uparrow_i \\ \text{---} \end{array} = \left| \begin{array}{c} \text{---} \\ \downarrow_i \\ \text{---} \\ \uparrow_i \\ \text{---} \end{array} \right.$$

Упражнение 5.59. Докажите приведенное выше уравнение разгибания, не используя самосопряженный базис.

В конце раздела 5.1.1 мы высказали утверждение, что всегда можно выбрать (однозначно определенные) чашки и крышки, при которых заданный ОНБ становится самосопряженным. Теперь мы готовы показать, как выбирать такие чашки и крышки.

Предложение 5.60. ОНБ

$$\mathcal{B} := \left\{ \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \right\}_i$$

является самосопряженным тогда и только тогда, когда

$$\cup = \sum_i \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \begin{array}{c} \downarrow \\ \triangle \\ i \end{array}$$

Доказательство. В предположении, что чашка и крышка определены, как показано выше, мы вычисляем сопряжения к базисным состояниям из \mathcal{B} , транспонируя адьюнкты:

$$\begin{array}{c} \triangle \\ j \end{array} \cup = \begin{array}{c} \triangle \\ j \end{array} \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} = \sum_i \delta_i^j \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} = \begin{array}{c} \downarrow \\ \triangle \\ j \end{array}$$

Таким образом, каждое базисное состояние самосопряженное. Обратно, предположим, что чашки и крышки выбраны так, что базис \mathcal{B} самосопряженный, т. е. для всех i :

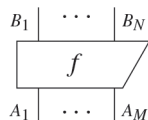
$$\begin{array}{c} \downarrow \\ \triangle \\ i \end{array} = \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \tag{5.38}$$

Тогда, применяя предложение 5.56, получаем:

$$\cup = \sum_i \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \stackrel{(5.38)}{=} \sum_i \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \quad \square$$

В принципе, матричные аналоги параллельной и последовательной композиций так же, как матрицы чашек и крышек, дают все необходимое для вычисления полной матрицы струнной диаграммы. Но есть и более прямой метод, с которым мы уже встречались в разделе 3.3.3 для частного случая **отношений**. Да, мы тогда не знали о струнных диаграммах, но, как выясняется, это и не важно.

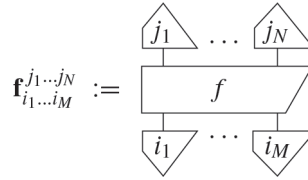
Напомним, что матрицу процесса



можно записать в виде:

$$\mathbf{f} = \left(\mathbf{f}_{i_1 \dots i_M}^{j_1 \dots j_N} \mid 0 \leq i_k < D_k, 0 \leq j_k < D'_k \right)$$

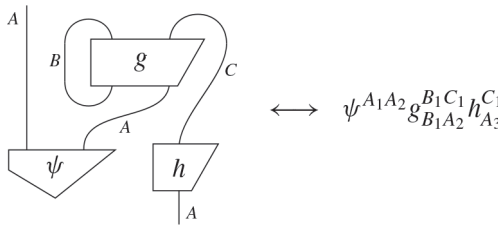
где D_k – размерность A , D'_k – размерность B_k и



Теорема 5.61. Матрицей диаграммы является диаграммная формула, получающаяся в результате следующих преобразований:

- имя блока f заменяется матрицей \mathbf{f} ;
- имена проводов A_k становятся индексами $0 \leq i_k < D_k$;
- по всем повторяющимся индексам производится суммирование.

Например, матрица \mathbf{m} диаграммы

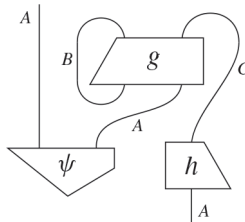


состоит из элементов

$$m_{i_3}^{i_1} = \sum_{i_2 j_1 k_1} \psi^{i_1 i_2} g_{j_1 i_2}^{j_1 k_1} h_{i_3}^{k_1}.$$

Если в диаграмме встречаются операции транспонирования, сопряжения или адьюнкции, то следует соответственно изменить элементы матрицы для таких процессов (см. теоремы 5.18 и 5.19).

Упражнение 5.62. Вычислите матрицу диаграммы



5.2.5. Матрицы как процессные теории

Матрицы – не только удобный способ описания процессов во многих процессных теориях, они также позволяют строить широкий спектр процессных теорий, допускающих струнные диаграммы.

Рассмотрим множество X , элементы которого будем записывать в виде $\diamond x$, $\diamond y$, ..., со следующими операциями:

- (i) умножение, обладающее свойствами параллельной (или, что эквивалентно, последовательной) композиции чисел, т. е.

$$\begin{aligned}
 (\diamond x \diamond y) \diamond z &= \diamond x (\diamond y \diamond z) & \boxed{} \diamond &= \diamond \\
 \diamond x \diamond y &= \diamond y \diamond x & 0 \diamond &= 0
 \end{aligned}$$

- (ii) сумма, удовлетворяющая условиям определения 5.21:

$$\diamond x + 0 = \diamond x \qquad \left(\sum_i \diamond x_i \right) \diamond y = \sum_i \diamond x_i \diamond y$$

- (iii) (возможно, тривиальная) операция сопряжения, удовлетворяющая свойствам адьюнкции (или, что эквивалентно, сопряжения) чисел:

$$\overline{(\diamond x)} = \diamond x \qquad \overline{(\diamond x \diamond y)} = \diamond \bar{x} \diamond \bar{y} \qquad \overline{\left(\sum_i \diamond x_i \right)} = \sum_i \diamond \bar{x}_i$$

Тогда можно определить процессную теорию, процессами которой будут матрицы с элементами из X . На самом деле все необходимое для определения этой процессной теории уже проделано, поскольку мы теперь знаем, как строить из комбинаций матриц струнные диаграммы, как выполнять адьюнкцию, транспонирование и т. д. Поэтому задание множества чисел X сообщает все, что нужно знать о процессах новой теории.

Но каковы в ней системные типы? Они должны способствовать композиции процессов. Для матриц возможность композиции определяется просто количеством строк и столбцов. Поэтому в качестве типов можно взять натуральные числа \mathbb{N} . Поскольку числа – это матрицы размера 1×1 , типу «отсутствие провода» соответствует «1».

Эту идею можно формализовать.

Определение 5.63. Пусть X – множество чисел с операциями композиции и суммирования, удовлетворяющими условиям выше. Процессная теория **matrices**(X) строится следующим образом:

- (1) системами являются натуральные числа \mathbb{N} ;
- (2) процессами с входным типом $m \in \mathbb{N}$ и выходным типом $n \in \mathbb{N}$ являются все матрицы размера $n \times m$ с элементами, принадлежащими X ;
- (3) диаграммы вычисляются, как в теореме 5.61.

Разумеется, правило (3) можно было бы расписать подробнее:

- (3a) чашки и крышки – это матрицы, вычисленные в упражнении 5.58;
- (3b) в роли адьюнкции выступает сопряженное транспонирование матриц;
- (3c) параллельная композиция определяется кронекеровским произведением;
- (3d) последовательная композиция определяется произведением матриц.

Кроме того, в этой главе мы видели, что матрицы могут точно представлять процессы в процессной теории, где у всех системных типов имеется конечный ОНБ. Поэтому следующий результат не должен вызывать удивления.

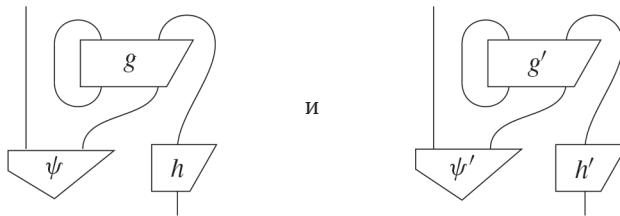
Теорема 5.64. Если для некоторой процессной теории выполняются условия:

- (1) у каждого системного типа имеется конечный ОНБ;
- (2) существует по меньшей мере один системный тип любой размерности $D \in \mathbb{N}$;
- (3) процессы одного типа допускают суммирование, –

и если множество чисел этой процессной теории равно X , то такая процессная теория эквивалентна процессной теории $\mathbf{matrices}(X)$.

А как понимать эквивалентность двух процессных теорий? Этот вопрос тоньше, чем может показаться на первый взгляд. Наивный подход состоит в том, чтобы просто потребовать выполнения следующих условий:

- существует взаимно однозначное соответствие между системными типами A, B, \dots теории 1 и системными типами A', B', \dots теории 2;
- для всех системных типов A, B (и соответствующих им системных типов A', B') существует взаимно однозначное соответствие между процессами, отображающими A в B в теории 1, и процессами, отображающими A' в B' в теории 2;
- эти взаимно однозначные соответствия сохраняют струнные диаграммы, например если ψ, g, h соответствуют ψ', g', h' , то соответствуют друг другу также диаграммы



Однако такое понятие эквивалентности зачастую оказывается слишком строгим. Например, если в процессной теории много типов с n -элементными ОНБ, то в теории $\mathbf{matrices}(X)$ все они «склеятся» в один тип « n ». Но для всех практических надобностей теория $\mathbf{matrices}(X)$ «эквивалентна» процессной теории, с которой мы начали. Интуитивно эквивалентные процессные теории определены, как описано выше, но с дополнительной возможностью «склеивать» практически одинаковые типы (в данном случае типы одной размерности). Этого описания эквивалентности достаточно для наших целей, а читателей, интересующихся деталями, отсылаем к разделу* 5.6.4.

Замечание* 5.65. Как описано в разделе* 5.6.4, это более тонкое понятие эквивалентности в теории категорий известно под названием *эквивалентность категорий*, тогда как наивное понятие называется *изоморфизмом категорий*.

В случае теории **отношений** мы уже видели в примере 5.17, что числами являются булевы величины \mathbb{B} . Обозначим **finrelations** подтеорию теории **отношений**, которая получается, если ограничить типы конечными множествами. Чтобы установить эквивалентность между теориями **finrelations** и $\mathbf{matrices}(\mathbb{B})$, мы должны идентифицировать все множества с одинаковым числом элементов. Сделав это, мы приходим к следующему выводу.

Следствие 5.66. Теория **finrelations** эквивалентна теории $\mathbf{matrices}(\mathbb{B})$.

Но можно выбрать много других множеств чисел X для построения теорий, допускающих струнные диаграммы, например: натуральные числа \mathbb{N} , целые числа \mathbb{Z} , рациональные числа \mathbb{Q} , вещественные числа \mathbb{R} или совсем уж эксцентричные «числа» типа открытых множеств в топологическом пространстве.

Упражнение* 5.67. Рассмотрим процессную теорию $\mathbf{matrices}(\mathbb{Z}_2)$, т. е. матрицы над полем с двумя элементами, которое отличается от \mathbb{B} тем, что $1 + 1 = 0$, а не $1 + 1 = 1$. Каковы ее свойства? Как она соотносится с теорией **отношений**? Заметим, что «полный» ответ на этот вопрос все еще является темой активных исследований.

5.3. ГИЛЬБЕРТОВЫ ПРОСТРАНСТВА

Теперь мы готовы определить процессную теорию гильбертовых и линейных отображений, и это станет важным шагом на пути к теории квантовых процессов. На самом деле почти все фрагменты головоломки уже на месте. Осталось только сказать, что такое числа.

5.3.1. От диаграмм к линейным отображениям и гильбертовым пространствам

В примере 3.35 мы видели, что в теории **функций** множество чисел тривиально, т. е. существует всего одно число. В примере 3.36 мы видели, что в теории **отношений** существует два числа, 0 и 1, соответствующих понятиям «невозможно» и «возможно». Только что мы видели, что можно построить процессную теорию, задав произвольное множество чисел, например все вещественные числа. Для гильбертовых пространств и линейных отображений даже вещественных чисел недостаточно. У новых чисел, которые нам понадобятся (впервые в этой книге), будет нетривиальная операция сопряжения, поэтому адъюнкция не будет совпадать с транспонированием. Иными словами, мы наконец-то сможем задействовать все богатство струнных диаграмм.

Определение 5.68. Процессная теория **линейных отображений** – это множество всех процессов, описываемых струнными диаграммами, удовлетворяющее следующим условиям:

- 1) у каждого типа имеется конечный ОНБ;
- 2) существует по меньшей мере один системный тип каждой размерности $D \in \mathbb{N}$;
- 3) процессы одного типа допускают суммирование;
- 4) числами является множество комплексных чисел \mathbb{C} .

Гильбертово пространство – это системный тип в теории **линейных отображений**, а D -мерные системы, предполагаемые в условии (2), мы будем обозначать \mathbb{C}^D .

Прежде всего отметим, что в определении 5.68 не сказано, что же такое гильбертово пространство. Нам достаточно знать, что это некоторый тип, который говорит, как компоновать линейные отображения. На самом деле из теоремы 5.64 нам известно, что теорию **линейных отображений** можно было бы определить как эквивалент теории $\mathbf{matrices}(\mathbb{C})$, поэтому для наших целей в качестве системных типов можно было бы с тем же успехом взять просто множество нату-

ральных чисел (т. е. размерностей). Это полностью согласуется с нашим обычным отношением к процессам как к вещи, более важной, чем системы. Для тех, кого это упущение беспокоит, в разделе 5.4.2 будет дано стандартное теоретико-множественное определение гильбертовых пространств и показано, как оно соотносится с определением 5.68.

Мы также еще не напомнили, что такое *комплексное число*. Но прежде мы хотим подчеркнуть, что большую часть материала в этой книге можно понять без основательного знакомства с комплексными числами, потому что, как было упомянуто во введении, наша конечная цель – заменить матрицы комплексных чисел диаграммами. Комплексное число представляет собой пару вещественных чисел $a, b \in \mathbb{R}$, записываемую в виде:

$$a + ib. \tag{5.39}$$

Вычисления с комплексными и действительными числами похожи, нужно только принять дополнительное соглашение:

$$i^2 = -1.$$

Из условия (4) в определении 5.68 должно быть понятно, что композиция чисел – это обычное *умножение комплексных чисел*:

$$\diamond_{\lambda_1} \diamond_{\lambda_2} \rightsquigarrow (a_1 + ib_1)(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2);$$

суммирование определяется *сложением комплексных чисел*:

$$\diamond_{\lambda_1} + \diamond_{\lambda_2} \rightsquigarrow (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2),$$

а потому 0 («всепоглощающая» диаграмма) и 1 (пустая диаграмма) – это обычные числа 0 и 1 в поле \mathbb{C} . Наконец, операции сопряжения чисел соответствует *комплексное сопряжение*:

$$\diamond_{\lambda} \mapsto \widehat{\diamond_{\lambda}} \rightsquigarrow a + ib \mapsto a - ib.$$

Очень важно, что это сопряжение не тривиально!

Замечание* 5.69. На самом деле если мы хотим, чтобы инволюция сохраняла суммы и произведения, то сопряжение обязано быть тривиальным для вещественных чисел. Более того, комплексное сопряжение – единственная (нетривиальная) инволюция, сохраняющая суммы и произведения комплексных чисел, являющаяся продолжением этой операции с подмножества \mathbb{R} .

Продолжая пример 5.26, заметим, что комплексные числа образуют *поле*, т. е. помимо вычитания определено *деление на числа, не равные нулю*. То есть для любого $\lambda \neq 0$ существует такое число $1/\lambda$, что:

$$\diamond_{\lambda} \diamond_{\frac{1}{\lambda}} = \boxed{}$$

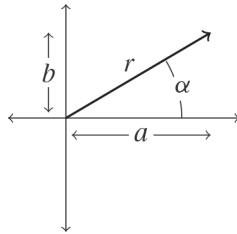
Комплексные числа можно также записывать в *полярной форме*:

$$re^{i\alpha}, \tag{5.40}$$

где r – положительное вещественное число, а α – угол, называемый *комплексной фазой*. Формы (5.39) и (5.40) связаны следующими соотношениями:

$$\begin{cases} a = r \cos(\alpha) \\ b = r \sin(\alpha) \end{cases} \quad \begin{cases} r = \sqrt{a^2 + b^2} \\ \alpha = \arctan\left(\frac{b}{a}\right) \end{cases}$$

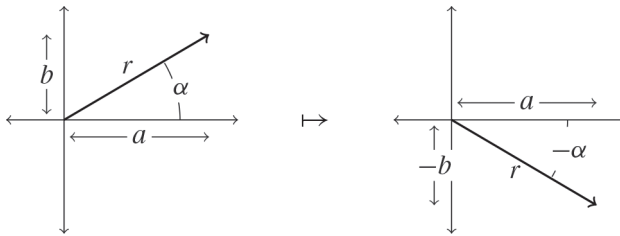
которые можно наглядно представить на *комплексной плоскости*:



Легко видеть, что операция сопряжения сводится к изменению знака комплексной фазы:

$$re^{i\alpha} \mapsto re^{-i\alpha}.$$

То есть это просто отражение комплексной плоскости относительно горизонтальной оси:



Наш выбор «отражения» для представления сопряжения на диаграммах продиктован следующим фактом:

$$\diamond \lambda = \begin{array}{c} \triangle \phi \\ | \\ \nabla \psi \end{array} \mapsto \begin{array}{c} \triangle \phi \\ | \\ \nabla \psi \end{array} = \diamond \bar{\lambda}$$

5.3.2. От сопряжения к положительности

Обычно комплексное число называют «положительным», если оно вещественное и ≥ 0 . Поскольку числа – частный случай процессов, это определение должно быть

согласовано с введенным ранее понятием «положительности» для процессов. Так оно и есть.

Предложение 5.70. Для комплексного числа λ следующие утверждения эквивалентны:

1. Оно вещественное и ≥ 0 .
2. Существует комплексное число μ такое, что:

$$\diamond \lambda = \diamond \mu \diamond \mu \tag{5.41}$$

3. Оно положительное в смысле определения 4.60, т. е. существует такое ψ , что:

$$\diamond \lambda = \begin{array}{c} \psi \\ \hline \psi \end{array} \tag{5.42}$$

Доказательство. Чтобы доказать импликацию $(1 \Rightarrow 2)$, предположим, что λ вещественное и ≥ 0 . Тогда, положив $\mu = \bar{\mu} = \sqrt{\lambda}$, будем иметь равенство (5.41). Импликация $(2 \Rightarrow 3)$ очевидна, т. к. (5.41) – частный случай (5.42). Для доказательства импликации $(3 \Rightarrow 1)$ сначала заметим, что произведение любого комплексного числа на сопряженное к нему вещественно и ≥ 0 :

$$\bar{\mu}\mu = (a + ib)(a - ib) = a^2 + b^2.$$

Вычисляя λ в (5.42) с использованием матрицы ψ , получаем:

$$\lambda = \begin{pmatrix} \overline{\psi^1} & \overline{\psi^2} & \dots & \overline{\psi^n} \end{pmatrix} \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = \sum_i \overline{\psi_i} \psi_i.$$

Это сумма чисел вида $\bar{\mu}\mu$, поэтому она вещественна и ≥ 0 . □

В примере* 4.41 мы сказали, что транспонирование в теории **линейных отображений** не дает «хороших» адьюнктов. В частности, для транспонирования не выполняется свойство положительной определенности:

$$\begin{array}{c} \psi \\ \hline \psi \end{array} = 0 \iff \begin{array}{c} | \\ \hline \psi \end{array} = 0 \tag{5.43}$$

Теперь мы готовы подкрепить это заявление, а затем показать, как комплексное сопряжение решает проблему.

Сначала рассмотрим (неправильное) выражение положительной определенности, в которое входит транспонирование:

$$(\psi^1 \ \psi^2 \ \dots \ \psi^n) \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = 0 \iff \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Это так для вещественных чисел, но неверно для комплексных. Например:

$$(1 \ i) \begin{pmatrix} 1 \\ i \end{pmatrix} = 1 + (-1) = 0, \quad \text{хотя} \quad \begin{pmatrix} 1 \\ i \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Проблема в том, что для комплексных чисел, в отличие от вещественных, $(\psi^i)^2$ может быть меньше нуля (в данном случае равно -1). Именно поэтому в (5.43) нам нужно сопряженное транспонирование, т. е. адьюнкция. Преобразуя в матричную форму, получаем:

$$(\overline{\psi^1} \ \overline{\psi^2} \ \dots \ \overline{\psi^n}) \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = 0 \iff \begin{pmatrix} \psi^1 \\ \psi^2 \\ \vdots \\ \psi^n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

или эквивалентно:

$$\sum_i \overline{\psi^i} \psi^i = 0 \iff \text{для всех } i : \psi^i = 0. \quad (5.44)$$

В силу предложения 5.70 все числа $\overline{\psi^i} \psi^i$ вещественны и больше или равны 0. Поэтому если бы хотя бы одно ψ^i было отлично от нуля, то сумма в (5.44) была бы больше нуля.

5.3.3. Почему математики любят комплексные числа

В этом разделе мы рассмотрим различные причины, по которым переход к комплексным числам существенно упрощает жизнь математиков. Хотя многие результаты этого раздела опираются на явное представление линейных отображений в матричной форме, позже мы сумеем дать для них диаграммные аналоги.

5.3.3.1. Спектральная теорема

Как было обещано в разделе 5.1.6, приведем следующую теорему.

Теорема 5.71. Любое самоадьюнктное линейное отображение f является диагонализуемым, т. е. существует ОНБ такой, что

$$\begin{array}{c} | \\ \diagdown \\ f \\ \diagup \\ | \end{array} = \sum_i r_i \begin{array}{c} | \\ \diagdown \\ i \\ \diagup \\ i \\ | \end{array} \quad (5.45)$$

где все r_i – вещественные числа. Кроме того, если f положительно, то $r_i \geq 0$ для всех i , а если f – проектор, то $r_i \in \{0, 1\}$ для всех i . Следовательно, любой проектор P можно записать в виде:

$$\begin{array}{|c} \hline P \\ \hline \end{array} = \sum_i \begin{array}{|c} \hline i \\ \hline \end{array} \begin{array}{|c} \hline i \\ \hline \end{array}$$

для некоторого ортонормированного множества (необязательно полного ОНБ).

Доказательство. Мы лишь наметим доказательство, поскольку полностью его можно найти в любом учебнике линейной алгебры. Оно состоит из двух основных частей. Первая – стандартный результат, согласно которому у любого линейного отображения системы в себя имеется, по крайней мере, одно собственное состояние. Это следствие того факта, что числа в теории **линейных отображений** – это комплексные числа, и «основной теоремы алгебры». Вторая часть – то, что самодъюнктные линейные отображения сохраняют ортогональность собственным состояниям, т. е. для любого собственного состояния ψ , если ϕ ортогонально ψ , то это верно и для $f \circ \phi$:

$$\begin{array}{|c} \hline \psi \\ \hline \end{array} \begin{array}{|c} \hline f \\ \hline \end{array} \begin{array}{|c} \hline \phi \\ \hline \end{array} = \begin{array}{|c} \hline \psi \\ \hline \end{array} \begin{array}{|c} \hline f \\ \hline \end{array} \begin{array}{|c} \hline \phi \\ \hline \end{array} = \bar{\lambda} \begin{array}{|c} \hline \psi \\ \hline \end{array} \begin{array}{|c} \hline \phi \\ \hline \end{array} = 0$$

Это позволяет продолжать выбор новых собственных состояний для f , ортогональных всем ранее выбранным, до тех пор пока не будет построен ОНБ. Коль скоро установлена диагонализируемость f , тот факт, что все r_i в теореме 5.71 вещественные, положительные или принадлежат множеству $\{0, 1\}$, следует из предложения 5.44. □

Теорема 5.71 называется *спектральной теоремой*. Нам особенно важна ее эквивалентная формулировка, приведенная ниже. Сначала подставим (5.45) в условие двойственности процессов и состояний

$$\begin{array}{|c} \hline f \\ \hline \end{array} = \sum_i r_i \begin{array}{|c} \hline i \\ \hline \end{array} \begin{array}{|c} \hline i \\ \hline \end{array}$$

а затем воспользуемся соответствиями, установленными в разделе 4.3.6.

Следствие 5.72. Для любого самосопряженного двухкомпонентного состояния ψ в теории **линейных отображений** существует такой ОНБ, что:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \psi \\ \text{---} \\ \text{---} \end{array} = \sum_i r_i \begin{array}{c} \text{---} \\ \text{---} \\ i \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ i \\ \text{---} \\ \text{---} \end{array} \quad (5.46)$$

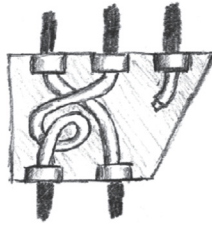
где все r_i – вещественные числа. Если $\psi \otimes$ -положительно, то $r_i \geq 0$ для всех i .

Объясним происхождение слово «спектральный» в названии «спектральная теорема».

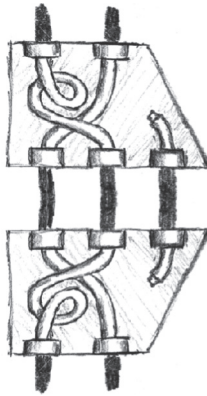
Определение 5.73. Для самоадьюнктного линейного отображения f будем называть список (r_i) из теоремы 5.71 *спектром* f и обозначать его $\text{spec}(f)$. Аналогично для самосопряженного двухкомпонентного состояния ψ будем называть числа из следствия 5.72 *спектром* ψ и обозначать $\text{spec}(\psi)$.

В разделе 8.2.5 мы приведем диаграммные аналоги теоремы 5.71 и следствия 5.72.

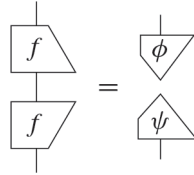
А теперь воспользуемся спектральной теоремой для доказательства одного факта об адьюнктах **линейных отображений**, который вытекает, если всерьез принять идею адьюнкции как отражения. Пусть имеется \circ -неразделимый процесс. Можно представить, что у него имеется некоторая внутренняя структура, например набор трубок или механизмов, соединяющих некоторые входы с выходами:



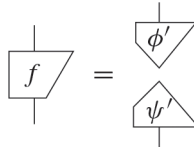
Если построить композицию этого процесса с его адьюнктом, т. е. вертикальное отражение, то эти внутренние соединения совместятся:



поэтому следует ожидать, что результирующий процесс тоже будет \circ -неразделимым. Следовательно, если композиция процесса с его адьюнктом \circ -разделима:



то и сам процесс должен быть \circ -разделимым:

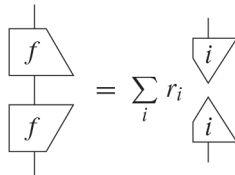


И действительно, спектральная теорема гарантирует, что композиция $f^\dagger \circ f$ является критерием разделимости f .

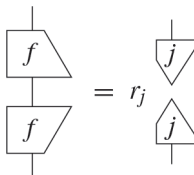
Предложение 5.74. Для любого линейного отображения f имеет место:

$$\left(\exists \psi, \phi : \begin{array}{c} \text{trapezoid } f \\ \text{trapezoid } f \end{array} = \begin{array}{c} \text{inverted trapezoid } \phi \\ \text{inverted trapezoid } \psi \end{array} \right) \iff \left(\exists \psi', \phi' : \text{trapezoid } f = \begin{array}{c} \text{inverted trapezoid } \phi' \\ \text{inverted trapezoid } \psi' \end{array} \right). \quad (5.47)$$

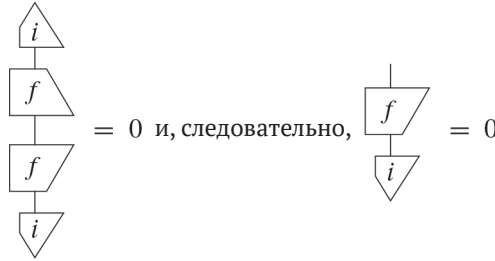
Доказательство. В направлении (\Leftarrow) утверждение тривиально. Для доказательства (\Rightarrow) предположим, что композиция $f^\dagger \circ f$ является \circ -разделимой. Тогда, будучи положительной, она допускает диагонализацию:



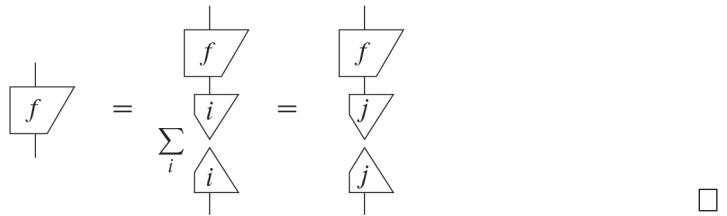
но раз так, то в силу \circ -разделимости $f^\dagger \circ f$ должно выполняться равенство



для некоторого j . В противном случае процесс $f^\dagger \circ f$ мог бы породить на выходе (ненулевые) ортогональные состояния, что невозможно, если он \circ -разделимый. Поэтому для всех $i \neq j$



в силу положительной определенности. Разрешение единицы завершает доказательство:



Замечание 5.75. Обратите внимание на аналогию между условием (5.47) и положительной определенностью. Если положительная определенность означает, что по числу $\psi^\dagger \circ \psi$ можно узнать, является ли нулевым состояние ψ , то условие (5.47) говорит, что по композиции $f^\dagger \circ f$ можно узнать, является ли процесс $f \circ$ -разделимым.

А теперь самое интересное. В примере 4.40 мы установили, что **отношения** удовлетворяют условию положительной определенности, но вот условию (5.47) эта теория не удовлетворяет.

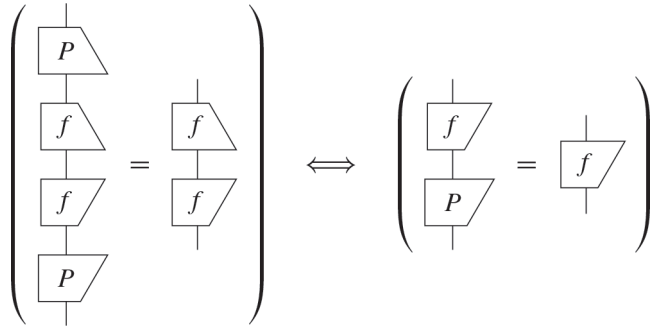
Упражнение 5.76. Проверьте, что отношение с матрицей

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

не удовлетворяет условию (5.47).

Таким образом, в теории **отношений** интуитивное предположение о том, что разделимость $f^\dagger \circ f$ влечет за собой разделимость f , оказывается неверным, и причина этого кроется в том, что для **отношений** неверна спектральная теорема. А это, в свою очередь, связано с тем, что в теории **отношений** попросту недостаточно чисел, чтобы гарантировать существование диагонального представления для каждого отношения.

Упражнение 5.77. Следуя по пути, намеченному в предложении 5.74, воспользуйтесь спектральной теоремой для доказательства того, что $f^\dagger \circ f$ обнаруживает, является ли f инвариантным относительно проектора. То есть покажите, что для любого проектора P



5.3.3.2. Теорема о размерности

В разделе 5.1.1 мы определили $\dim(A)$ как размер наименьшего базиса типа A . Это не очень удобно практически, поскольку, захоти мы найти размерность A , придется перебирать все базисы A , чтобы найти среди них наименьший. По счастью, в теории **линейных отображений** этого делать не нужно, потому что комплексные числа образуют поле. Поэтому мы можем опереться на *теорему о размерности*.

Теорема 5.78. Если процессная теория допускает матричное исчисление и ее числа образуют поле, то все базисы данного типа A имеют одинаковый размер, $\dim(A)$.

Благодаря теореме о размерности в теории **линейных отображений** $\dim(A)$ равна размеру любого базиса A . Как следствие любое ортонормированное множество размера $\dim(A)$ является ОНБ. Чтобы убедиться в этом, понадобится только лишь следующее

Предложение 5.79. Любое ортонормированное множество

$$A = \left\{ \begin{array}{c} \downarrow \\ i \\ \uparrow \end{array} \right\}$$

можно расширить до ОНБ, содержащего A .

Доказательство. Нетрудно показать, что

$$P := \sum_i \begin{array}{c} \downarrow \\ i \\ \uparrow \end{array} \quad \text{и} \quad Q := \left| \begin{array}{c} \downarrow \\ i \\ \uparrow \end{array} \right. - P$$

являются проекторами. В силу спектральной теоремы мы можем диагонализировать Q относительно второго ортонормированного множества состояний A' :

$$Q = \sum_i \begin{array}{c} \downarrow \\ i \\ \uparrow \\ i \\ \uparrow \end{array}$$

Из того, что P – проектор, сразу следует, что $P \circ Q = 0$, а отсюда столь же легко вывести, что все состояния из \mathcal{A}' должны быть ортогональны состояниям из \mathcal{A} . Далее, поскольку

$$\sum_i \begin{array}{|c} \triangle \\ \hline i \end{array} + \sum_i \begin{array}{|c} \triangle \\ \hline i \end{array} = \begin{array}{|c} \square \\ \hline P \end{array} + \begin{array}{|c} \square \\ \hline Q \end{array} = \left| \right.$$

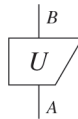
$\mathcal{A} \cup \mathcal{A}'$ дает разрешение единицы и, следовательно, по теореме 5.32, $\mathcal{A} \cup \mathcal{A}'$ является ОНБ, который, очевидно, содержит \mathcal{A} . □

Таким образом, если имеется ортонормированное множество \mathcal{A} размера $\dim(\mathcal{A})$, то существует ОНБ \mathcal{B} , содержащий \mathcal{A} . Но по теореме 5.78 \mathcal{B} должен иметь размер $\dim(\mathcal{A})$, поэтому $\mathcal{A} = \mathcal{B}$.

Следствие 5.80. Любое ортонормированное множество размера $\dim(\mathcal{A})$ является ОНБ.

Теперь посмотрим, как теорема о размерности может по-настоящему облегчить нам жизнь (а не просто сделать ее «не такой противной»). Напомним, что в предложениях 5.37 и 5.38 мы охарактеризовали изометрические и унитарные процессы в терминах их поведения на ортонормированных множествах. В сочетании с теоремой о размерности это дает нам следующее

Предложение 5.81. Для любой изометрии



$\dim(\mathcal{A}) \leq \dim(\mathcal{B})$, а если $\dim(\mathcal{A}) = \dim(\mathcal{B})$, то процесс U унитарный. В частности, любая изометрия гильбертова пространства в себя обязательно унитарна.

Доказательство. Из предложения 5.79 следует, что любое ортонормированное множество на B должно иметь размер $\leq \dim(B)$. Далее, по предложению 5.37, процесс U переводит любой ОНБ \mathcal{B} на A в ортонормированное множество \mathcal{B}' размера $\dim(\mathcal{A})$. Таким образом, $\dim(\mathcal{A}) \leq \dim(\mathcal{B})$. Если $\dim(\mathcal{A}) = \dim(\mathcal{B})$, то в силу следствия 5.80 \mathcal{B}' является ОНБ для B . Поэтому в силу предложения 5.38 U унитарный. □

5.3.4. Классические логические вентили как линейные отображения

Мы предположили, что гильбертовы пространства \mathbb{C}^n существуют для любого n . Особый интерес представляет пространство \mathbb{C}^2 в связи с его ролью в квантовых вычислениях, а именно в описании квантовых битов, или *кубитов*. Гильбертово пространство \mathbb{C}^2 имеет базис из двух элементов:

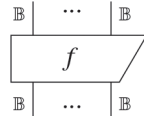
$$\left\{ \begin{array}{|c} \triangle \\ \hline 0 \end{array}, \begin{array}{|c} \triangle \\ \hline 1 \end{array} \right\}$$

который называется *вычислительным базисом*, или *Z-базисом*. По аналогии с (классическими) битами мы будем нумеровать элементы базиса \mathbb{C}^2 , начиная с нуля.

Замечание 5.82. В нотации Дирака эти базисные состояния обозначаются

$$\{|0\rangle, |1\rangle\}.$$

Классическими *логическими вентилями* называются функции:



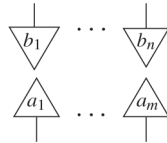
из которых строятся цифровые схемы. Благодаря вычислительному базису мы теперь можем записать любой логический вентиль в виде линейного отображения, применив следующее преобразование для $a, b \in \{0, 1\}$:

$$a \mapsto b \quad \rightsquigarrow \quad \begin{array}{c} \downarrow \\ a \end{array} \mapsto \begin{array}{c} \downarrow \\ b \end{array}$$

или в общем случае для $a_1, \dots, a_m, b_1, \dots, b_n \in \{0, 1\}$:

$$a_1 \cdots a_m \mapsto b_1 \cdots b_n \quad \rightsquigarrow \quad \begin{array}{c} \downarrow \\ a_1 \end{array} \cdots \begin{array}{c} \downarrow \\ a_m \end{array} \mapsto \begin{array}{c} \downarrow \\ b_1 \end{array} \cdots \begin{array}{c} \downarrow \\ b_n \end{array}$$

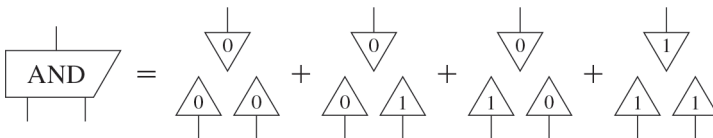
Каждое такое отображение одного конкретного входа вносит член:



а все линейное отображение получается как сумма всех членов такого вида. Например, *вентиль AND*

$$\text{AND} :: \begin{cases} (0, 0) \mapsto 0 \\ (0, 1) \mapsto 0 \\ (1, 0) \mapsto 0 \\ (1, 1) \mapsto 1 \end{cases}$$

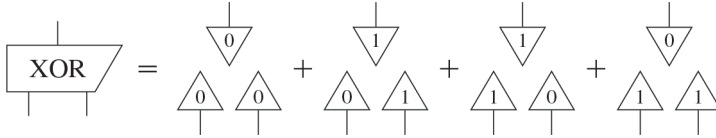
индуцирует линейное отображение



А для вентилей исключающее OR, или XOR,

$$\text{XOR} :: \begin{cases} (0, 0) \mapsto 0 \\ (0, 1) \mapsto 1 \\ (1, 0) \mapsto 1 \\ (1, 1) \mapsto 0 \end{cases}$$

индуцированное линейное отображение имеет вид:



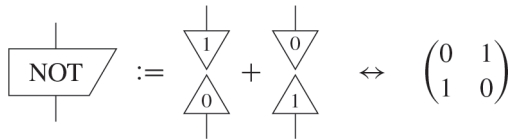
В главе 12 мы увидим, что этот процесс преобразования логических вентилей в линейные отображения играет ключевую роль в *схемной модели квантовых вычислений*. Однако в этом контексте приходится ограничиваться логическими вентилями, которые порождают унитарные линейные отображения, по причинам, которые станут понятны в следующей главе. Определенное же выше линейное отображение AND не является унитарным. У него даже нет обратного отображения.

Упражнение 5.83. Покажите, что логический вентиль определяет унитарное линейное отображение тогда и только тогда, когда он обратим (см. определение 4.24).

Простой пример обратимого логического вентиля дает вентиль NOT:

$$\text{NOT} :: \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$$

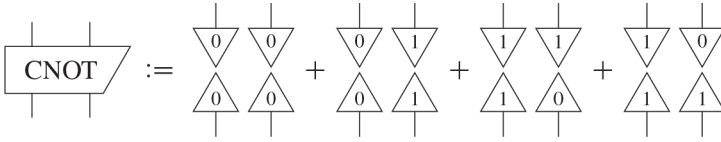
индуцирующий линейное отображение



Еще один важный пример дает вентиль *управляемое NOT*, или CNOT:

$$\text{CNOT} :: \begin{cases} (0, 0) \mapsto (0, 0) \\ (0, 1) \mapsto (0, 1) \\ (1, 0) \mapsto (1, 1) \\ (1, 1) \mapsto (1, 0) \end{cases}$$

Это вентиль называется управляемым NOT, потому что первый бит «управляет» применением NOT ко второму биту. Индуцированное им линейное отображение имеет вид:

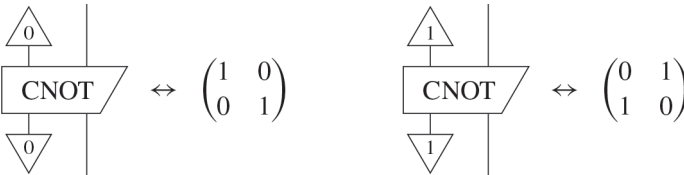


а его матрица равна

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

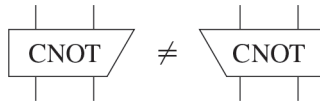
Упражнение 5.84. Воспользовавшись предложением 5.38, докажите, что линейные отображения NOT и CNOT унитарны.

Заметим, что в левом верхнем углу матрицы линейного отображения CNOT находится единичная матрица. Это общая черта матриц «контролируемых» вентилях, поскольку первый элемент базиса «выбирает», какую из двух меньших матриц применять ко второму:



Заметим также, что линейное отображение CNOT является самоадьюнктным, и это оправдывает диаграммное представление, инвариантное относительно вертикального отражения, с которым мы встретимся в следующем разделе. С другой стороны, относительно горизонтального отражения оно не инвариантно.

Упражнение 5.85. Докажите, что линейное отображение CNOT не инвариантно относительно горизонтального отражения.



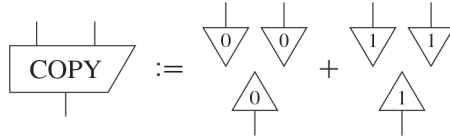
Поэтому и его диаграммное представление тоже не должно быть инвариантно.

5.3.5. X-базис и линейное отображение Адамара

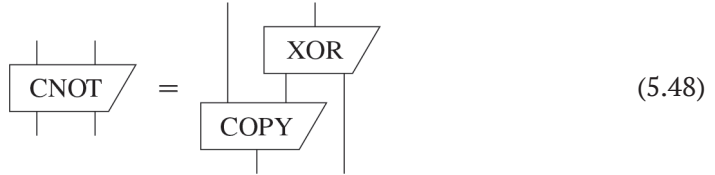
Альтернативный взгляд на вентиль CNOT дает вентиль COPY:

$$\text{COPY} :: \begin{cases} 0 \mapsto (0, 0) \\ 1 \mapsto (1, 1) \end{cases}$$

индуцирующий линейное отображение



Один из способов выполнить CNOT состоит в том, чтобы применить COPY к первому биту, а затем XOR – к копии первого бита и второму биту:

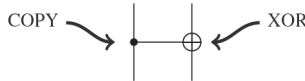


Упражнение 5.86. Докажите равенство (5.48).

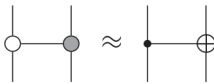
В большинстве учебников вентиль CNOT записывается так:



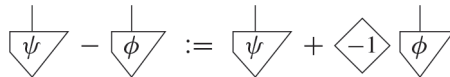
Это та же самая интерпретация CNOT в виде COPY+XOR, если учесть, что в классических схемах копирование обычно представляется маленькой черной точкой, а операция XOR – символом \oplus :



Однако мы будем пользоваться более симметричной нотацией:



Это объясняется тем, что линейные отображения XOR и COPY очень тесно связаны. Оба они являются отображением COPY, но в разных базисах. Чтобы убедиться в этом, рассмотрим другой базис в \mathbb{C}^2 . Прежде всего заметим, что поскольку $-1 \in \mathbb{C}$, состояния можно вычитать:



Определим такой X -базис:

$$\begin{array}{c} \downarrow \\ 0 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \right) \qquad \begin{array}{c} \downarrow \\ 1 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} - \begin{array}{c} \downarrow \\ 1 \end{array} \right)$$

Легко проверить, что

$$\begin{array}{c} \uparrow \\ j \\ \downarrow \\ i \end{array} = \delta_i^j$$

и поскольку оба эти состояния имеют вещественные коэффициенты в Z -базисе, они являются самосопряженными. Таким образом, мы имеем два самосопряженных ОНБ в \mathbb{C}^2 :

$$\left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\} \qquad \text{и} \qquad \left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\}$$

Замечание 5.87. В нотации Дирака X -базис обычно обозначается

$$\{|+\rangle, |-\rangle\}.$$

Это отражает тот факт, что мы берем сумму и разность состояний в Z -базисе. Мы будем использовать эти базисы в разделе 6.1.2, чтобы пометить оси Z и X на сфере состояний кубита, именно поэтому выбраны странные, на первый взгляд, названия « Z -базис» и « X -базис».

Теперь мы можем определить два варианта всех показанных ранее отображений: одно в Z -базисе, другое в X -базисе. Вот как выглядят два варианта линейного отображения COPY:

$$\begin{array}{c} \text{Z-COPY} \end{array} := \sum_i \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \uparrow \\ i \end{array} \qquad \begin{array}{c} \text{X-COPY} \end{array} := \sum_i \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \uparrow \\ i \end{array}$$

Очевидно, что такие отображения COPY имеют смысл в гильбертовом пространстве любой размерности n . Впоследствии мы будем использовать их так часто, что удобно записывать их просто кружочками подходящего цвета:

$$\begin{array}{c} \text{white circle} \end{array} := \sum_i \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \uparrow \\ i \end{array} \qquad \begin{array}{c} \text{grey circle} \end{array} := \sum_i \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \uparrow \\ i \end{array}$$

Представляя адьюнкты этих отображений с помощью вертикального отражения (как обычно)



мы можем записать часть XOR вентиля CNOT в виде серого кружочка с точностью до числа.

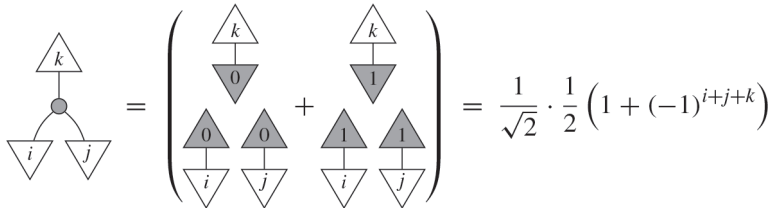
Предложение 5.88.



Доказательство. Докажем это, вычислив элементы матрицы в Z-базисе. Подставляя в правую часть

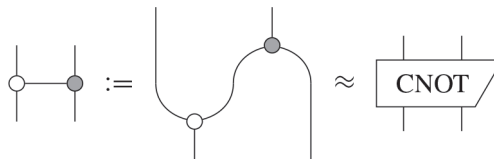


получаем:

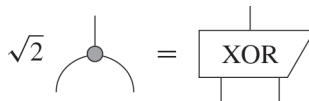


Это выражение равно $1/\sqrt{2}$, если $i + j + k$ четно, и 0 в противном случае. Но $i + j + k$ четно тогда и только тогда, когда $i \oplus j = k$. Если не обращать внимания на множитель $1/\sqrt{2}$, то получается как раз матрица XOR.

Поэтому положим



Если не игнорировать числа, то имеем



и, следовательно,

$$\sqrt{2} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \begin{array}{|c|} \hline \text{CNOT} \\ \hline \end{array}$$

Пример 5.89. Поскольку X -базис зависит от вычитания, он не имеет смысла в теории **отношений** (см. замечание 5.27). Но так как процесс COPY в X -базисе – то же самое, что XOR, он остается в силе и для **отношений**. Таким образом, присутствует «тьень» этого базиса и, главное, его взаимодействие с Z -базисом.

Упражнение 5.90. Докажите, что вентиль CNOT подчиняется таким правилам:



В главе 9 мы увидим, что это не просто случайные диаграммные равенства, а выражение фундаментальной концепции *дополнительности* в квантовой теории.

Мы можем также определить унитарное линейное отображение, которое переводит X -базис в Z -базис, воспользовавшись рецептом, приведенным в следствии 5.39.

Определение 5.91. *Отображением Адамара* называется

$$\begin{array}{|c|} \hline H \\ \hline \end{array} := \sum_i \begin{array}{c} \triangle \\ i \\ \triangle \\ i \end{array}$$

Мы не рисуем отображение Адамара асимметрично, как большинство блоков, по следующей причине.

Предложение 5.92. Линейное отображение Адамара H является самосопряженным и самоадьюнктным, а следовательно, самотранспонированным:

$$\begin{array}{|c|} \hline H \\ \hline \end{array} = \begin{array}{|c|} \hline H \\ \hline \end{array} = \begin{array}{|c|} \hline H \\ \hline \end{array}$$

Доказательство. Убедиться в том, что H самоадьюнктное и самосопряженное, можно, выразив X -базис через Z -базис:

$$\begin{array}{|c|} \hline H \\ \hline \end{array} = \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} - \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \right). \quad (5.49)$$

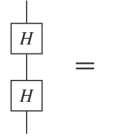
Из (5.49) видно, что матрица H в Z -базисе имеет вид:

$$\begin{array}{|c|} \hline H \\ \hline \end{array} \leftrightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Упражнение 5.93. Как выглядит матрица H в X -базисе?

Поскольку адьюнкт унитарного отображения является обратным к нему, имеет также место

Следствие 5.94. Линейное отображение Адамара обратнo самому себе:



Замечание 5.95. Как и для вентиля CNOT, мы впоследствии введем альтернативную нотацию для вентиля NOT, а именно:



Кружочек закрашен серым, потому что, как и XOR, этот вентиль естественно выражается в X -базисе, как будет объяснено позже. Итак, перечислим все операции, встретившиеся в этом разделе:



С отображениями копирования мы снова столкнемся в разделе 8.2.2, когда будем выражать *классические данные* в терминах диаграмм. Декорации типа π в вентиле NOT будут объяснены в разделе 9.1, а взаимодействие двух цветов – в разделе 9.2. Все эти кусочки в совокупности будут играть важную роль в мощнейшем диаграммном языке, который называется *ZX-исчислением* и описан в разделе 9.4.

5.3.6. Базис Белла и отображения Белла

Теперь мы опишем базис в $\mathbb{C}^2 \otimes \mathbb{C}^2$, который является не просто произведением двух базисов в \mathbb{C}^2 . Легко показать, что следующие четыре состояния

$$\left\{ \begin{array}{l} B_0 := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} \right) \\ B_1 := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} \right) \\ B_2 := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} - \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} \right) \\ B_3 := \frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} - \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} \right) \end{array} \right\} \quad (5.50)$$

образуют ортонормированное множество, т. е.

$$\begin{aligned}
 \begin{array}{c} \triangle \\ B_0 \\ \triangle \\ B_0 \end{array} &= \frac{1}{2} \left(\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \right) \\
 &= \frac{1}{2} (1 + 0 + 0 + 1) = 1
 \end{aligned}$$

$$\begin{aligned}
 \begin{array}{c} \triangle \\ B_1 \\ \triangle \\ B_0 \end{array} &= \frac{1}{2} \left(\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} + \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \right) \\
 &= \frac{1}{2} (0 + 0 + 0 + 0) = 0
 \end{aligned}$$

$$\begin{aligned}
 \begin{array}{c} \triangle \\ B_2 \\ \triangle \\ B_0 \end{array} &= \frac{1}{2} \left(\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} - \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} + \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} - \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \right) \\
 &= \frac{1}{2} (1 - 0 + 0 - 1) = 0
 \end{aligned}$$

и т. д. Таким образом, B_i образуют ортонормированное множество размера $\dim(\mathbb{C}^2 \otimes \mathbb{C}^2) = 4$, и, значит, в силу следствия 5.80 они образуют ОНБ. Действительно, мы можем выразить каждый элемент базиса произведения для $\mathbb{C}^2 \otimes \mathbb{C}^2$ через состояния (5.50):

$$\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} \triangle \\ B_0 \\ \triangle \\ B_0 \end{array} + \begin{array}{c} \triangle \\ B_2 \\ \triangle \\ B_0 \end{array} \right)$$

$$\begin{array}{c} \triangle \\ 0 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} \triangle \\ B_1 \\ \triangle \\ B_0 \end{array} + \begin{array}{c} \triangle \\ B_3 \\ \triangle \\ B_0 \end{array} \right)$$

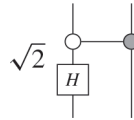
$$\begin{array}{c} \triangle \\ 1 \\ \triangle \\ 0 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} \triangle \\ B_1 \\ \triangle \\ B_0 \end{array} - \begin{array}{c} \triangle \\ B_3 \\ \triangle \\ B_0 \end{array} \right)$$

$$\begin{array}{c} \triangle \\ 1 \\ \triangle \\ 1 \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \\ 0 \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} \triangle \\ B_0 \\ \triangle \\ B_0 \end{array} - \begin{array}{c} \triangle \\ B_2 \\ \triangle \\ B_0 \end{array} \right)$$

Определение 5.96. ОНБ (5.50) называется *базисом Белла*.

Из предложения 5.38 мы знаем, что унитарные процессы всегда переводят ОНБ в ОНБ. Поэтому убедиться, что состояния (5.50) образуют ОНБ, можно и по-другому, показав, что они получаются применением некоторого унитарного процесса к другому ОНБ.

Упражнение 5.97. Покажите, что базис Белла получается применением следующего унитарного линейного отображения



к базису произведения

$$\left\{ \begin{array}{c} \downarrow \\ i \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ j \\ \uparrow \end{array} \right\}_{ij}$$

Иными словами, покажите, что состояния (5.50) можно выразить в виде:

$$\left\{ \begin{array}{c} \sqrt{2} \\ \begin{array}{c} \text{Circuit with } H \text{ gate and CNOT gate} \\ \downarrow \\ i \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ j \\ \uparrow \end{array} \end{array} \right\}_{ij}$$

и потому они образуют ОНБ.

Первое состояние Белла – это просто чашка, умноженная на $1/\sqrt{2}$, а остальные три – вариации, полученные обращением бита, или переменной знака. Отсюда легко видеть, что все состояния Белла неразделимы. Более того, они максимально неразделимы в смысле определения 4.80, и этот факт играет важнейшую роль в квантовой телепортации. Доказать максимальную неразделимость можно, следующим образом соотнеся специальные унитарные линейные отображения, называемые *отображениями Белла*, с состояниями Белла:

$$B_i = \text{Circuit with } B_i \text{ box and } \frac{1}{\sqrt{2}} \text{ label} \quad (5.51)$$

где

$$B_i := \sqrt{2} \text{ Circuit with } B_i \text{ box and curved line}$$

Упражнение 5.98. Покажите, что матричные формы отображений Белла имеют вид:

$$\begin{array}{l} B_0 := \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} + \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \\ B_1 := \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} + \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \\ B_2 := \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} - \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \\ B_3 := \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} - \begin{array}{c} \downarrow \\ 0 \\ \uparrow \end{array} \begin{array}{c} \downarrow \\ 1 \\ \uparrow \end{array} \end{array} \quad (5.52)$$

и, следовательно, им соответствуют матрицы

$$\begin{array}{cc}
 \begin{array}{c} | \\ \hline \text{B}_0 \\ \hline | \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{array}{c} | \\ \hline \text{B}_1 \\ \hline | \end{array} \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 \begin{array}{c} | \\ \hline \text{B}_2 \\ \hline | \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \begin{array}{c} | \\ \hline \text{B}_3 \\ \hline | \end{array} \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
 \end{array} \tag{5.53}$$

Также покажите, что эти линейные отображения унитарны.

Неудивительно, что матрицы, ассоциированные с отображениями Белла, называются *матрицами Белла*. Но в большинстве учебников вы встретите не матрицы Белла, а их близких родственников.

Замечание 5.99. Следующие матрицы называются *матрицами Паули*:

$$\begin{array}{cc}
 \sigma_0 = 1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \sigma_1 = \sigma_X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
 \sigma_2 = \sigma_Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \sigma_3 = \sigma_Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
 \end{array}$$

Они почти совпадают с матрицами Белла:

$$\sigma_0 = B_0, \quad \sigma_1 = B_1, \quad \sigma_3 = B_2;$$

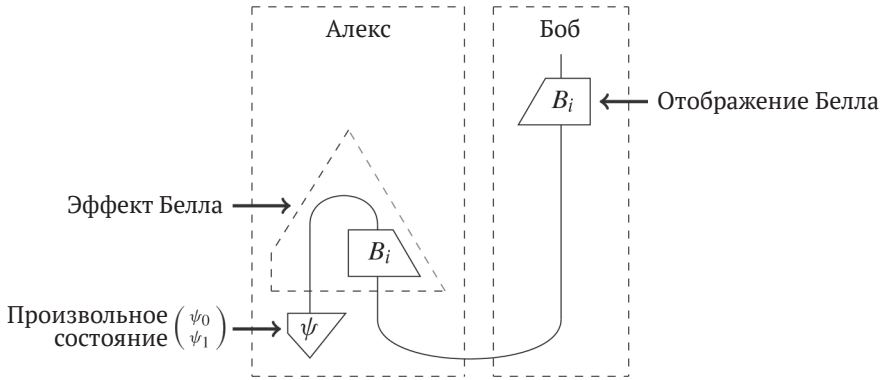
единственное отличие состоит в том, что

$$\sigma_2 = iB_3. \tag{5.54}$$

В следующей главе мы увидим, что умножение на i никак не влияет на физический смысл этого процесса. Так какое нам дело до матриц Паули? Нам – никакого! Но другим дело есть. Выражение (5.54) нужно для того, чтобы сделать все матрицы Паули самосопряженными. В обычном изложении квантовой теории самосопряженные матрицы используются для определения измерений (см. замечание 7.25). Но наше определение измерений не зависит от самосопряженных линейных отображений, поэтому мы сохраним верность отображениям Белла.

Заметим, что с помощью равенства (5.51) все состояния Белла получаются путем применения некоторых процессов к одному фиксированному состоянию. Этот факт напрямую связан с той ролью, которую состояния и отображения Белла играют в квантовой телепортации. Детали мы объясним в следующей главе, а пока – небольшой анонс.

Упражнение 5.100. Вычислите состояние



воспользовавшись матричными представлениями его составных частей, и убедитесь, что с точностью до числа мы действительно получаем ψ для любого i .

Эта связь между базисом Белла и отображениями Белла является частным случаем общей связи между ОНБ и некоторыми семействами линейных отображений, индуцированной двойственностью процессов и состояний.

Определение 5.101. Множество линейных отображений

$$\left\{ \begin{array}{c} B \\ \diagdown \\ i \\ \diagup \\ A \end{array} \right\}_i \tag{5.55}$$

называется ОНБ *Гильберта–Шмидта*, если ассоциированные двухкомпонентные состояния

$$\begin{array}{c} \diagdown \\ i \\ \diagup \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} | \\ \diagdown \\ i \\ \diagup \\ | \end{array} \tag{5.56}$$

образуют ОНБ для $D = \dim(A)$.

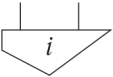
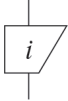
Вычисление внутреннего произведения состояний (5.56) дает

$$\begin{array}{c} \diagdown \\ j \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} = \frac{1}{D} \begin{array}{c} \diagdown \\ j \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} = \frac{1}{D} \text{tr} \left(\begin{array}{c} \diagdown \\ j \\ \diagup \\ \diagdown \\ i \\ \diagup \end{array} \right)$$

Самое правое выражение (без множителя $1/D$) иногда называют *внутренним произведением Гильберта–Шмидта* линейных отображений. Очевидно, что имеется альтернативное выражение ортонормированности (5.55) в терминах этого внутреннего произведения:

$$\text{tr} \left(\begin{array}{c} \boxed{j} \\ \boxed{i} \end{array} \right) = D \delta_i^j$$

Вспомнив определение 4.80 максимально неразделимых состояний, приходим к выводу, что следующие утверждения эквивалентны:

- базисные состояния  максимально неразделимы и
- соответствующие базисные отображения  унитарны.

5.4. ГИЛЬБЕРТОВЫ ПРОСТРАНСТВА И ДИАГРАММЫ

Так какое же отношение струнные диаграммы в действительности имеют к гильбертовым пространствам и линейным отображениям? Мы определили гильбертовы пространства и линейные отображения как специальный вид струнных диаграмм. Но чтобы сделать это, нам пришлось допустить существование базисов, сумм и того факта, что числами теории являются комплексные числа. Как-то все это выглядит притянутым за уши. К тому же многие другие вещи тоже описываются струнными диаграммами, например множества и отношения, так что, возможно, связь между гильбертовыми пространствами и линейными отображениями не такая уж специальная.

Однако мы представим поразительный результат, который тесно связывает диаграммные рассуждения с гильбертовыми пространствами и линейными отображениями. Учитывая, что дополнительная структура гильбертовых пространств позволяет доказывать многочисленные утверждения о процессах, возникает соблазнительная мысль о том, что мы сможем доказать больше соотношений между диаграммами линейных отображений, чем для обычных диаграмм, для которых не определены базисы, суммы и т. д. Оказывается, что это не так. Равенства, справедливые для диаграмм линейных отображений, – это в точности те равенства, которые можно доказать простой деформацией диаграмм. И в этом разделе мы, во-первых, дадим точную формулировку этого утверждения.

Во-вторых, мы выведем обычное теоретико-множественное определение гильбертова пространства из определения, основанного на диаграммах. В разделе 5.4.2 мы увидим, что это определение наряду с линейными отображениями и тензорным произведением получается автоматически, если рассматривать системные типы для **линейных отображений** не просто как метки, а как множества всех их состояний.

Отметим, что материал следующих двух разделов факультативный, далее в этой книге он не будет явно использоваться. Но многим читателям они могут показаться полезными, поскольку раскрывают мощь диаграммных доказательств и связь нашего понятия гильбертова пространства с обычным определением, встречающимся в литературе.

5.4.1. Струнные диаграммы полны относительно линейных отображений

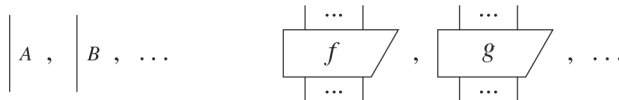
Цель этого раздела – охарактеризовать те новые равенства между диаграммами, которые появляются, если предположить, что диаграммы в действительности представляют линейные отображения и наделены дополнительной структурой в виде сумм, базисов и комплексных чисел. И, как уже отмечалось выше, ответ оказывается удивительным: новых равенств нет! То есть язык струнных диаграмм уже достаточно мощный для выражения всех равенств, справедливых для диаграмм линейных отображений общего вида. Или, пользуясь терминологией математической логики:

Струнные диаграммы *полны* относительно **линейных отображений**.

Для выражения этого факта есть еще один технический термин, который подчеркивает тот факт, что добавление ОНБ, сумм и комплексных чисел «ничего не дает»:

линейные отображения – консервативное расширение струнных диаграмм.

Напомним (см. раздел 3.1.2), что данные, составляющие струнную диаграмму, – это ее блоки, включающие спецификацию входных и выходных проводов, и соединения блоков между собой. Иначе говоря, под «струнной диаграммой» мы понимаем «рисование» блоков и проводов без какой-либо интерпретации в контексте процессной теории. Следуя этой логике, струнные диаграммы считаются равными, если одну можно деформировать в другую. Для различения проводов и блоков мы используем метки:

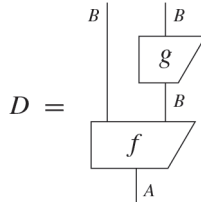


С диаграммами связано также понятие вертикального отражения, весьма важное для результата о полноте, который мы вскоре представим. Этот результат касается сравнения таких «свободных», или «неинтерпретируемых», диаграмм с диаграммами, интерпретируемыми в процессной теории **линейных отображений**. Давайте теперь формализуем идею интерпретации.

Определение 5.102. *Интерпретация в теории линейных отображений* $\llbracket \cdot \rrbracket$ струнной диаграммы D состоит из двух частей: выбора гильбертова пространства $\llbracket A \rrbracket$ для каждого типа A , встречающегося в D , и выбора линейного отображения $\llbracket f \rrbracket$ (принимающего во внимание входные и выходные типы) для каждого блока f , встречающегося в D .

В частности, интерпретация определяет линейное отображение $\llbracket D \rrbracket$, полученное путем подстановки всех линейных отображений $\llbracket f \rrbracket$, $\llbracket g \rrbracket$, ... в диаграмму D и их вычисления как линейных отображений (с применением, например, теоремы 5.61).

Пример 5.103. Рассмотрим диаграмму



У диаграммы D два типа и два блока, и ниже показана ее интерпретация:

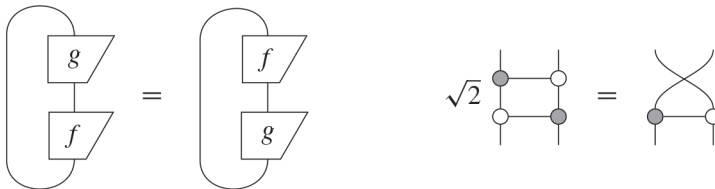
$$\left\{ [A] := \mathbb{C}^3, [B] := \mathbb{C}^2, [f] := \begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 4 \\ 5 & 5 & 5 \\ 0 & 1 & 0 \end{pmatrix}, [g] := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

При такой интерпретации

$$[[D]] = \begin{pmatrix} 1 & 2 & 0 \\ 4 & 3 & 4 \\ 5 & 5 & 5 \\ 5 & 6 & 5 \end{pmatrix}$$

Аналогично можно дать интерпретацию набору диаграмм D, E, F, \dots , интерпретировав все блоки и провода, встречающиеся во всех диаграммах, что, в свою очередь, дает линейные отображения $[[D]], [[E]], [[F]], \dots$

Теперь рассмотрим два равенства, с которыми мы уже встречались:



Оба равенства допустимы в процессной теории линейных отображений, но в первом f и g могут быть произвольными линейными отображениями (с соответствующими друг другу типами), а второе имеет место только в частном случае вентиля CNOT. Иными словами, второе равенство подразумевает лишь одну интерпретацию диаграмм в теории **линейных отображений**, а первое распространяется на все возможные интерпретации. Здесь нас будут интересовать только равенства первого вида, допускающие все возможные интерпретации в теории **линейных отображений**.

Теперь мы готовы сформулировать теорему о полноте.

Теорема 5.104. Струнные диаграммы полны относительно **линейных отображений**. Это означает, что для любых двух струнных диаграмм D, E следующие утверждения эквивалентны:

- $D = E$;
- для любых интерпретаций D, E в теории **линейных отображений** $\llbracket D \rrbracket = \llbracket E \rrbracket$.

Доказательство (набросок). Доказательство этой теоремы выходит за рамки книги. Грубо говоря, нужно взять какую-то диаграмму D и определить интерпретацию, «характерную» для D . Такая интерпретация дает некоторое фиксированное линейное отображение L для D , и для любой другой диаграммы $D' \neq D$ можно показать, что $\llbracket D' \rrbracket$ не может быть равно L . □

В итоге приходим к следующему выводу:

равенство между струнными диаграммами имеет место для всех гильбертовых пространств и линейных отображений тогда и только тогда, когда эти диаграммы равны.

Это убедительное свидетельство в пользу того факта, что струнные диаграммы выражают композиционное содержание линейных отображений.

Условие $\llbracket D \rrbracket = \llbracket E \rrbracket$ для **всех** интерпретаций довольно сильное, поэтому интересно понять, справедлива ли теорема 5.104 для любой процессной теории, допускающей струнные диаграммы. Ответ отрицательный.

Теорема 5.105. Струнные диаграммы неполны относительно теории **отношений**. То есть существуют неравные струнные диаграммы $D \neq E$ такие, что для всех интерпретаций как **отношений** $\llbracket D \rrbracket = \llbracket E \rrbracket$.

Доказательство. Нам нужно только найти две различные струнные диаграммы, для которых все интерпретации в теории **отношений** были бы равны. Напомним, что в теории отношений только два числа: 0 и 1. В обоих случаях $\lambda^2 = \lambda$, поэтому следующие две диаграммы:

$$\begin{array}{c} \diamond \lambda \\ \diamond \lambda \end{array} \quad \text{и} \quad \begin{array}{c} \diamond \lambda \end{array}$$

равны для всех интерпретаций как **отношений**. Однако они, очевидно, не равны как струнные диаграммы. □

Иными словами, существуют такие равенства между струнными диаграммами, которые справедливы для (всех) множеств и отношений, но сами струнные диаграммы при этом не равны. Поскольку единственное реальное различие между **линейными отображениями** и **отношениями** – выбор чисел, то может показаться удивительным, что такая простая вещь, как булевы величины, нарушает полноту, тогда как для множества комплексных чисел \mathbb{C} со всей его дополнительной структурой ничего подобного не происходит.

5.4.2. Теоретико-множественное определение гильбертовых пространств

Читатели, довольные нашим определением процессной теории **линейных отображений** (и, следовательно, гильбертовых пространств), могут спокойно пропустить этот раздел. Здесь мы ставим себе целью связать наше определение с традиционным. Иными словами, мы определим гильбертово пространство H

как множество, наделенное дополнительными операциями (сложением, умножением на скаляр, внутренним произведением), и линейные отображения как функции, сохраняющие эти операции (отчасти). Составные системы образуются путем конструирования *тензорного произведения* гильбертовых пространств, которое мы также определим. Это альтернативное определение приводится по двум причинам:

- для полноты, чтобы читатель имел представление о том, как выглядит традиционное определение гильбертова пространства;
- для контраста, чтобы подчеркнуть различие обоих определений по духу.

Напомним (см. раздел 3.4.1), что в теории **функций** состояния типа A находятся во взаимно однозначном соответствии с элементами множества A . Мы определим теоретико-множественный аналог \tilde{H} «наших гильбертовых пространств» H (т. е. системных типов в теории **линейных отображений**), имитировав это взаимно однозначное соответствие:

$$\tilde{H} := \left\{ \left\langle \begin{array}{c} H \\ \psi \end{array} \right\rangle \mid \psi \text{ является состоянием типа } H \right\}.$$

То есть для заданного типа H в теории **линейных отображений** мы определяем *гильбертово пространство* \tilde{H} как его множество состояний. Элементы \tilde{H} мы называем не состояниями, а *векторами*. Ниже будет показано, что заодно мы получаем все теоретико-множественные операции гильбертова пространства (включая и тензорное произведение!) «бесплатно» – выразив их в терминах состояний. Начнем со сложения и умножения на скаляр. Поскольку в теории **линейных отображений** определено понятие суммы, имеем:

- $\left\langle \begin{array}{c} 0 \\ \psi \end{array} \right\rangle$;
- если $\left\langle \begin{array}{c} \psi \\ \psi \end{array} \right\rangle \in \tilde{H}$, $\left\langle \begin{array}{c} \phi \\ \phi \end{array} \right\rangle \in \tilde{H}$, то $\left\langle \begin{array}{c} \psi + \phi \\ \psi + \phi \end{array} \right\rangle \in \tilde{H}$;
- если $\left\langle \begin{array}{c} \lambda \\ \lambda \end{array} \right\rangle \in \mathbb{C}$, $\left\langle \begin{array}{c} \psi \\ \psi \end{array} \right\rangle \in \tilde{H}$, то $\left\langle \begin{array}{c} \lambda \psi \\ \lambda \psi \end{array} \right\rangle \in \tilde{H}$.

Иначе говоря, множество состояний H образует *комплексное векторное пространство*.

Определение 5.106. *Комплексным векторным пространством* называется множество \tilde{V} с выделенным элементом $0 \in \tilde{V}$ и двумя операциями:

- $\psi + \phi$ для всех $\psi, \phi \in \tilde{V}$;
- $\lambda \cdot \psi$ для всех $\lambda \in \mathbb{C}$ и $\psi \in \tilde{V}$,

которые называются соответственно *суммой* и *умножением на скаляр* и удовлетворяют условиям:

- 1) $0 + \psi = \psi$;
- 2) $(\psi + \phi) + \xi = \psi + (\phi + \xi)$;
- 3) $\psi + \phi = \phi + \psi$;
- 4) $0 \cdot \psi = 0$;
- 5) $\lambda \cdot (\lambda' \cdot \psi) = (\lambda\lambda') \cdot \psi$;

6) $\lambda \cdot (\psi + \phi) = \lambda \cdot \psi + \lambda \cdot \phi;$

7) $(\lambda + \lambda') \cdot \psi = \lambda \cdot \psi + \lambda' \cdot \psi.$

Для всех $\psi, \phi, \xi \in \tilde{V}$ и $\lambda, \lambda' \in \mathbb{C}.$

Обычно произведение на скаляр $\lambda \cdot \psi$ записывается просто в виде $\lambda\psi$. Как и в разделе 5.1.3, если установлено, что операция $(- + -)$ ассоциативна и коммутативна, то удобнее использовать нотацию суммирования и заменить равенства 6 и 7 их эквивалентами, содержащими символ суммы:

6') $\lambda(\sum_i \psi_i) = \sum_i (\lambda\psi_i);$

7') $(\sum_i \lambda_i)\psi = \sum_i (\lambda_i\psi).$

Упражнение 5.107. Пользуясь условиями 1–3 в определении 5.21, покажите, что \tilde{H} удовлетворяет всем семи аксиомам комплексного векторного пространства.

В теории **линейных отображений** у каждого системного типа имеется конечный базис:

$$\mathcal{B} = \left\{ \begin{array}{c} \downarrow \\ i \\ \triangle \end{array} \right\}_i.$$

По теореме 5.30 любое состояние $\psi \in \tilde{H}$ можно записать в этом базисе:

$$\begin{array}{c} \downarrow \\ \psi \\ \triangle \end{array} = \sum_i \begin{array}{c} \diamond \\ \psi_i \\ \triangle \end{array} \begin{array}{c} \downarrow \\ i \\ \triangle \end{array}$$

Это означает, что наше комплексное векторное пространство *конечномерно*.

Определение 5.108. *Базисом* векторного пространства \tilde{V} называется минимальное множество векторов

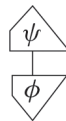
$$\{\phi_i\}_i \subseteq \tilde{V},$$

которое *стягивает* \tilde{V} , т. е. для любого $\psi \in \tilde{V}$ существуют такие $\{\lambda_i\}_i \subseteq \mathbb{C}$, что

$$\psi = \sum_i \lambda_i \phi_i. \tag{5.57}$$

Если множество $\{\phi_i\}_i$ конечно, то \tilde{V} называется *конечномерным*, а количество элементов в $\{\phi_i\}_i$ – размерностью \tilde{V} .

В теории **линейных отображений** есть адъюнкция, поэтому мы можем образовать диаграмму



для всех $\psi, \phi \in \tilde{H}$. Это дает нам всю необходимую структуру для следующего определения.

Определение 5.109. *Конечномерным гильбертовым пространством* называется конечномерное векторное пространство \tilde{H} с дополнительной операцией

$$\langle - | - \rangle : \tilde{H} \times \tilde{H} \mapsto \mathbb{C},$$

которая называется внутренним¹ произведением и обладает следующими свойствами:

- 1) $\langle \psi | \lambda \phi + \xi \rangle = \lambda \langle \psi | \phi \rangle + \langle \psi | \xi \rangle;$
- 2) $\langle \lambda \psi + \phi | \xi \rangle = \bar{\lambda} \langle \psi | \xi \rangle + \langle \phi | \xi \rangle;$
- 3) $\langle \psi | \phi \rangle = \overline{\langle \phi | \psi \rangle};$
- 4) $\langle \psi | \psi \rangle > 0$ для всех $\psi \neq 0,$

где символ $\overline{(-)}$ означает комплексное сопряжение.

Заметим, что 2 следует из 1 и 3. Большую часть этих свойств мы уже встречали в предложении 4.51. Исключение составляет сохранение суммы в условии 1, которое, как мы видели в разделе 5.1.3, сводится к

$$\sum_i \langle \lambda_i | \psi_i \rangle = \sum_i \langle \lambda_i | \psi_i \rangle$$

и точно так же для условия 2.

Замечание* 5.110. Мы определяем только конечномерные гильбертовы пространства, поскольку ничего другого нам в этой книге не нужно. Определение произвольного гильбертова пространства сложнее, поскольку требуется, чтобы множество векторов было топологически замкнуто относительно взятия предела некоторой последовательности векторов. Для конечного числа измерений это условие удовлетворяется автоматически.

Обычное понятие ОНБ в гильбертовом пространстве совпадает с нашим.

Определение 5.111. Базис $\{\phi_i\}_i$ конечномерного гильбертова пространства \tilde{H} называется *ортонормированным*, если

$$\langle \phi_i | \phi_j \rangle = \delta^i_j.$$

Далее нам предстоит ввести линейные отображения как функции из множества в множество. При таком определении гильбертова пространства, для того чтобы определить общее *мультилинейное* отображение (т. е. отображение, имеющее несколько входов и выходов), придется потрудиться. Но отображения, имеющие ровно по одному входу и выводу, не представляют сложностей. Если даны гильбертовы пространства \tilde{H} и \tilde{K} , то, рассмотрев функции вида

$$\tilde{f} : \tilde{H} \rightarrow \tilde{K} :: \psi \mapsto f(\psi)$$

мы действительно получим все обычные свойства линейных отображений.

¹ В русскоязычной литературе больше распространено название «скалярное произведение». – Прим. перев.

Определение 5.112. Для векторных (или гильбертовых) пространств \tilde{H} и \tilde{K} линейным отображением $f: \tilde{H} \rightarrow \tilde{K}$ называется функция из множества \tilde{H} в множество \tilde{K} , удовлетворяющая условиям:

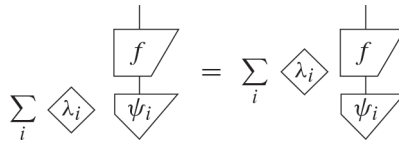
$$(\lambda\psi) = \lambda f(\psi) \quad \text{и} \quad f(\psi + \phi) = f(\psi) + f(\phi).$$

Эти два условия называются *линейностью*.

Оба условия можно выразить компактнее, воспользовавшись суммированием:

$$f\left(\sum_i \lambda_i \psi_i\right) = \sum_i \lambda_i f(\psi_i). \tag{5.58}$$

Как мы видели в разделе 5.1.3, эта формула сводится к



Замечание 5.113. Первоначально мы определили теоретико-множественный аналог гильбертовых пространств, имитировав взаимно однозначное соответствие между множествами A и функциями из множества, представляющего тип «отсутствие провода», в множество A . В случае гильбертовых пространств именно благодаря линейности такое взаимно однозначное соответствие работает. Прежде всего отметим, что \mathbb{C} – особенно простое векторное пространство, в котором число 1 само по себе образует одноэлементный ОНБ, поскольку все остальные числа $\lambda \in \mathbb{C}$ можно представить в виде (см. (5.57)):

$$\lambda = \lambda \cdot 1,$$

и условие ортонормированности тривиально удовлетворяется. Сложение «векторов» в \mathbb{C} – это просто сложение комплексных чисел, согласно правилу 7 из определения 5.106:

$$\lambda + \lambda' = \lambda \cdot 1 + \lambda' \cdot 1 = (\lambda + \lambda') \cdot 1 = \lambda + \lambda'.$$

Далее, вектор $\psi \in \tilde{H}$ однозначно определяет линейное отображение:

$$\tilde{\psi} : \mathbb{C} \rightarrow \tilde{H} :: 1 \mapsto \psi,$$

поскольку, в силу линейности, для любого $\lambda \in \mathbb{C}$ имеет место равенство

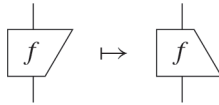
$$\tilde{\psi} :: \lambda = \lambda \cdot 1 \mapsto \lambda \cdot \psi.$$

Если взять в качестве \tilde{H} само \mathbb{C} , то каждое $\lambda \in \mathbb{C}$ однозначно определяет линейное отображение:

$$\tilde{\lambda} : \mathbb{C} \rightarrow \mathbb{C} :: 1 \mapsto \lambda.$$

Следовательно, существует также взаимно однозначное соответствие между элементами \mathbb{C} и линейными отображениями \mathbb{C} в себя. Таким образом, линейные отображения, векторы и числа из \mathbb{C} – различные проявления одного и того же, и вы уже это знаете, поскольку все они – разновидности процессов.

Для струнных диаграмм, а следовательно, и для **линейных отображений** адьюнктом является

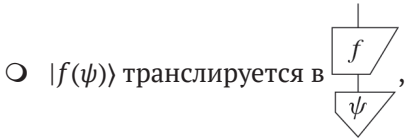


Для традиционных линейных отображений мы имеем следующий стандартный результат.

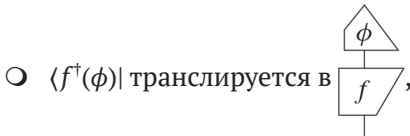
Предложение 5.114. Для гильбертовых пространств \tilde{H} и \tilde{K} и линейного отображения $f : \tilde{H} \rightarrow \tilde{K}$ существует единственное линейное отображение f^\dagger такое, что для всех $\psi \in \tilde{H}$, $\phi \in \tilde{K}$:

$$\langle \phi | f(\psi) \rangle = \langle f^\dagger(\phi) | \psi \rangle. \tag{5.59}$$

Однозначно определенное линейное отображение f^\dagger называют также *адьюнктом*. На струнных диаграммах равенство (5.59) является тавтологией. В самом деле, поскольку:



то



и, стало быть, левая часть $\langle \phi | f(\psi) \rangle$ и правая часть $\langle f^\dagger(\phi) | \psi \rangle$ равенства (5.59) равны



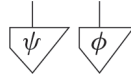
Понятия унитарного и положительного отображения одинаковы и в нашем, и в традиционном изложении гильбертовых пространств – см. определения 4.56 и 4.60 соответственно.

Последняя и самая тонкая часть теоретико-множественного аналога **линейных отображений** – определение параллельной композиции гильбертовых про-

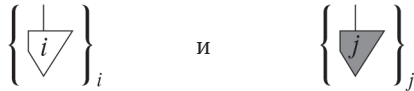
пространств. Мы должны определить операцию $\tilde{\otimes}$, которая на уровне гильбертовых пространств \tilde{H} и \tilde{K} имитирует результат параллельной композиции типов H и K , т. е.

$$\tilde{H} \tilde{\otimes} \tilde{K} \text{ должно совпадать с } \widetilde{H \otimes K}.$$

Пусть \tilde{H} и \tilde{K} – гильбертовы пространства, рассмотрим некоторые свойства $\widetilde{H \otimes K}$. Произвольные состояния $\psi \in \tilde{H}$ и $\phi \in \tilde{K}$ дают состояние



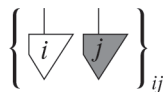
принадлежащее $\widetilde{H \otimes K}$. Поначалу возникает искушение определить $\tilde{H} \tilde{\otimes} \tilde{K}$ как декартово произведение $H \times K$, как мы и поступали для **функций**. Однако быстро выясняется, что это неправильно, потому что $\widetilde{H \otimes K}$ содержит много неразделимых состояний. Напомним (см. раздел 5.2.2), что можно построить базис $H \otimes K$ из базисов H и K по отдельности. Точнее, если известны ОНБ



H и K соответственно, то все состояния $\Phi \in \widetilde{H \otimes K}$ можно записать в следующем виде:

$$\text{[Triangle with } \Phi \text{]} = \sum_i \text{[Diamond with } \Phi_{i,j} \text{]} \text{[Triangle with } i \text{]} \text{[Triangle with } j \text{]}$$

Поэтому для заданных гильбертовых пространств \tilde{H} и \tilde{K} мы хотим построить такое гильбертово пространство, для которого



играет роль ОНБ. Сначала нужно сформировать множество векторов, и сделать это можно, например, рассмотрев множество «формальных сумм»:

$$\tilde{H} \tilde{\otimes} \tilde{K} := \left\{ \sum_{ij} \lambda_{ij} \phi_i \tilde{\otimes} \phi'_j \mid \lambda_{ij} \in \mathbb{C} \right\},$$

где $\{\phi_i\}$ и $\{\phi'_j\}$ – ОНБ \tilde{H} и \tilde{K} соответственно. Мы говорим «формальные суммы», потому что в данный момент символ суммы еще не имеет никакой семантики. Как и символ $\tilde{\otimes}$ между ϕ_i и ϕ'_j . Мы могли с тем же успехом представить эти элементы в виде списков чисел, индексированных парами (i, j) , т. е. матрицами, составленными из коэффициентов λ_{ij} . Далее нам предстоит превратить это множество в векторное пространство, чтобы «формальные суммы» вели себя как «настоящие» при нашем определении сложения векторов и умножения вектора на скаляр:

$$\left(\sum_{ij} \lambda_{ij} \phi_i \tilde{\otimes} \phi'_j \right) + \left(\sum_{ij} \lambda'_{ij} \phi_i \tilde{\otimes} \phi'_j \right) := \sum_{ij} (\lambda_{ij} + \lambda'_{ij}) \phi_i \tilde{\otimes} \phi'_j;$$

$$\lambda \cdot \left(\sum_{ij} \lambda_{ij} \phi_i \tilde{\otimes} \phi'_j \right) := \sum_{ij} \lambda \lambda_{ij} \phi_i \tilde{\otimes} \phi'_j.$$

При этом мы, очевидно, сможем сопоставить элементам \tilde{H} и \tilde{K} соответственные элементы $\tilde{H} \tilde{\otimes} \tilde{K}$. Точнее, элементам

$$\sum_i \lambda_i \phi_i \in \tilde{H} \quad \text{и} \quad \sum_i \lambda'_i \phi'_i \in \tilde{K}$$

сопоставляется элемент

$$\sum_{ij} \lambda_i \lambda'_j \phi_i \tilde{\otimes} \phi'_j \in \tilde{H} \tilde{\otimes} \tilde{K}.$$

Обозначив это отображение символом $\tilde{\otimes}$, получим:

$$\left(\sum_i \lambda_i \phi_i \right) \tilde{\otimes} \left(\sum_j \lambda'_j \phi'_j \right) = \sum_{ij} \lambda_i \lambda'_j \phi_i \tilde{\otimes} \phi'_j.$$

Это равенство называется $\tilde{\otimes}$ -*билинейностью*. Как и в случае линейности, на диаграммах ему соответствует просто перестановка чисел и знаков суммы:

$$\sum_i \diamond \lambda_i \downarrow \phi_i \quad \sum_j \diamond \lambda'_j \downarrow \phi'_j = \sum_{ij} \diamond \lambda_i \diamond \lambda'_j \downarrow \phi_i \downarrow \phi'_j$$

Горизонтальная композиция линейных отображений на разделимых векторах определяется следующим образом:

$$(f \tilde{\otimes} g)(\psi \tilde{\otimes} \phi) := f(\psi) \tilde{\otimes} g(\phi).$$

Тогда определение для неразделимых векторов вытекает из линейности:

$$(f \tilde{\otimes} g)(\Psi) = (f \tilde{\otimes} g) \left(\sum_i \psi_i \tilde{\otimes} \phi_i \right) = \sum_i f(\psi_i) \tilde{\otimes} g(\phi_i).$$

На диаграмме это не что иное, как:

$$\begin{array}{c} \begin{array}{|c|c|} \hline f & g \\ \hline \end{array} \\ \downarrow \\ \Psi \end{array} = \sum_i \begin{array}{|c|c|} \hline f & g \\ \hline \phi_i & \psi_i \\ \hline \end{array} = \sum_i \begin{array}{|c|c|} \hline f & g \\ \hline \phi_i & \psi_i \\ \hline \end{array}$$

Наконец, остается показать, что $\tilde{H} \tilde{\otimes} \tilde{K}$ – гильбертово пространство, т. е. обладает внутренним произведением. Для разделимых векторов в $\tilde{H} \tilde{\otimes} \tilde{K}$ мы можем определить его как

$$\langle \phi \tilde{\otimes} \phi' | \psi \tilde{\otimes} \psi' \rangle_{\tilde{H} \tilde{\otimes} \tilde{K}} := \langle \phi | \psi \rangle_{\tilde{H}} \langle \phi' | \psi' \rangle_{\tilde{K}}.$$

А определение для неразделимых векторов снова вытекает из линейности:

$$\langle \Phi | \Psi \rangle_{\tilde{H} \tilde{\otimes} \tilde{K}} = \left\langle \sum_i \phi_i \tilde{\otimes} \phi'_i \mid \sum_j \psi_j \tilde{\otimes} \psi'_j \right\rangle_{\tilde{H} \tilde{\otimes} \tilde{K}} = \sum_{ij} \langle \phi_i | \psi_j \rangle_{\tilde{H}} \langle \phi'_i | \psi'_j \rangle_{\tilde{K}}.$$

Как и все остальное, это равенство совершенно очевидно из картинки:

Определение 5.115. Построенная выше операция $\tilde{\otimes}$ над гильбертовыми пространствами и линейными отображениями называется *тензорным произведением*.

Замечание 5.116. Выше для построения тензорного произведения гильбертовых пространств мы опирались на их ОНБ. Этого можно избежать и тем самым показать, что результирующий тензор не зависит от выбора ОНБ. Однако такое не зависящее от ОНБ построение сложнее.

Теперь у нас есть все ингредиенты для определения новой процессной теории:

- системными типами являются теоретико-множественные гильбертовы пространства \tilde{H} ;
- процессами являются теоретико-множественные линейные отображения \tilde{f} ;
- горизонтальной композицией является теоретико-множественная композиция;
- вертикальной композицией является тензорное произведение $\tilde{\otimes}$;
- типом «без проводов» является одномерное гильбертово пространство \mathbb{C} .

Назовем ее теорией линейных отображений.

Теорема 5.117. Теории линейных отображений и линейных отображений эквивалентны в смысле, описанном в разделе 5.2.5.

5.5. Итоги: что следует запомнить

1. **Линейные отображения** – это процессная теория, допускающая струнные диаграммы такие, что:
 - 1) для каждого типа имеется *ортонормированный базис* (ОНБ);
 - 2) для каждой размерности $D \in \mathbb{N}$ существует, по меньшей мере, один системный тип;
 - 3) процессы одного типа допускают сумму;
 - 4) числами являются комплексные числа \mathbb{C} .

В этом случае ОНБ – это множество состояний, удовлетворяющих условиям:

$$\begin{array}{c} \triangleleft j \\ \downarrow \\ \triangleleft i \end{array} = \delta_i^j$$

и

$$\left(\text{для всех } \triangleleft i : \begin{array}{c} \triangleleft f \\ \downarrow \\ \triangleleft i \end{array} = \begin{array}{c} \triangleleft g \\ \downarrow \\ \triangleleft i \end{array} \right) \Rightarrow \begin{array}{c} \triangleleft f \\ \downarrow \\ \triangleleft \end{array} = \begin{array}{c} \triangleleft g \\ \downarrow \\ \triangleleft \end{array}$$

Фраза «допускают сумму» означает, что для любого множества $\{f_i\}$ процессов одного типа существует процесс того же типа

$$\sum_i \begin{array}{c} \triangleleft f_i \\ \downarrow \\ \triangleleft \end{array}$$

удовлетворяющий диаграммному равенству

$$\left(\sum_i \begin{array}{c} \triangleleft h_i \\ \downarrow \\ \triangleleft g \end{array} \right) \begin{array}{c} \triangleleft g \\ \downarrow \\ \triangleleft f \end{array} = \sum_i \left(\begin{array}{c} \triangleleft g \\ \downarrow \\ \triangleleft h_i \end{array} \begin{array}{c} \triangleleft f \\ \downarrow \\ \triangleleft g \end{array} \right)$$

и сохраняющий адъюнкты

$$\left(\sum_i \begin{array}{c} \triangleleft f_i \\ \downarrow \\ \triangleleft \end{array} \right)^\dagger = \sum_i \begin{array}{c} \triangleleft \end{array} \begin{array}{c} \triangleleft f_i \\ \downarrow \\ \triangleleft \end{array}$$

Гильбертово пространство – это тип в теории **линейных отображений**, а традиционное понятие гильбертова пространства возникает как множество всех состояний для фиксированного типа:

$$\tilde{H} := \left\{ \begin{array}{c} \triangleleft H \\ \downarrow \\ \triangleleft \psi \end{array} \mid \psi \text{ является состоянием типа } H \right\}.$$

2. В теории **линейных отображений** каждый процесс допускает *матрицу*

$$\begin{array}{c} \diagup \\ f \\ \diagdown \end{array} \leftrightarrow \begin{pmatrix} f_1^1 & f_2^1 & \cdots & f_m^1 \\ f_1^2 & f_2^2 & \cdots & f_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ f_1^n & f_2^n & \cdots & f_m^n \end{pmatrix}, \quad \text{где} \quad \begin{array}{c} \diamond \\ f_i^j \\ \diamond \end{array} := \begin{array}{c} \triangle \\ j \\ \square \\ f \\ \triangle \\ i \end{array}$$

которая позволяет записать его в *матричной форме*:

$$\begin{array}{c} \diagup \\ f \\ \diagdown \end{array} = \sum_{ij} \begin{array}{c} \diamond \\ f_i^j \\ \diamond \end{array} \begin{array}{c} \triangle \\ j \\ \triangle \\ i \end{array}$$

Матричные аналоги суммы, последовательной и параллельной композиций, транспонирования и адьюнкции процессов – это обычные операции над матрицами, известные из линейной алгебры. Матрица **m** диаграммы

$$\begin{array}{c} A \\ | \\ \begin{array}{c} B \\ \diagup \\ g \\ \diagdown \\ C \end{array} \\ | \\ A \\ \begin{array}{c} \psi \\ \diagdown \\ \end{array} \\ | \\ A \\ \begin{array}{c} \diagup \\ h \\ \diagdown \\ A \end{array} \end{array} \leftrightarrow \psi^{A_1 A_2} g_{B_1 A_2}^{C_1} h_{A_3}^{C_1}$$

вычисляется по диаграммной формуле

$$m_{i_3}^{i_1} = \sum_{i_2 j_1 k_1} \psi^{i_1 i_2} g_{j_1 i_2}^{j_1 k_1} h_{i_3}^{k_1}$$

3. Процессная теория **линейных отображений** эквивалентна следующей теории **matrices**(\mathbb{C}):

- 1) системами являются натуральные числа \mathbb{N} ;
- 2) процессами с входным типом $m \in \mathbb{N}$ и выходным типом $n \in \mathbb{N}$ являются матрицы размера $n \times m$ с элементами из множества комплексных чисел \mathbb{C} ;
- 3) диаграммы вычисляются, как описано выше.

Более того, для любого множества чисел X , допускающего суммы, матричное исчисление **matrices**(X) является процессной теорией, допускающей струнные диаграммы. Аналогичное построение показывает, что процессная теория **отношений** (ограниченная конечными множествами) эквивалентна теории **matrices**(\mathbb{B}).

4. Мы ввели ряд полезных линейных отображений, которые пригодятся позже:

- *базис Белла*:

$$\begin{aligned}
 B_0 &:= \frac{1}{\sqrt{2}} \left(\begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \right) \\
 B_1 &:= \frac{1}{\sqrt{2}} \left(\begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \right) \\
 B_2 &:= \frac{1}{\sqrt{2}} \left(\begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} - \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \right) \\
 B_3 &:= \frac{1}{\sqrt{2}} \left(\begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} - \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \right)
 \end{aligned}$$

○ соответствующие отображения Белла:

$$\begin{array}{cc}
 \begin{array}{|c|} \hline \downarrow \\ \hline B_0 \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{array}{|c|} \hline \downarrow \\ \hline B_2 \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
 \begin{array}{|c|} \hline \downarrow \\ \hline B_1 \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{array}{|c|} \hline \downarrow \\ \hline B_3 \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
 \end{array}$$

○ отображения копирования для Z-базиса (белый) и X-базиса (серый):

$$\begin{array}{cc}
 \begin{array}{|c|} \hline \downarrow \\ \hline \text{CNOT} \\ \hline \end{array} := \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} & \begin{array}{|c|} \hline \downarrow \\ \hline \text{CNOT} \\ \hline \end{array} := \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array}
 \end{array}$$

○ отображения Адамара и CNOT:

$$\begin{array}{cc}
 \begin{array}{|c|} \hline \downarrow \\ \hline H \\ \hline \end{array} := \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} & \sqrt{2} \begin{array}{|c|} \hline \downarrow \\ \hline \text{CNOT} \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
 \end{array}$$

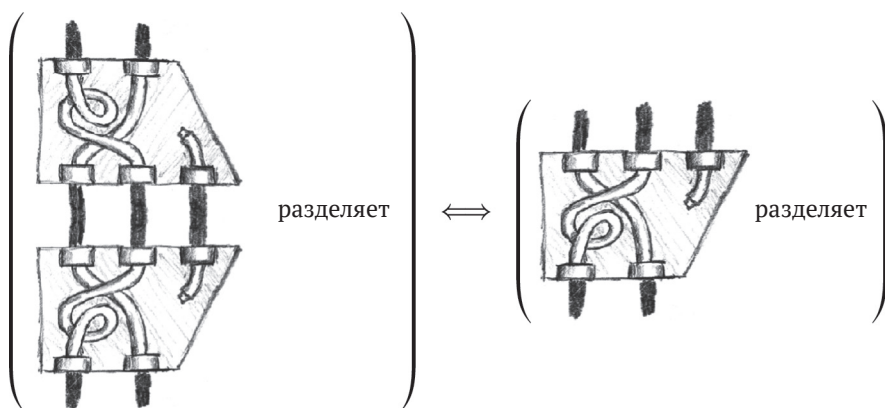
5. *Спектральная теорема* утверждает, что самоадьюнктные линейные отображения являются *диагонализуемыми*, т. е.

$$\begin{array}{|c|} \hline \downarrow \\ \hline f \\ \hline \end{array} = \sum_i r_i \begin{array}{|c|} \hline \downarrow \\ \hline i \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline i \\ \hline \end{array}$$

для некоторого ОНБ и вещественных чисел r_i . У этого факта много следствий, и одно из них заключается в том, что композиция $f^+ \circ f$ является критерием разделимости f :

$$\left(\exists \psi, \phi : \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ f \\ \diagup \quad \diagdown \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \phi \\ \diagup \quad \diagdown \\ \psi \\ \text{---} \end{array} \right) \iff \left(\exists \psi', \phi' : \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ f \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \phi' \\ \psi' \\ \text{---} \end{array} \right)$$

Этот факт допускает естественную интерпретацию, если всерьез относиться к идее о том, что адьюнкция в действительности является отражением:



▲ Формулировка спектральной теоремы с привлечением сумм временная. В главе 8 мы приведем пикторалистскую формулировку.

- 6. Струнные диаграммы *полны* относительно **линейных отображений**: множество равенств между диаграммами линейных отображений в точности совпадает с множеством всех равенств струнных диаграмм.
- 7. Для многих диаграммных концепций имеется соответствующее представление с использованием (самосопряженного) ОНБ. В таблице ниже приведена сводка.

| Концепция | Диаграмма | В терминах базиса |
|-----------|-----------|---|
| Процесс | | $\sum_{ij} \diamond f_i^j \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ j \\ \diagup \quad \diagdown \\ i \\ \text{---} \end{array}, \text{ где } \diamond f_i^j = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ j \\ \diagup \quad \diagdown \\ f \\ \diagup \quad \diagdown \\ i \\ \text{---} \end{array}$ |

| Концепция | Диаграмма | В терминах базиса |
|-----------------------|-----------|--|
| Состояние | | $\sum_i \diamond \psi^i \downarrow_i$, где $\diamond \psi^i = \begin{array}{c} \triangle i \\ \psi \\ \downarrow \end{array}$ |
| Тождественный процесс | | $\sum_i \begin{array}{c} \downarrow i \\ \triangle i \\ \uparrow \end{array}$ |
| Чашки | | $\sum_i \downarrow_i \downarrow_i$ |
| Крышки | | $\sum_i \triangle_i \triangle_i$ |
| Размерность | | $\sum_i \text{---} = \dim(H)$ |
| След | | $\sum_i \begin{array}{c} \triangle i \\ \text{---} \\ \triangle i \end{array}$ |
| Транспонирование | | $\sum_{ij} \diamond f_j^i \begin{array}{c} \downarrow j \\ \triangle i \end{array}$, где $\diamond f_i^j$, как и выше |
| Сопряжение | | $\sum_{ij} \diamond \overline{f_i^j} \begin{array}{c} \downarrow j \\ \triangle i \end{array}$, где $\diamond f_i^j$, как и выше |
| Адьюнкция | | $\sum_{ij} \diamond \overline{f_j^i} \begin{array}{c} \downarrow j \\ \triangle i \end{array}$, где $\diamond f_i^j$, как и выше |

5.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

В этом разделе мы рассмотрим определение бесконечномерного гильбертова пространства и приведем несколько интересных примеров, упомянув и о связанных с ними трудностях. Затем мы продолжим экскурс в теорию категорий и покажем, как в ней представляются суммы и ОНБ. Мы также объясним, почему в теории узлов используется аналогичная комбинация диаграммных рассуждений и сумм. И напоследок расскажем о том, как первопроходцы теории категорий формулировали, что означает эквивалентность двух процессных теорий.

5.6.1. За пределами конечного числа измерений*

Напомним, что внутреннее произведение определяет норму: $\|v\| := \sqrt{\langle v|v \rangle}$. В бесконечномерном случае ее роль неизмеримо важнее, поскольку она дает возможность говорить о сходимости последовательностей – той части определения гильбертова пространства, на которую можно не обращать внимания в конечномерном случае. Полное определение гильбертова пространства выглядит так.

Определение 5.118. *Гильбертово пространство* (возможно, бесконечномерное) – это комплексное векторное пространство, наделенное внутренним произведением и *полное в смысле Коши*. То есть для любой сходящейся (в смысле Коши) последовательности $(v_i)_i$ векторов H существует такой вектор $v \in H$, что $\|v_i - v\| \rightarrow 0$.

Это означает, что мы можем говорить о пределах последовательностей, поэтому к гильбертовым пространствам (а значит, и к квантовой механике) можно применить богатейший инструментарий *функционального анализа*. Всего лишь один пример: наличие пределов позволяет определить бесконечные суммы:

$$\sum_{i=0}^{\infty} \psi_i := \lim_{n \rightarrow \infty} \sum_{i=0}^n \psi_i.$$

Есть два примера гильбертовых пространств, которые исторически играли важную роль в квантовой механике как (эквивалентные) представления пространства квантово-механических состояний.

Пример 5.119. L^2 – множество всех функций $\psi : \mathbb{R}^n \mapsto \mathbb{C}$ с конечным интегралом

$$\int \overline{\psi(x)} \psi(x) dx < \infty.$$

Это множество становится гильбертовым пространством, если определить операции следующим образом:

$$(\lambda_1 \psi + \lambda_2 \phi)(x) := \lambda_1 \psi(x) + \lambda_2 \phi(x) \quad \text{и} \quad \langle \psi | \phi \rangle := \int \overline{\psi(x)} \phi(x) dx.$$

Пример 5.120. ℓ^2 – множество всех счетных последовательностей комплексных чисел с конечной «суммой квадратов»:

$$\sum_{i=0}^{\infty} \overline{a_i} a_i < \infty.$$

Оно образует гильбертово пространство, если определить такие операции:

$$\lambda_1 (a_i)_i + \lambda_2 (b_i)_i := (\lambda_1 a_i + \lambda_2 b_i)_i \quad \text{и} \quad \langle (a_i)_i | (b_i)_i \rangle := \sum_{i=0}^{\infty} \overline{a_i} b_i.$$

Как L^2 , так и ℓ^2 позволяют выразить состояние квантовой частицы и вычислить ее положение или импульс. Удивительно не то, что оба они являются математическими объектами одного вида (бесконечномерным гильбертовым пространством), а то, что эти пространства *изоморфны* (подробности см. в разделе 5.7).

И это вновь приводит нас к вопросу **В3** из раздела 2.3:

Почему бесконечномерные гильбертовы пространства не играют никакой роли в этой книге?

Или, если на то пошло, в квантовых вычислениях вообще? Краткий ответ – потому что многие вещи в них, похоже, не работают. Возьмем, к примеру, чашки и крышки, которые мы теперь знаем (и любим), и попробуем применить их в бесконечномерном пространстве. На первый, наивный взгляд, все вроде бы выглядит нормально:

$$\begin{array}{c} \text{U-образная диаграмма} \end{array} = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \begin{array}{c} \text{Диаграмма с чашкой } j \text{ и крышкой } i \end{array} = \sum_{i,j=0}^{\infty} \begin{array}{c} \text{Диаграмма с чашкой } j \text{ и крышкой } i \end{array} = \sum_{i=0}^{\infty} \begin{array}{c} \text{Диаграмма с крышкой } i \end{array} = \left| \right.$$

(предположим пока, что «бесконечные суммы» корректно определены). Но если ввести окружность, то ситуация оказывается печальной:

$$\begin{array}{c} \text{Окружность} \end{array} = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \begin{array}{c} \text{Диаграмма с чашкой } j \text{ и крышкой } i \end{array} = \sum_{i,j=0}^{\infty} \begin{array}{c} \text{Диаграмма с чашкой } j \text{ и крышкой } i \end{array} = \sum_{i=0}^{\infty} \begin{array}{c} \text{Пустая диаграмма} \end{array} = \infty \quad (5.60)$$

Проблема возникает, потому что чашки и крышки не являются *ограниченными* линейными отображениями, т. е. не удовлетворяют условию $\|M(v)\| < \infty$, если $\|v\| < \infty$. Таким образом, бесконечномерные гильбертовы пространства и ограниченные отображения образуют процессную теорию, но корректно определены только схемные диаграммы, поскольку в них нет чашек и крышек.

Можно было бы возразить, что это проблема струнных диаграмм. С другой стороны, ситуация (5.60) возникает не только для чашек и крышек, но и для любой прямолинейной корреляции. Следовательно:

формализм гильбертовых пространств явно исключает прямолинейные корреляции между бесконечномерными системами.

Далеко не очевидно, является ли это «свойством природы» или просто побочным эффектом математики гильбертовых пространств. И тут возникает два интересных вопроса:

- 1) какую часть теоретико-процессной формулировки квантовой теории можно обобщить на бесконечное число измерений (т. е. не прибегая к струнным диаграммам)?
- 2) можно ли модифицировать теорию гильбертовых пространств и ограниченных линейных отображений, так чтобы она включала струнные диаграммы и (или) прямолинейные корреляции в бесконечномерных пространствах?

В изучении обоих вопросов удалось продвинуться (см. раздел 5.7), но многое еще остается сделать.

5.6.2. Категории с суммами и базисами*

В теории категории есть большой подраздел (иногда называемый теорией абелевых категорий), где изучаются категории, морфизмы которых можно складывать. Категория, обладающая дополнительной структурой на множестве морфизмов, называется *обогащенной*. Интересующая нас дополнительная структура – это *коммутативный моноид*, т. е. множество M , обладающее ассоциативной и коммутативной операциями сложения с единицей. Например, согласно **условию 1** в определении 5.21, процессы одного типа в процессной теории с суммами образуют коммутативный моноид. А **условие 2** гарантирует, что категории, соответствующие процессным теориям с суммами, обладают еще и следующей структурой.

Определение 5.121. Говорят, что категория \mathcal{C} является *обогащенной коммутативными моноидами*, если для любой пары объектов A и B множество $\mathcal{C}(A, B)$ образует коммутативный моноид и структура этого моноида совместима с \circ -композицией:

$$\begin{cases} 0 \circ f = 0 = g \circ 0 \\ h \circ (f + g) = (h \circ f) + (h \circ g) \\ (g + h) \circ f = (g \circ f) + (h \circ f) \end{cases}$$

К понятию *суммы морфизмов* примыкает *прямая сумма объектов* (например, векторных пространств). В теории категорий это называется *бипроизведением*.

Определение 5.122. Пусть \mathcal{C} – категория, обогащенная коммутативными моноидами. Тогда \mathcal{C} обладает *бипроизведениями*, если для любой пары объектов A_1, A_2 существует третий объект $A_1 \oplus A_2$, пара отображений

$$l_j : A_j \mapsto A_1 \oplus A_2,$$

называемых *инъекциями*, и пара отображений:

$$\pi_j : A_1 \oplus A_2 \mapsto A_j,$$

называемых *проекциями*, которые удовлетворяют условиям

$$l_1 \circ \pi_1 + l_2 \circ \pi_2 = 1_{A_1 \oplus A_2}, \quad \pi_k \circ l_j = \begin{cases} 1_{A_j} & \text{если } j = k \\ 0 & \text{в противном случае} \end{cases}$$

Ну как, знакомо? Если еще нет, давайте привлечем инволюцию.

Определение 5.123. Пусть \mathcal{C} – инволютивная компактная замкнутая категория, обогащенная коммутативными моноидами. Говорят, что \mathcal{C} обладает *инволютивными бипроизведениями*, если для любой пары объектов A_1, A_2 существует третий объект

$$A_1 \oplus A_2,$$

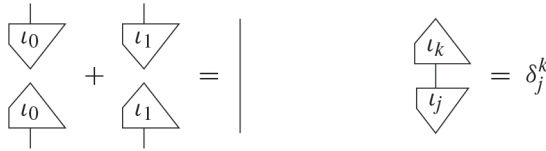
а также пара отображений:

$$l_j : A_j \mapsto A_1 \oplus A_2,$$

удовлетворяющих условиям:

$$l_1 \circ l_1^\dagger + l_2 \circ l_2^\dagger = 1_{A_1 \oplus A_2}, \quad l_k^\dagger \circ l_j = \begin{cases} 1_{A_j} & \text{если } j = k \\ 0 & \text{в противном случае} \end{cases}.$$

Если $A_1 = A_2 := I$ – тривиальный объект, то эти условия выглядят так:



Именно так:



образует двумерный ОНБ! С помощью равенств из определения 5.123 можно доказать, что операция \oplus ассоциативна (с точностью до изоморфизма), поэтому можно определить бипроизведения трех объектов:

$$A \oplus B \oplus C := (A \oplus B) \oplus C \cong A \oplus (B \oplus C)$$

и вообще N объектов. Тогда объекты, являющиеся бипроизведениями N экземпляров I :

$$A \cong I \oplus I \oplus \dots \oplus I, \tag{5.61}$$

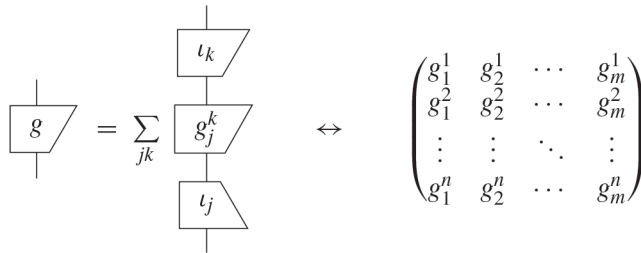
обладают N -мерными ОНБ. Чтобы понять, допускает ли объект что-то вроде ОНБ, мы можем сначала разложить его на *неприводимые* компоненты.

Определение 5.124. Объект называется *неприводимым*, если его нельзя представить в виде бипроизведения двух ненулевых объектов.

Теории **отношений** и **линейных отображений** имеют ОНБ для каждого типа, потому что единственным неприводимым объектом является тривиальная система. Иными словами, любой объект можно разложить в произведение вида (5.61). Однако существует много интересных алгебраических категорий (кольца, модули, представления алгебр и т. д.), обладающих гораздо более богатым набором неприводимых объектов. Интересно, что в нашем распоряжении по-прежнему имеется полезное матричное исчисление, только матрицы теперь состоят не из чисел, а из процессов. Предположим, что имеется такое довольно сложное отображение:

$$g : A_1 \oplus \dots \oplus A_m \rightarrow B_1 \oplus \dots \oplus B_n.$$

Тогда g можно разложить в «матричную форму», обобщающую матричную форму из равенства (5.14):



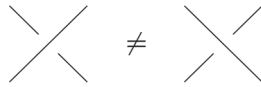
Элементами этой матрицы являются не числа, а морфизмы

$$g_j^k : A_j \rightarrow B_k.$$

Композиция таких матриц выглядит как композиция обычных матриц: суммы – это суммы, а «произведения» – композиция морфизмов. Поэтому мы можем продолжать считать, что занимаемся обычным матричным исчислением, но на самом деле это гораздо более общий (и мощный!) механизм.

5.6.3. Суммы в теории узлов*

В этой книге провода похожи на электрические провода в том смысле, что значение имеют только соединения. А вот если бы они были кусками веревки, то было бы интересно узнать, завязаны они в узел или заплетены в косу. И хорошо было бы различать такие две диаграммы:



Существует раздел математики – теория узлов, который как раз и занимается вопросами о том, завязаны ли веревки в узел или заплетены в косу. И, как выясняется, ответить на этот вопрос очень трудно.

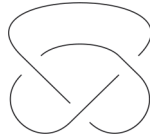
Изучение узлов и кос интересно не только само по себе, но и лежит в основе конкретной модели квантовых вычислений – *топологических квантовых вычислений*, в которой структура кос используется для кодирования квантовых вентилей. В исторических замечаниях в конце этого раздела мы приведем несколько ссылок на литературу.

Во введении мы уже приводили пример равенства, встречающегося в любом современном учебнике по теории узлов:

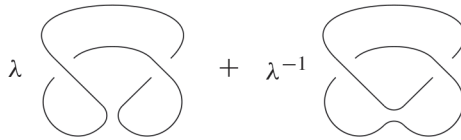
$$\text{Crossing} = \lambda \left| \text{Vertical} \right| + \lambda^{-1} \left| \text{Braid} \right| \tag{5.62}$$

А теперь мы объясним, как оно используется, – в качестве примера гибридного исчисления, включающего как диаграммы, так и традиционные математические понятия. Скобка *Кауффмана* (5.62) позволяет ассоциировать с любым узлом некий полином.

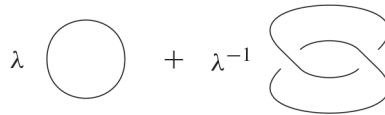
Рассмотрим *трилистный узел*, или просто *трилистник*:



Применив (5.62) к нижнему пересечению, получим:



После деформирования диаграмм получается:



Второе применение (5.62) дает:

$$\lambda \bigcirc + \bigcirc + \lambda^{-2} \bigcirc = (\lambda + 1 + \lambda^{-2}) \bigcirc$$

Помимо (5.62), имеет место равенство

$$\bigcirc = 1$$

Поэтому остается полином от λ :

$$\lambda + 1 + \lambda^{-2}.$$

Этот полином, называемый *скобочным полиномом*, является нормированным вариантом *полинома Джонса*, представляющего собой *инвариант узла*. То есть он одинаков для всех узлов, которые могут быть преобразованы друг в друга деформацией, и, значит, является чрезвычайно полезным средством классификации узлов.

5.6.4. Эквивалентность симметричных моноидальных категорий*

В разделе 5.2.5 мы дали неформальное определение эквивалентности процессных теорий. А сейчас мы формализуем его, воспользовавшись языком теории категорий.

Чтобы говорить об эквивалентности категорий, мы сначала должны определить, что значит интерпретировать морфизмы (т. е. процессы) одной симметрич-

ной моноидальной категории (СМК) как морфизмы другой категории. Мы сделаем это с помощью *функторов*, стандартных «отображений» между категориями.

Определение 5.125. (Строгий) *симметричный моноидальный функтор* F из СМК \mathcal{C} в СМК \mathcal{D} состоит из функции, отображающей объекты \mathcal{C} в объекты \mathcal{D} :

$$F : \text{ob}(\mathcal{C}) \mapsto \text{ob}(\mathcal{D}),$$

и для любой пары объектов A, B – функции, отображающей морфизмы \mathcal{C} в морфизмы \mathcal{D} (которая тоже обозначается буквой F):

$$F : \mathcal{C}(A, B) \mapsto \mathcal{D}(F(A), F(B)),$$

такой что « F сохраняет диаграммы», т. е.

- 1) F сохраняет параллельную композицию объектов и единичный объект:

$$F(A \otimes B) = F(A) \otimes F(B), \quad F(I) = I;$$

- 2) F сохраняет параллельную и последовательную композиции морфизмов:

$$F(f \otimes g) = F(f) \otimes F(g), \quad F(g \circ f) = F(g) \circ F(f);$$

- 3) F сохраняет единичные морфизмы и перекоммутации:

$$F(1_A) = 1_{F(A)}, \quad F(\sigma_{A,B}) = \sigma_{F(A),F(B)}.$$

Как и в определении моноидальной категории, прилагательное «строгий» означает, что равенства, в которых участвует параллельная композиция объектов, – «настоящие», т. е. выполняются буквально, а не с точностью до изоморфизма. Если его опустить, то условие 1 примет вид:

$$F(A \otimes B) \cong F(A) \otimes F(B), \quad F(I) \cong I, -$$

и мы должны будем потребовать, чтобы эти изоморфизмы подчинялись каким-то условиям когерентности, как для нестрогих СМК.

Простейший пример функтора – единичный функтор:

$$1_{\mathcal{C}} : \mathcal{C} \mapsto \mathcal{C},$$

который переводит любой объект и морфизм в себя. Можно очевидным образом определить последовательную композицию функторов:

$$(G \circ F)(X) = G(F(X)), \quad (G \circ F)(f) = G(F(f)), -$$

и тогда становится очевидно, что

$$F \circ 1_{\mathcal{C}} = F = 1_{\mathcal{D}} \circ F.$$

Более строгий способ придать смысл «одинаковости» двух категорий – установить изоморфизм между ними, который определяется так же, как изоморфизм объектов любого вида.

Определение 5.126. Две симметричные моноидальные категории называются *изоморфными*, если существуют симметричные моноидальные функторы:

$$F : \mathcal{C} \mapsto \mathcal{D}, \quad G : \mathcal{D} \mapsto \mathcal{C}, -$$

такие что

$$G \circ F = 1_{\mathcal{C}}, \quad F \circ G = 1_{\mathcal{D}}.$$

Другими словами, если выполнить сначала F , а потом G , то мы вернемся **точно** в исходную точку. Однако во многих случаях, например когда речь идет об эквивалентности теорий **линейных отображений** и $\mathbf{matrices}(\mathbb{C})$, мы вернемся не туда, откуда начали, а в какое-то место, которое «выглядит в точности так», как то, из которого мы отправлялись в путь. Иначе говоря, для любого объекта X объект $G(F(X))$ изоморфен X . Присвоим этому изоморфизму имя:

$$\eta_X : X \mapsto G(F(X)).$$

Разумеется, такой изоморфизм не единственный, мы имеем целое семейство изоморфизмов η_X, η_Y, \dots – для каждого объекта \mathcal{C} .

Итак, мы теперь знаем, что означает, что объекты выглядят в точности одинаковыми после путешествия по кругу, но что это может означать для морфизмов? Другими словами, как понимать, что

$$f : X \mapsto Y \quad \text{и} \quad G(F(f)) : G(F(X)) \mapsto G(F(Y))$$

делают «одно и то же»? Это означает, что если мы «закодируем» X как $G(F(X))$ посредством изоморфизма η_X , затем выполним $G(F(f))$, а потом «декодируем» результат, то должно получиться то же самое, что при выполнении просто f :

$$\eta_Y^{-1} \circ G(F(f)) \circ \eta_X = f. \tag{5.63}$$

Это значит, что η – не просто какое-то семейство изоморфизмов, а то, что мы называем *естественным изоморфизмом*. Перенеся η_Y в правую часть, получаем:

$$G(F(f)) \circ \eta_X = \eta_Y \circ f. \tag{5.64}$$

Это равенство обычно записывается в виде *коммутативной диаграммы*:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \eta_X \downarrow & & \downarrow \eta_Y \\ G(F(X)) & \xrightarrow{G(F(f))} & G(F(Y)) \end{array} \tag{5.65}$$

Коммутативная диаграмма – наглядный способ выразить равенство морфизмов. Она утверждает, что любые два пути с одинаковыми началом и концом дают один и тот же морфизм, получаемый посредством последовательной композиции. Таким образом, диаграмма выше выражает в точности то же самое, что равенство (5.64).

Замечание 5.127. Определение естественного изоморфизма на самом деле имеет смысл для любой пары функторов:

$$D, E : \mathcal{C} \mapsto \mathcal{D}, -$$

и в таком случае становится семейством изоморфизмов:

$$\{\iota_X : D(X) \mapsto E(X)\}_{X \in \mathcal{C}},$$

удовлетворяющим условию:

$$\begin{array}{ccc} D(X) & \xrightarrow{D(f)} & D(Y) \\ \iota_X \downarrow & & \downarrow \iota_Y \\ E(X) & \xrightarrow{E(f)} & E(Y) \end{array}$$

Тогда (5.65) является частным случаем, где $D := 1_{\mathcal{C}}$, а $E := G \circ F$. Мы также можем опустить требование о том, что каждый ι_X должен быть изоморфизмом, и тогда такое семейство будет называться *естественным преобразованием*.

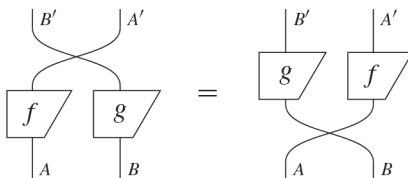
Пример 5.128. Обозначим $\mathcal{C} \times \mathcal{C}$ категорию, объектами которой являются пары (A, B) объектов из \mathcal{C} , а морфизмами – пары (f, g) морфизмов из \mathcal{C} . Тогда параллельная композиция в СМК индуцирует два функтора из произведения категорий $\mathcal{C} \times \mathcal{C}$ в категорию \mathcal{C} :

$$P_1 :: \begin{cases} (A, B) \mapsto A \otimes B \\ (f, g) \mapsto f \otimes g \end{cases} \qquad P_2 :: \begin{cases} (A, B) \mapsto B \otimes A \\ (g, f) \mapsto g \otimes f \end{cases}$$

Морфизмы перекоммутации в \mathcal{C} определяют естественный изоморфизм P_1 в P_2 . Естественность в данном случае приводит к следующей коммутативной диаграмме:

$$\begin{array}{ccc} A \otimes B & \xrightarrow{f \otimes g} & A' \otimes B' \\ \sigma_{A,B} \downarrow & & \downarrow \sigma_{A',B'} \\ B \otimes A & \xrightarrow{g \otimes f} & B' \otimes A' \end{array}$$

каковая, будучи записана в виде равенства между диаграммами, выглядит очень знакомо:



Аналогично изоморфизм ассоциативности и единичный изоморфизм для нестрогих СМК, упомянутые в разделе* 3.6.2:

$$\begin{aligned} \alpha_{A,B,C} : (A \otimes B) \otimes C &\mapsto A \otimes (B \otimes C), \\ \lambda_A : I \otimes A &\mapsto A, \quad \rho_A : A \otimes I \mapsto A, - \end{aligned}$$

тоже дают примеры естественных изоморфизмов для соответственно определенных функторов.

И последнее, что нужно для выражения «одинаковости» СМК, – определить естественный изоморфизм, сохраняющий параллельную композицию объектов:

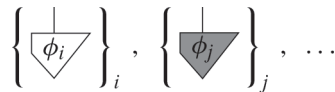
$$\eta_{X \otimes Y} = \eta_X \otimes \eta_Y,$$

который называется *моноидальным естественным изоморфизмом*. Тогда эквивалентность СМК – это пара функторов такая, что любая «круговая» композиция $(G \circ F$ и $F \circ G)$ дает нечто, изоморфное (конечно, моноидально) тому, с чего мы начинали.

Определение 5.129. Две симметричные моноидальные категории называются *эквивалентными*, если существуют симметричные моноидальные функторы $F : \mathcal{C} \mapsto \mathcal{D}$ и $G : \mathcal{D} \mapsto \mathcal{C}$ такие, что существуют моноидальные естественные изоморфизмы

$$\{\eta_X : X \mapsto G(F(X))\}_{X \in \text{ob } \mathcal{C}} \text{ и } \{\epsilon_Y : Y \mapsto F(G(Y))\}_{Y \in \text{ob } \mathcal{D}}.$$

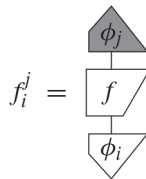
Можно разглядеть связь между теориями **линейных отображений** и **matrices**(\mathbb{C}), выраженную в этих терминах. Эти теории, рассматриваемые как СМК, обычно называются FHilb (finite-dimensional Hilbert spaces – конечномерные гильбертовы пространства) и Mat(\mathbb{C}) соответственно. Для гильбертовых пространств A, B, \dots зафиксируем базисы:



Затем обозначим

$$F : \text{FHilb} \mapsto \text{Mat}(\mathbb{C})$$

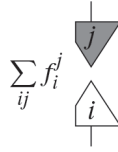
функтор, который сопоставляет каждому гильбертову пространству его размерность, а каждому линейному отображению – матрицу с элементами



В обратном направлении обозначим

$$G : \text{Mat}(\mathbb{C}) \mapsto \text{FHilb}$$

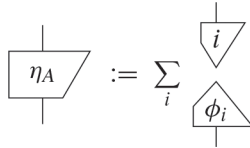
функтор, который сопоставляет натуральному числу $d \in \text{ob}(\text{Mat}(\mathbb{C}))$ гильбертово пространство \mathbb{C}^d , а матрице с элементами f_i^j – линейное отображение



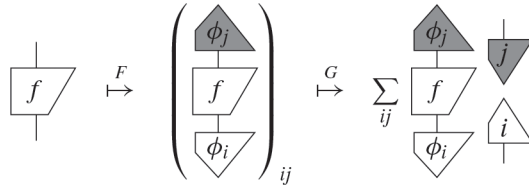
Таким образом, имеем

$$A \xrightarrow{F} d = \dim(A) \xrightarrow{G} \mathbb{C}^d$$

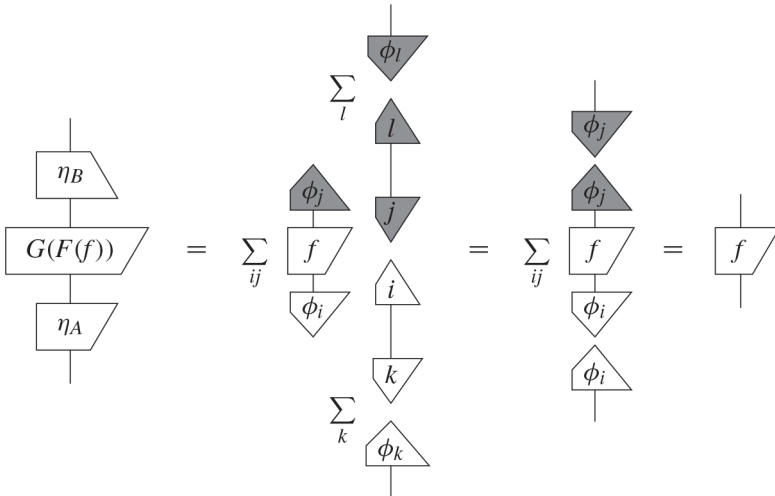
В данном случае $A \neq \mathbb{C}^d$, но поскольку эти два гильбертова пространства имеют одинаковую размерность, существует унитарный процесс



который, конечно, является также изоморфизмом. Теперь взглянем на композицию линейных отображений:



Это не тождественное отображение. Но его можно «декодировать», как мы сделали в (5.63), используя естественные изоморфизмы:



ко всему базису. Иногда состояние Белла также называют «ЭПР-состоянием», но чаще под *ЭПР-состоянием* понимают состояние B_3 из описанных в формулах (5.50). Причина такого выделения этого состояния заключается в том, что из всех состояний Белла только оно *антисимметрично* и на самом деле является единственным антисимметричным состоянием для пары двумерных квантовых систем. Здесь под *антисимметричностью* понимается тот факт, что если поменять две системы местами, то получится то же состояние с точностью до умножения на -1 .

$$\begin{array}{c} \downarrow \\ \text{---} \end{array}
 \left(\begin{array}{c} \diagup \diagdown \\ \diagdown \diagup \end{array} \right) - \left(\begin{array}{c} \diagdown \diagup \\ \diagup \diagdown \end{array} \right) = \diamond(-1) \left(\begin{array}{c} \downarrow \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \downarrow \end{array} - \begin{array}{c} \downarrow \\ \downarrow \end{array} \begin{array}{c} \downarrow \\ \downarrow \end{array} \right)$$

Системы, обладающие свойством антисимметрии, называются *фермионами*. Три остальных состояния Белла называются *бозонами*, это означает, что после перестановки двух систем получается в точности то же самое состояние. Использование сумм и матричной структуры в дополнение к струнным диаграммам для моделирования квантовых систем было инициировано в работе Abramsky and Coecke (2004) в форме бипроизведений – теоретико-категорного аналога матричного исчисления, описанного в разделе* 5.6.2. Кстати говоря, второму автору этой статьи бипроизведения никогда не нравились. И если бы ничего, кроме бипроизведений, не было, то книга на этом месте и закончилась бы. К счастью, это не так, и тому, что есть еще, посвящены оставшиеся 66,6 %.

Бипроизведения возникли в ходе изучения абелевых категорий, которые в некоторых важных отношениях напоминают абелевы группы. Впервые они появились в работе Mac Lane (1950) по следам обсуждения с Эйленбергом вопроса о том, какие категории подходят для работы с гомологиями и когомологиями топологических пространств. В результате последующих работ Buchsbaum (1955) и Grothendieck (1957) такие категории стали играть важную роль в магистральном направлении развития алгебраической топологии и геометрии. Стандартным учебником по этой теме является книга Freyd (1964).

Теорию категорий придумали Эйленберг и Маклейн (Eilenberg and Mac Lane, 1945) специально для того, чтобы ответить на вопрос, что такое эквивалентность процессных теорий. Однако идея о том, что морфизм следует рассматривать как процесс, получила широкое распространение много позже (см. Baez and Lauda, 2011). Процессные теории, которые первоначально имели в виду Эйленберг и Маклейн, обладали только последовательной, но не параллельной композицией, поэтому эквивалентность в их понимании должна была сохранять лишь операцию \circ . Но с появлением параллельной композиции, т. е. моноидальных категорий (Benabou, 1963; Mac Lane, 1963), пришло и понятие моноидальной эквивалентности категорий, введенное в разделе* 5.6.4.

В работе Selinger (2011a) доказана полнота струнных диаграмм относительно **линейных отображений**, что стало развитием аналогичного результата для векторных пространств (т. е. без операции адьюнкции), полученного в работе Hasegawa, Hofmann and Plotkin (2008).

Обсуждение квантовых протоколов в терминах несамодвойственных чашек и крышек, в т. ч. и успешной попытки реализовать их, содержится в работах Coecke

et al. (2008a), Paquette (2008) и Kissinger (2012a). Гораздо раньше эта тема активно изучалась в математике, например при рассмотрении квантовых групп (Kassel, 1995). За открытие полинома Джонса, впервые описанного в работе Jones (1985), Вон Джонс был удостоен филдсовской медали, которую иногда называют нобелевской премией для математиков. Спустя несколько лет Луис Кауффман в работе Kauffman (1987) описал свою скобку как простой способ порождения полинома Джонса. В работе Kauffman (1991) исследуются взаимосвязи между теорией узлов и физикой. Работа Panangaden and Paquette (2011) посвящена топологическим квантовым вычислениям, а связи между перекрестьями и теми видами диаграмм, которые рассматриваются в этой книге, исследуются в работе Fauser (2013).

Глава 6

Квантовые процессы

Искусство прогресса состоит в том, чтобы сохранять порядок среди изменений и сохранять изменения среди порядка.

– Альфред Норт Уайтхед
«Процесс и реальность», 1929

Начиная с этого момента, не будет никаких младенцев, удлинителей и кулинарии: мы сосредоточимся исключительно на квантовых процессах. Естественно, нашей первой целью будет построение теории **квантовых процессов**. К счастью, благодаря проделанной выше работе мы уже довольно близки к этой цели.

Начать с того, что процессная теория **линейных отображений** не слишком далека от полномасштабной теории **квантовых процессов**. В частности, теория **квантовых процессов** наследует от нее описание струнных диаграмм. Это дает нам высокоуровневый язык, который сильно упрощает рассуждения о квантовых процессах, например в контексте квантовых вычислений и проектирования квантовых протоколов. Это также означает, что мы уже знакомы с некоторыми особенностями квантовых процессов по разделу 4.4, а точнее с теми, которые справедливы для всех процессных теорий, допускающих струнные диаграммы: существование неразделимых состояний, теорема о невозможности клонирования, телепортация и т. д.

Заметьте – мы говорим, что **линейные отображения** не слишком далеки от **квантовых процессов**, но не утверждаем, будто они являются квантовыми процессами. В этой главе мы перейдем от **линейных отображений** к **квантовым процессам** за несколько шагов (рис. 6.1) и по ходу дела исправим присущие первым недостатки. Первая проблема состоит в том, что теория **линейных отображений**, рассматриваемая как модель квантовых процессов, содержит избыточные данные – «глобальные фазы». Они не могут быть обнаружены никакими квантовыми измерениями (о которых речь пойдет в следующей главе), а потому никак не влияют на то, какой процесс протекает в действительности.

Ну и что с того? Кому какое дело? Мы могли бы продолжать пользоваться линейными отображениями, игнорируя глобальные фазы, когда возникает такая необходимость. На самом деле во многих учебниках квантовой теории так и поступают. С другой стороны, обобщенное правило Борна

$$\left. \begin{array}{l} \text{Испытание} \\ \text{Состояние} \end{array} \right\} \left\{ \begin{array}{c} \triangle \phi \\ \downarrow \\ \triangle \psi \end{array} \right\} \text{Вероятность} \quad (6.1)$$

не работало бы, поскольку генерируются не положительные вещественные числа (которые можно интерпретировать как вероятности), а комплексные числа.

Мы решим эту проблему, произведя простое построение, которое порождает из теории **линейных отображений** новую теорию **квантовых отображений**, правильно описывающую процессы, которые могут иметь место в квантовой теории.

Сначала в разделе 6.1 мы преобразуем **линейные отображения** в **чистые квантовые отображения**, создав *дубль* каждого процесса. Это одним махом разрешит проблему глобальных фаз и вероятностей.

Затем в разделе 6.2.1 мы покажем, что чистые квантовые отображения не включают один очень важный процесс: процесс *отбрасывания* системы. Часто мы хотим игнорировать какую-то часть большой системы, если она находится вне нашего контроля (например, потенциальное средство подслушивания в протоколе безопасности) или просто несущественно (например, электроны, летающие вокруг Марса). Добавив процесс отбрасывания в теорию чистых квантовых отображений, мы получим теорию **квантовых отображений**. Путем композиции чистых квантовых отображений с процессом отбрасывания можно получить много *нечистых* (или *смешанных*) квантовых отображений.

Альтернативную интерпретацию нечистоты некоторых квантовых отображений дает *вероятностное смешивание*. В классической физике вероятности можно рассматривать как способ учесть неполноту наших знаний о состоянии системы. В разделе физики, который называется *статистической механикой*, состояния системы описываются с помощью распределений вероятностей, поскольку почти невозможно знать состояние каждой частицы. Такой же смысл вероятностное смешивание имеет в квантовой теории: недостаток знаний о том, какой процесс протекает в действительности.

Обратите внимание на наши слова о том, что квантовые отображения описывают процессы, которые **«могут иметь место»**. В отличие от классической физики, в квантовой теории существуют принципиально недетерминированные процессы. Иначе говоря, существуют процессы, недетерминированность которых обусловлена не только недостаточностью знаний о квантовой системе. Вне зависимости от того, насколько полны наши знания о состоянии системы, исход такого процесса становится известен только после того, как он произойдет. Именно эта особенность квантовой теории категорически не устраивала Эйнштейна, обронившего знаменитую фразу «Бог не играет в кости». Чтобы учесть это «квантовое бросание костей», мы предпримем третий и последний шаг в этой главе – определим **квантовые процессы** как наборы **квантовых отображений**, в совокупности определяющих альтернативные варианты развития событий. Правило, диктующее, какие совокупности **квантовых отображений** образуют допустимые **квантовые процессы**, называется *принципом причинности*.

Эти принципиально недетерминированные процессы составляют неотъемлемую часть квантовой теории, по крайней мере, по двум причинам:

- 1) *квантовое измерение* – единственный способ взаимодействия с квантовыми системами – является недетерминированным процессом (вспомните о недетерминированных путешествиях Дэйва, про которые мы рассказывали во введении);

- 2) принцип причинности налагает строгое ограничение на то, какие квантовые отображения могут входить в состав детерминированных квантовых процессов. Например, единственный детерминированный квантовый эффект – это отбрасывание. С другой стороны, любое квантовое отображение можно реализовать как часть недетерминированного квантового процесса. Этот факт имеет первостепенное значение для реализации квантовой телепортации, и не только.

Принцип причинности тесно связан с концепцией причинности в физике. В частности, в разделе 6.3.2 мы увидим, что он запрещает «распространение сигнала со скоростью больше скорости света» и тем самым гарантирует, что квантовая теория не вступает в конфликт с другой экстравагантной физической теорией – *теорией относительности*. Мы не хотим расстраивать Эйнштейна еще сильнее!

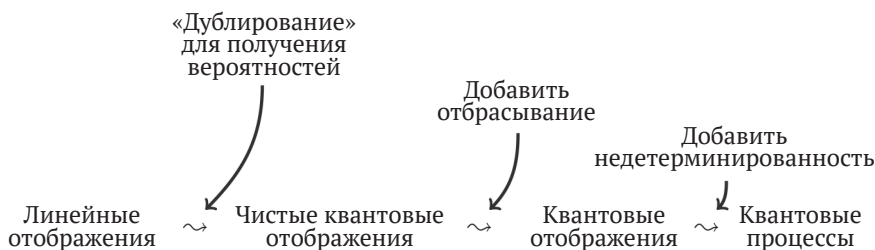


Рис. 6.1. Переход от линейных отображений к квантовым процессам

6.1. ПЕРЕХОД К ЧИСТЫМ КВАНТОВЫМ ОТОБРАЖЕНИЯМ ПУТЕМ ДУБЛИРОВАНИЯ

В предыдущей главе мы проделали большую работу, чтобы определить и изучить **линейные отображения**, поэтому может возникнуть мысль, будто это и есть вся квантовая теория. Это почти правда. Напомним, что в разделе 3.4.1 мы говорили, что эффекты можно интерпретировать как «испытания», а в разделе 4.3.1 – что адьюнкт состояния ψ соответствует проверке нахождения системы в состоянии ψ . Когда такое испытание компонуется с состоянием, получающееся число должно быть вероятностью получить в испытании ответ «да».

Однако в случае **линейных отображений** при выборе двух произвольных состояний ψ и ϕ вполне может оказаться, что их внутреннее произведение не является вещественным числом, а уж тем более вероятностью (т. е. вещественным числом от 0 до 1). Поэтому процессная теория **линейных отображений** – неподходящий кандидат для описания квантовых процессов. Но мы можем поправить это с помощью *дублирования* и назвать результат процессной теорией **чистых квантовых отображений**.

Ко всему прочему, у дублирования есть два приятных следствия.

1. Оно автоматически устраняет избыточные *глобальные фазы* (раздел 6.1.2).
2. Оно оставляет место для двух новых ингредиентов, которых не было в теории **линейных отображений**: *отображения отбрасывания* (раздел 6.2.1.1) и *классических проводов* (глава 8).

6.1.1. Дублирование порождает вероятности

Напомним (см. предложение 5.70), что если умножить число на сопряженное к нему, то получится положительное число:

$$0 \leq \begin{array}{c} \triangle \phi \\ | \\ \nabla \psi \end{array} \begin{array}{c} \triangle \phi \\ | \\ \nabla \psi \end{array} \quad (6.2)$$

Более того, если ψ и ϕ нормированны, то это будет вещественное число от 0 до 1, т. е. вероятность. Вместо того чтобы доказывать это утверждение напрямую, мы установим более общий факт, которые впоследствии окажется полезен.

Лемма 6.1. Для любого ОНБ и любого нормированного состояния ψ

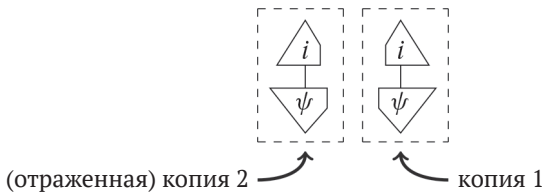
$$\sum_i \begin{array}{c} \triangle i \\ | \\ \nabla \psi \end{array} \begin{array}{c} \triangle i \\ | \\ \nabla \psi \end{array} = 1 \quad (6.3)$$

Доказательство. Имеем

$$1 = \begin{array}{c} \triangle \psi \\ | \\ \nabla \psi \end{array} \stackrel{(5.17)}{=} \sum_i \begin{array}{c} \triangle \psi \\ | \\ \triangle i \\ | \\ \triangle i \\ | \\ \nabla \psi \end{array} = \sum_i \begin{array}{c} \triangle i \\ | \\ \nabla \psi \end{array} \begin{array}{c} \triangle i \\ | \\ \nabla \psi \end{array}$$

где на последнем шаге используется самотранспонированность чисел. □

Эта лемма утверждает, что для любого нормированного состояния в совокупности с любым ОНБ рассмотрение «дублированного внутреннего произведения»



дает распределение вероятностей (см. определение 5.35), т. е. список положительных вещественных чисел, сумма которых равна 1.

Замечание 6.2. В следующей главе мы увидим, что ОНБ представляют некие квантовые измерения, а тогда лемма 6.1 гарантирует, что сумма вероятностей всех возможных исходов равна 1.

В предложении 5.79 мы показали, что любое ортонормированное множество можно продолжить до ОНБ. В частности, это верно для единственного нормированного состояния ϕ :

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} := \begin{array}{c} \downarrow \\ \triangle \\ \phi \end{array}, \begin{array}{c} \downarrow \\ \triangle \\ 2 \end{array}, \dots, \begin{array}{c} \downarrow \\ \triangle \\ n \end{array} \right\}.$$

Для этого ОНБ равенство (6.3) может выполняться, только если

$$\begin{array}{cc} \triangle & \triangle \\ \phi & \phi \\ \downarrow & \downarrow \\ \triangle & \triangle \\ \psi & \psi \end{array} \leq 1$$

поэтому мы получаем

Следствие 6.3. Для нормированных состояний и эффектов имеет место неравенство

$$0 \leq \begin{array}{cc} \triangle & \triangle \\ \phi & \phi \\ \downarrow & \downarrow \\ \triangle & \triangle \\ \psi & \psi \end{array} \leq 1 \tag{6.4}$$

Эти диаграммы дублированного внутреннего произведения составляют основной механизм вычисления вероятностей в квантовой теории, это именно то, что называется «правилом Борна» в стандартных учебниках. Поначалу эта новая штука не кажется похожей на обобщенное правило Борна из раздела 3.4. Но ничего, скоро все изменится!

Замечание 6.4. Чаше встречается вторая или третья из следующих трех эквивалентных форм правила Борна:

$$\begin{array}{cc} \triangle & \triangle \\ \phi & \phi \\ \downarrow & \downarrow \\ \triangle & \triangle \\ \psi & \psi \end{array} = \begin{array}{cc} \triangle & \triangle \\ \phi & \psi \\ \downarrow & \downarrow \\ \triangle & \triangle \\ \psi & \phi \end{array} = \begin{array}{c} \triangle \\ \phi \\ \downarrow \\ \triangle \\ \psi \\ \downarrow \\ \triangle \\ \psi \end{array}$$

Первое равенство следует из того факта, что числа самотранспонированные, второе является просто результатом деформирования диаграммы. В более традиционной нотации эти альтернативные формы выглядят соответственно так:

$$\langle \psi | \phi \rangle \langle \phi | \psi \rangle = |\langle \psi | \phi \rangle|^2, \quad \text{tr}(P_{|\phi\rangle} \rho_{|\psi\rangle}),$$

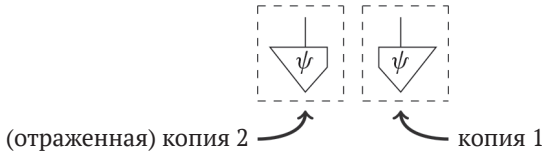
где

$$P_{|\psi\rangle} = \rho_{|\psi\rangle} := |\psi\rangle\langle\psi|.$$

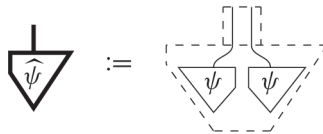
Смысл нашего выражения правила Борна – это как раз то, чему в основном посвящена оставшаяся часть этого раздела: благодаря преобразованию состояний

и эффектов в «дублированную» форму правило Борна сводится к простейшему способу порождения числа из состояния и эффекта, а именно их композиции.

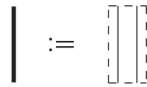
Ключевой момент состоит в том, что вероятности в дублированном внутреннем произведении (6.4) зависят не от самого ψ , а от «дублированного ψ »:



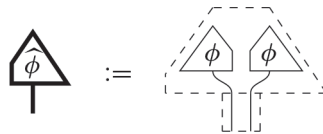
Таким образом, чтобы реализовать их в виде экземпляра обобщенного правила Борна (6.1), мы можем просто рассматривать дублированное ψ как полноправного гражданина, т. е. как состояние



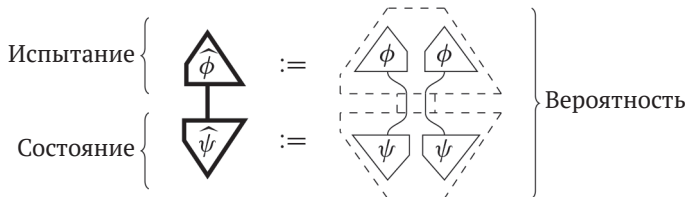
в новой «дублированной процессной теории». Иными словами, для любого состояния ψ гильбертова пространства A мы определяем новое состояние $\hat{\psi}$, являющееся дублированной версией ψ , и приписываем $\hat{\psi}$ новый тип \hat{A} , который втайне является не чем иным, как двумя копиями A . На диаграмме это выглядит так:



Аналогично мы можем определить новые эффекты для этого типа \hat{A} :

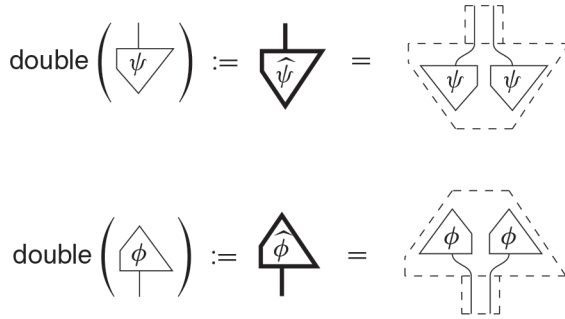


Вместе новое состояние и новый эффект дают:



Бинго! Мы видим правило Борна (6.4) из квантовой теории, возникшее как частный случай обобщенного правила Борна (6.1).

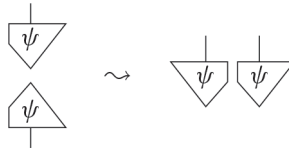
Эти дублированные состояния и эффекты мы называем *чистыми квантовыми состояниями* и *чистыми квантовыми эффектами* соответственно. Иногда мы будем использовать следующую нотацию:



Замечание 6.5. Этот «прием с дублированием» тесно связан с конструкцией, встречающейся в квантовой теории, а именно переходом от вектора чистого состояния $|\psi\rangle$ к ассоциированному с ним оператору плотности:

$$\tilde{\psi} := |\psi\rangle\langle\psi|.$$

Данные здесь те же, что в дублированном состоянии, в чем легко убедиться, транспонировав эффект ψ в сопряжение состояния ψ :



Если состояние ψ нормированное, то в силу (4.53) оператор плотности $\tilde{\psi}$ является проектором. Эти проекторы играют роль квантовых состояний в традиционной литературе. Однако в парадигме процессных теорий состояния считаются процессами без входов. Очевидно, что операторы плотности нарушают это соглашение, что впоследствии станет источником некоторых неприятностей (см. замечание 6.50). С другой стороны, наши дублированные состояния не противоречат соглашению (что очень удобно).

6.1.2. Дублирование устраняет глобальные фазы

Как мы уже отмечали, вероятности, порождаемые по правилу Борна, зависят не от ψ , а от «дублированного ψ ». Это различие может показаться тривиальным, пока мы не осознаем, что соответствие между состояниями и дублированными состояниями не взаимно однозначное, а типа «многие к одному». Этот феномен имеет место и для чисел. Существует много комплексных чисел λ таких, что

$$\bar{\lambda} = 1, \tag{6.5}$$

например $1, -1, i, -i$.

В разделе 5.3.1 мы видели, что любое комплексное число можно записать в виде:

$$re^{i\alpha}.$$

Равенство (6.5) просто означает, что $r = 1$, т. е. любое подходящее λ имеет вид:

$$e^{i\alpha}.$$

По определению, произведение такого числа на сопряженное к нему равно 1, поэтому на дублированное состояние они не оказывают влияния. На самом деле это единственные данные, которые теряются при переходе к дублированному состоянию.

Предложение 6.6. Два состояния ψ и ϕ переходят в одно и то же дублированное состояние тогда и только тогда, когда они равны с точностью до числа вида $e^{i\alpha}$, т. е.

$$\begin{array}{c} \downarrow \\ \psi \end{array} \begin{array}{c} \downarrow \\ \psi \end{array} = \begin{array}{c} \downarrow \\ \phi \end{array} \begin{array}{c} \downarrow \\ \phi \end{array} \iff \begin{array}{c} \downarrow \\ \psi \end{array} = e^{i\alpha} \begin{array}{c} \downarrow \\ \phi \end{array}$$

для некоторого $\alpha \in [0, 2\pi)$. Число $e^{i\alpha}$ называется *глобальной фазой*.

Это частный случай более общего утверждения, которое мы докажем ниже как теорему 6.17.

Вообще-то, с самого начала квантовой теории, сформулированной фон Нейманом, глобальные состояния были объявлены бессмысленными, но оставались явной частью формализма. В большинстве учебников по квантовой теории с этим затруднением борются, резервируя термин «квантовое состояние» за «классом эквивалентности» состояний, равных с точностью до глобальной фазы. Однако дублирование дает более простой и элегантный способ решения этой проблемы.

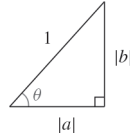
Обычное обоснование объявления глобальных фаз физически бессмысленными заключается в том, что они эмпирически недоступны, т. е. их нельзя обнаружить с помощью квантовых измерений, которые мы будем изучать в главе 7. Это явствует уже из того факта, что все вероятности, порождаемые квантовой теорией, дает правило Борна, которое зависит только от дублированных состояний и эффектов. Поэтому нет никакого смысла различать состояния, отличающиеся только глобальной фазой.

Игнорирование глобальных фаз имеет и полезные практические следствия: оно позволяет нашему слабому человеческому мозгу представлять квантовые системы геометрически. Это очень удобно в физике, и мы прибегаем к этому постоянно.

Состояния простейшей нетривиальной квантовой системы, кубиты, принадлежат $\widehat{\mathbb{C}}^2$. Поскольку такое состояние можно представить двумя комплексными числами, то можно и четырьмя вещественными. Поэтому на первый, наивный взгляд кажется, что для записи состояния кубита нужно четырехмерное пространство. Но это на одно измерение больше, чем способен вообразить человек (по крайней мере, большинство из нас)! Задача существенно упрощается, если рассматривать только нормированные состояния. Пусть

$$\begin{array}{c} \downarrow \\ \psi \end{array} = a \begin{array}{c} \downarrow \\ 0 \end{array} + b \begin{array}{c} \downarrow \\ 1 \end{array}$$

Тогда если ψ нормированно, то должно выполняться условие $|a|^2 + |b|^2 = 1$. Стало быть, если мы хотим знать $|a|$ и $|b|$, то можем воспользоваться теоремой Пифагора:



Если вы еще не забыли тригонометрию, то знаете, что $|a| = \cos \theta$, $|b| = \sin \theta$. Ну а если забыли, поверьте нам на слово.

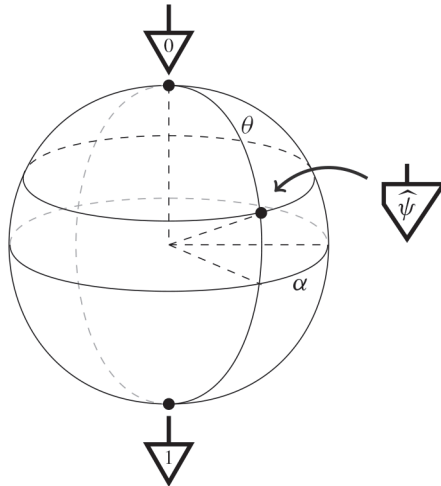
Технически немного удобнее использовать $\theta/2$ вместо θ , поэтому положим $|a| = \cos(\theta/2)$ и $|b| = \sin(\theta/2)$. Затем мы можем избавиться от абсолютных величин, введя комплексные фазы, что дает:

$$\downarrow\psi = \cos \frac{\theta}{2} e^{i\beta} \downarrow 0 + \sin \frac{\theta}{2} e^{i\gamma} \downarrow 1$$

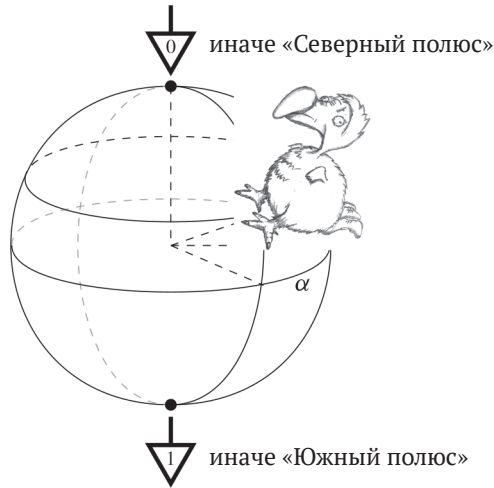
Итак, мы заменили четыре вещественных параметра тремя углами. Вот тут и вступает в игру дублирование. Поскольку дублирование уничтожает глобальные фазы, угол β на самом деле избыточен, т. к. мы можем умножить все выражение на $e^{-i\beta}$. Поэтому квантовое состояние $\widehat{\psi}$ можно удобно записать в виде

$$\downarrow\widehat{\psi} := \text{double} \left(\cos \frac{\theta}{2} \downarrow 0 + \sin \frac{\theta}{2} e^{i\alpha} \downarrow 1 \right)$$

для некоторого угла α (а именно $\alpha := \gamma - \beta$). Поскольку квантовое состояние теперь полностью описывается двумя углами, его можно изобразить на сфере, которая называется *сферой Блоха*:



Этот рисунок полезен для тренировки интуиции. Например, чем сильнее «похожи» два состояния, тем больше их внутреннее произведение и тем ближе они друг к другу на сфере Блоха. В частности, ортогональные состояния всегда являются антиподами. Помните путешествия Дэйва в разделе 1.1? Теперь мы знаем, по какой сфере он скакал:



Упражнение 6.7. Покажите, что точки

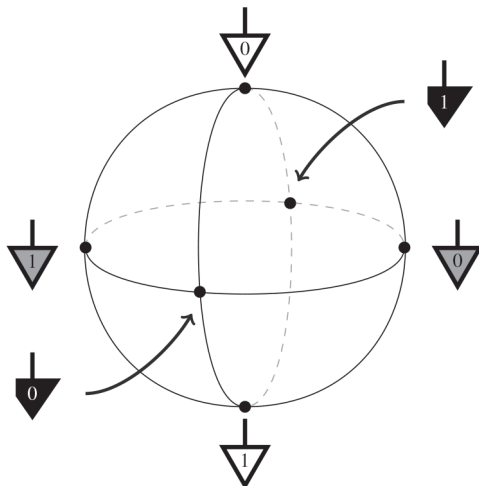
$$\begin{array}{c} \downarrow \\ 0 \end{array} := \text{double} \left(\frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \right) \right)$$

$$\begin{array}{c} \downarrow \\ 1 \end{array} := \text{double} \left(\frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} - \begin{array}{c} \downarrow \\ 1 \end{array} \right) \right)$$

$$\begin{array}{c} \downarrow \\ 0 \end{array} := \text{double} \left(\frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} + i \begin{array}{c} \downarrow \\ 1 \end{array} \right) \right)$$

$$\begin{array}{c} \downarrow \\ 1 \end{array} := \text{double} \left(\frac{1}{\sqrt{2}} \left(\begin{array}{c} \downarrow \\ 0 \end{array} - i \begin{array}{c} \downarrow \\ 1 \end{array} \right) \right)$$

расположены на сфере Блоха следующим образом:



чистые квантовые отображения \subseteq линейные отображения.

Специально отметим: тот факт, что теория **линейных отображений** допускает струнные диаграммы, наследуется теорией **чистых квантовых отображений**. Применение равенства (6.7) к чашке дает «перекрещенную» дублированную чашку:

$$\cup := \text{double}(\cup) = \text{diagram with two strands crossing} = \text{dashed double cup}$$

и аналогично для дублированной крышки:

$$\cap := \text{diagram with two strands crossing} = \text{dashed double cap}$$

Композиция того и другого сокращает «перекрещивания», и получается первое уравнение разгибания:

$$\text{cup followed by cap} = \text{dashed double cup followed by dashed double cap} = \text{two vertical lines} = \text{one vertical line}$$

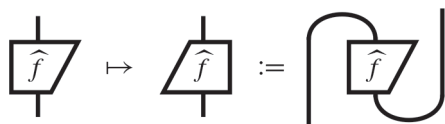
Что касается остальных двух уравнений разгибания, то применение первого уравнения (6.7) к отображению перекоммутации дает дублированную перекоммутацию:

$$\times := \text{double}(\times) = \text{diagram with four strands crossing} = \text{dashed double crossing}$$

а его композиция с крышкой или чашкой дает

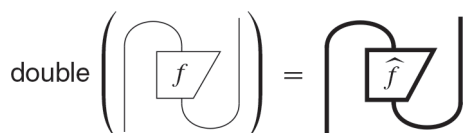
$$\text{cup followed by crossing} = \text{cup} \quad \text{cap followed by crossing} = \text{cap}$$

Поскольку существуют чашки и крышки, в дублированной теории определено также понятие транспонирования:

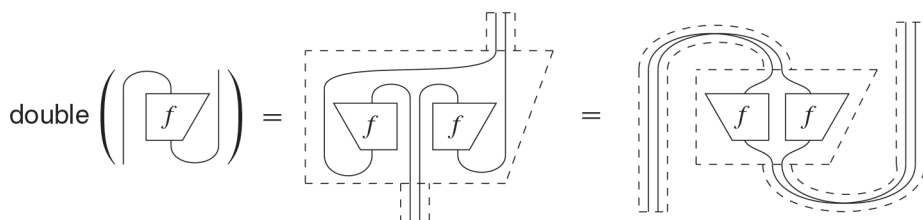


которое, как выясняется, совпадает с транспонированием в недублированной теории.

Предложение 6.9. Дублирование сохраняет транспонирование:

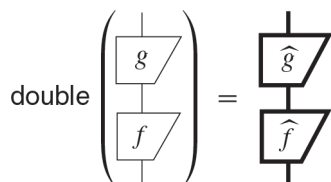


Доказательство. В случае одного входа и выхода имеем:

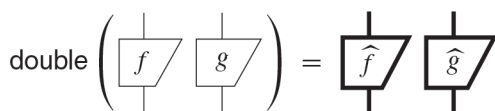


Для случая нескольких входов и выходов равенство (6.7) доказывается аналогично. □

То, что дублирование сохраняет транспонирование, – проявление более общего факта: дублирование сохраняет диаграммы. Убедиться в этом проще всего, разложив струнную диаграмму на составляющие процессы. Мы уже знаем, что дублирование переводит чашки в чашки, а крышки в крышки. Очевидно, что дублирование сохраняет последовательную композицию:



Упражнение 6.10. Докажите, что дублирование сохраняет параллельную композицию:



Дублированная теория также наследует адьюнкты от недублированной:

$$\widehat{f} := \text{double}(f) \quad (6.8)$$

Если сложить все это вместе, то мы приходим к следующему утверждению.

Следствие 6.11. Дублирование сохраняет струнные диаграммы:

$$\text{double} \left(\text{diagram with } g, f, h \right) = \text{diagram with } \widehat{g}, \widehat{f}, \widehat{h}$$

Таким образом, любые вычисления, возможные для диаграмм **линейных отображений**, переносятся на **чистые квантовые отображения** – нужно лишь удвоить все диаграммы.

Пример 6.12. В разделе 5.3.6 мы реализовали телепортацию в теории **линейных отображений** с помощью отображений Белла. Для перехода к квантовым отображениям нужно просто все удвоить (кроме Алекса и Боба, конечно):

$$\text{double} \left(\text{Bell state diagram} \right) = \text{doubled Bell state diagram}$$

Пример 6.13. В разделах 5.3.4 и 5.3.5 мы показали, как преобразовать классические логические вентили в линейные отображения. Теперь, опираясь на дублирование, мы можем преобразовать их в **квантовые (логические) вентили**. Вот, например, как выглядят **квантовый вентиль NOT**:

$$\widehat{\pi} := \text{double}(\pi)$$

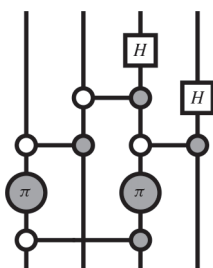
квантовый вентиль CNOT:

$$\text{CNOT} := \text{double} \left(\text{CNOT}_{\text{classical}} \right)$$

и вентиль Адамара:

$$H := \text{double} \left(H_{\text{classical}} \right)$$

у которого даже нет классического аналога. Квантовые схемы описывают применение квантовых вентилях к фиксированному числу кубитов, например:

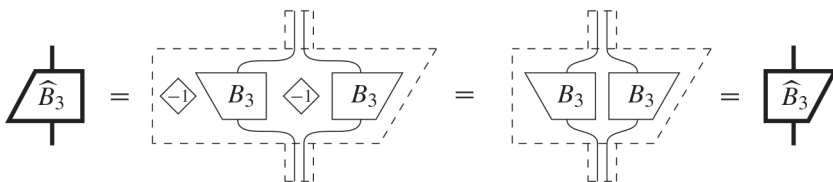


За исключением вентилях Адамара, все это можно было бы сделать, применяя классические логические вентили. Интересное начнется, когда в главе 9 мы введем в рассмотрение фазовые вентили.

Пример 6.14. При дублировании матриц Белла из раздела 5.3.6 матрица

$$B_3 \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

становится самотранспонированной, поскольку дублирование устраняет глобальные фазы:



Для соответствующего состояния Белла также имеем:

$$\text{double} \left(\begin{matrix} \downarrow 0 & \downarrow 1 \\ \downarrow 1 & \downarrow 0 \end{matrix} - \begin{matrix} \downarrow 1 & \downarrow 0 \\ \downarrow 0 & \downarrow 1 \end{matrix} \right) = \text{double} \left(\begin{matrix} \downarrow 1 & \downarrow 0 \\ \downarrow 0 & \downarrow 1 \end{matrix} \right)$$

Вообще, мы будем и дальше пользоваться для **чистых квантовых отображений** той же терминологией, что для процессов в любой другой теории. Но некоторые концепции настолько важны, что заслуживают специальных «квантовых» названий.

Определение 6.15. \otimes -неразделимое чистое квантовое состояние называется *запутанным состоянием*.

Таким образом, запутанным чистым состоянием является любое двухкомпонентное состояние $\hat{\psi}$ в теории **чистых квантовых отображений**, которое не разлагается на два односистемных состояния $\hat{\psi}_1$ и $\hat{\psi}_2$:



Примером может служить (дублированное) состояние Белла:

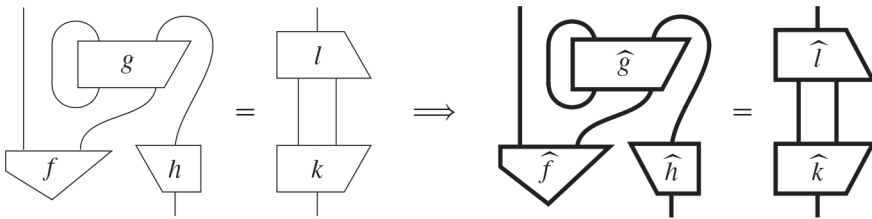
$$\text{double} \left(\frac{1}{\sqrt{D}} \cup \right) = \frac{1}{D} \cup$$

Как отмечалось в замечании 4.1, нам придется уточнить это определение запутанности при переходе от чистых квантовых состояний к более общим квантовым состояниям. Мы сделаем это в разделе 8.3.5.

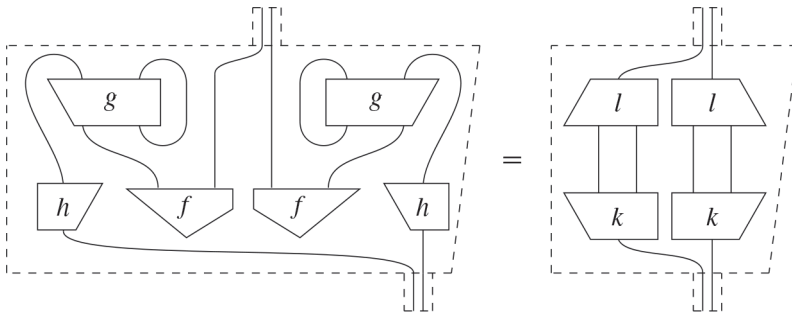
6.1.4. Что сохраняется при дублировании

В силу следствия 6.11 дублирование сохраняет струнные диаграммы, т. е. если две диаграммы равны, то результаты их дублирования тоже будут равны.

Следствие 6.16. Любое равенство между струнными диаграммами «одиночных» процессов справедливо также для дублированных диаграмм:



В этом можно убедиться, просто раскрыв обе части дублированного равенства:

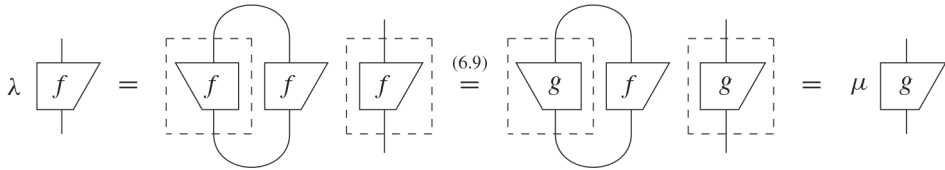


$$1 = \frac{\mu \bar{\mu}}{\lambda \bar{\lambda}} = \left(\frac{\mu}{\lambda}\right) \overline{\left(\frac{\mu}{\lambda}\right)}$$

Таким образом, μ/λ – глобальная фаза, т. е.

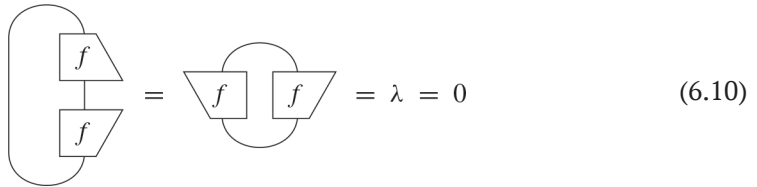
$$\frac{\mu}{\lambda} = e^{i\alpha}$$

для некоторого α , и

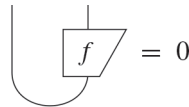


поэтому действительно имеет место равенство $f = e^{i\alpha}g$.

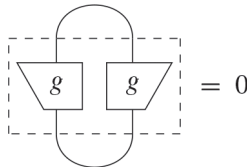
Во втором случае



Значит, в силу положительной определенности (см. раздел 5.3.2)



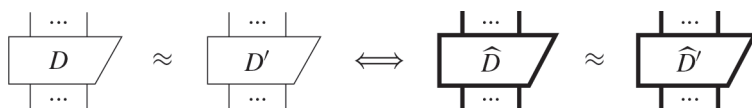
поэтому $f = 0$, а следовательно, $\hat{f} = 0$, и, стало быть, по предположению, $\hat{g} = 0$. Так может быть только тогда, когда сам g равен нулю. Чтобы убедиться в этом, присоединим чашку и крышку к \hat{g} :



и, воспользовавшись положительной определенностью, как и в (6.10), получаем $g = 0$. Поэтому $f = e^{i\alpha}g = 0$, где угол α может быть любым. □

Разумеется, если в теореме 6.17 заменить точное равенство равенством с точностью до числа (см. раздел 3.4.3), то фаза исчезнет.

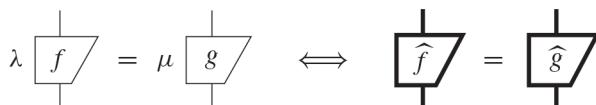
Следствие 6.18. Для диаграмм D и \widehat{D} в теории линейных отображений:



Замечание 6.19. Помимо собственно утверждения теоремы 6.17, из этого доказательства можно извлечь еще один поучительный урок. Основная идея доказательства чисто диаграммная! В частности, числа λ и μ определены в виде диаграмм:



и с помощью диаграммных подстановок мы показали, что

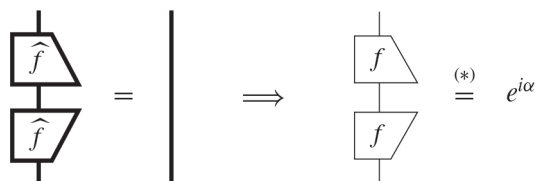


где $\lambda\bar{\lambda} = \mu\bar{\mu}$, а единственное место, где использовалась специфика структуры **линейных отображений**, а именно комплексные числа, – преобразование этого равенства в форму, содержащую $e^{i\alpha}$, для чего также требуется различать регистр. Но и этого можно избежать (см. ссылки в разделе 6.7). Отсюда следует, что не только для **линейных отображений**, но и для любой другой процессной теории дублирование идентифицирует в точности те процессы, которые различаются только этими «обобщенными глобальными фразами». Урок такой: не судите о книге по обложке – то, что на первый взгляд вовсе не выглядит как диаграмма (например, устранение глобальных фаз), на поверку может оказаться фундаментально диаграммным.

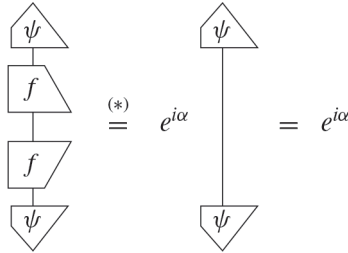
Теперь мы покажем, что ряд свойств «одинокных» и дублированных процессов совпадает.

Предложение 6.20. Чистое квантовое отображение \widehat{f} является изометрией (унитарным процессом) тогда и только тогда, когда f является изометрией (унитарным процессом).

Доказательство. Если f – изометрия, то \widehat{f} – изометрия в силу следствия 6.16. Обратное, мы можем воспользоваться теоремой 6.17, чтобы преобразовать дублированные равенства в одиночные с точностью до фазы:



Это означает, что если \widehat{f} – изометрия, то f – изометрия с точностью до глобальной фазы $e^{i\alpha}$. Далее можно показать, что $\alpha = 0$. Во-первых, для любого нормированного состояния ψ имеем:

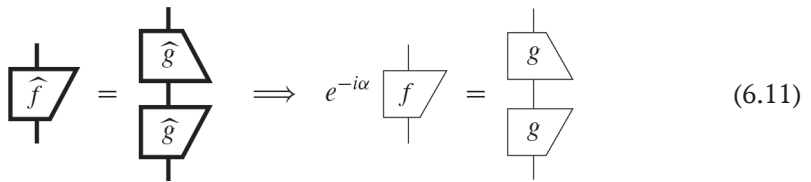


Левая часть этого равенства – внутреннее произведение состояния с самим собой, поэтому оно должно быть положительно. Поскольку единственная глобальная фаза, являющаяся положительным вещественным числом, – это 1, то $e^{i\alpha} = 1$, так что f – изометрия. Унитарность доказывается аналогично. □

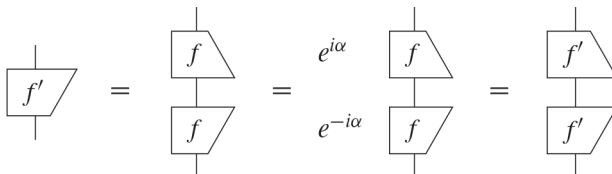
Далее мы докажем результат, аналогичный предложению 6.20 для положительных отображений и проекторов, но с одной небольшой оговоркой. Если f – изометрия или унитарный процесс, то $e^{i\alpha}f$ – тоже изометрия или унитарный процесс, поэтому мы можем выбрать произвольного «недублированного представителя» \widehat{f} . Однако для положительных процессов и проекторов это не так – для получения желаемого свойства нужно выбирать конкретного представителя.

Предложение 6.21. Чистое квантовое отображение \widehat{f} положительно (соответственно, является проектором) тогда и только тогда, когда существует положительное линейное отображение (соответственно, проектор) f' , для которого $\widehat{f'} = \widehat{f}$.

Доказательство. Опять-таки, в одну сторону утверждение вытекает из следствия 6.16. Для доказательства обратного предположим, что \widehat{f} положительно, и применим теорему 6.17 (перенеся глобальную фазу в левую часть):



Отсюда видно, что $f' := e^{-i\alpha}f$ положительно. Поскольку дублирование устраняет глобальные фазы, $\widehat{f'} = \widehat{f}$. Если f – проектор, то (6.11) справедливо для $g := f$ (см. предложение 4.70). Поэтому f' также является проектором:



□

Следующее упражнение – еще одна вариация на ту же тему.

Упражнение 6.22. Покажите, что чистое квантовое состояние $\widehat{\psi}$ нормированно тогда и только тогда, когда ψ нормированно, и что два чистых квантовых состояния $\widehat{\psi}$ и $\widehat{\phi}$ ортогональны тогда и только тогда, когда ψ и ϕ ортогональны.

Из всех приведенных выше результатов следует, что мы (в большинстве случаев) можем работать с чистыми квантовыми отображениями, как с обычными линейными отображениями, но с тем дополнительным преимуществом, что правило Борна просто выражает связь между состоянием и эффектом и что избыточные глобальные фазы устранены.

Конечно, есть и исключения, иначе вообще не было бы смысла все дублировать.

6.1.5. Что не сохраняется при дублировании

В определении **линейных отображений** входило три требования:

- числами являются комплексные числа;
- для процессов определены суммы;
- для каждого типа существует ОНБ.

Сейчас мы увидим, что при дублировании ни одно из этих свойств не сохраняется! Точнее:

- дублированные числа не являются комплексными числами;
- суммы в дублированной теории не являются дублированными суммами;
- результат дублирования ОНБ не является ОНБ в дублированной теории.

Однако то, что мы получаем взамен, играет ключевую роль в квантовой теории.

6.1.5.1. Дублированные числа являются вероятностями

Собственно, именно для этого мы и вводили дублирование.

Предложение 6.23. Числами в теории **чистых квантовых отображений** являются положительные вещественные числа.

Доказательство. Это следует из предложения 5.70, характеризующего положительные числа:

$$p = \diamond \mu = \widehat{\mu} = \mu$$

В частности, любое положительное число является чистым квантовым отображением. □

6.1.5.2. Суммы в дублированной теории представляют «смешивание»

Сумма дублированных процессов

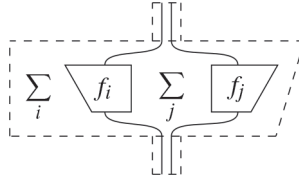
$$\sum_i \widehat{f}_i$$

в общем случае не является дублем суммы процессов:

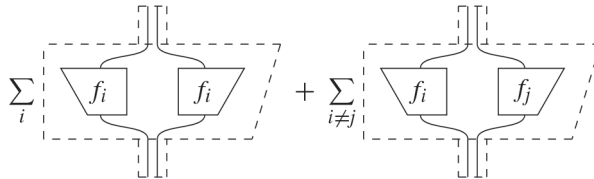
$$\text{double} \left(\sum_i f_i \right)$$

На самом деле нетривиальные суммы дублированных отображений не являются даже **чистыми квантовыми отображениями**, поэтому их вообще нельзя получить путем дублирования.

Все дело в том, что раскрытие операции дублирования дает два независимых суммирования (по разным индексам):



Эту сумму можно разбить на части, где $i = j$ и $i \neq j$:



Таким образом, левая часть равна правой плюс «внедиагональные» члены:

$$\text{double} \left(\sum_i \left[\begin{array}{c} | \\ \hline f_i \\ \hline | \end{array} \right] \right) = \sum_i \left[\begin{array}{c} | \\ \hline \hat{f}_i \\ \hline | \end{array} \right] + \sum_{i \neq j} \left[\begin{array}{c} | \\ \hline f_i \quad f_j \\ \hline | \end{array} \right]$$

Эти внедиагональные члены в общем случае не обращаются в ноль, что видно уже на примере чисел. Полагая $\lambda_0 = \lambda_1 = 1$, получаем:

$$\text{double} \left(\sum_i \diamond \lambda_i \right) = \text{double}(1 + 1) = 4 \neq 2 = 1 + 1 = \sum_i \diamond \lambda_i$$

Это не ошибка, а особенность. Суммирование чистых квантовых отображений играет концептуально важную роль, не имеющую аналога в теории линейных отображений. Ему можно придать ясную физическую интерпретацию – введение неопределенности относительно того, какой процесс имел место. Это называется «смешиванием» и будет подробно обсуждаться в разделе 6.2.7.

Другой вид суммирования, а именно производимого в теории **линейных отображений** до дублирования, приводит к *квантовой суперпозиции*, которую мы будем обсуждать в разделе 7.1.2. Таким образом, мы имеем два вида сумм с различной семантикой.

С другой стороны, тот факт, что дублирование не сохраняет суммы, подтверждает то, на что мы уже указывали в замечании 5.34: суммам не место в диаграммных рассуждениях, поскольку они легко приводят к ошибкам. Поэтому стоит по

возможности избегать их. В следующих двух главах многие концепции, которые первоначально были сформулированы с помощью сумм, будут заменены чисто диаграммными аналогами.

6.1.5.3. Эффекты дублированного ОНБ – «квантовые измерения»

Если ОНБ в теории линейных отображений

$$\mathcal{B} = \left\{ \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \right\}_i$$

содержит, по крайней мере, два состояния, то

$$\text{double}(\mathcal{B}) := \left\{ \begin{array}{c} \downarrow \\ \triangle \\ i \\ \downarrow \\ \triangle \\ i \end{array} \right\}_i$$

не является базисом в теории **чистых квантовых отображений**. Чтобы убедиться в этом, рассмотрим два состояния:

$$\begin{array}{c} \downarrow \\ \triangle \\ \psi \end{array} := \sum_j \begin{array}{c} \downarrow \\ \triangle \\ j \end{array} \quad \begin{array}{c} \downarrow \\ \triangle \\ \phi \end{array} := \sum_j e^{i\alpha_j} \begin{array}{c} \downarrow \\ \triangle \\ j \end{array}$$

где все α_j различны. Поскольку ϕ содержит, по крайней мере, два члена с разными коэффициентами $e^{i\alpha_j}$, то ψ и ϕ не равны с точностью до глобальной фазы, т. е.

$$\begin{array}{c} \downarrow \\ \triangle \\ \psi \end{array} \neq \begin{array}{c} \downarrow \\ \triangle \\ \phi \end{array}$$

Однако легко проверить, что для всех i :

$$\begin{array}{c} \triangle \\ i \\ \downarrow \\ \triangle \\ \psi \end{array} = \begin{array}{c} \triangle \\ i \\ \downarrow \\ \triangle \\ \phi \end{array}$$

Поэтому $\text{double}(\mathcal{B})$ не может быть базисом.

Причина, по которой $\text{double}(\mathcal{B})$ не является базисом в теории **чистых квантовых отображений**, заключается в том, что он теряет всю информацию о «локальных» фазах (т. е. числах $e^{i\alpha_j}$ выше) из ϕ , которая (в отличие от глобальных фаз) весьма и весьма существенна для квантового состояния $\hat{\phi}$. У этого факта есть важное физическое следствие – *квантовые измерения* могут дать лишь часть информации о состоянии системы. В следующей главе мы определим квантовые измерения и покажем, что измерения, определенные в терминах эффектов ОНБ, – на самом деле лучшее, что можно сделать (хотя все равно плоховато!) в части извлечения информации из одного квантового состояния.

В этот момент у вас, наверное, возник вопрос, а есть ли вообще базисы в теории **чистых квантовых состояний**. Теорема 5.14 показывает, что базисы позволяют

полностью охарактеризовать процессы с помощью конечного множества чисел (матрицы процесса). Это основа *квантовой томографии*, которая, как мы увидим в следующей главе, занимается идентификацией состояния или процесса посредством квантовых измерений. И это возможно, только если базисы существуют. К счастью, так оно и есть.

Теорема 6.24. Для любого ОНБ

$$\mathcal{B} = \left\{ \left\langle \begin{array}{c} | \\ \hline j \\ \hline \end{array} \right\rangle_j \right\}$$

в гильбертовом пространстве A множество состояний $\text{double}(\mathcal{B})$ можно продолжить до (неортогонального) базиса в теории **линейных отображений** для типа $A \otimes A$, который будет целиком состоять из чистых квантовых состояний. И он является базисом в теории **чистых квантовых отображений** для дублированного системного типа \hat{A} .

Доказательство. Существует много способов продолжить базис на чистые состояния. Например, пусть \mathcal{A} – множество всех состояний вида

$$\left\langle \begin{array}{c} | \\ \hline \psi_{jk} \\ \hline \end{array} \right\rangle := \begin{cases} \frac{1}{2} \left(\left\langle \begin{array}{c} | \\ \hline j \\ \hline \end{array} \right\rangle + \left\langle \begin{array}{c} | \\ \hline k \\ \hline \end{array} \right\rangle \right) & \text{если } j \leq k \\ \frac{1}{2} \left(\left\langle \begin{array}{c} | \\ \hline j \\ \hline \end{array} \right\rangle + i \left\langle \begin{array}{c} | \\ \hline k \\ \hline \end{array} \right\rangle \right) & \text{если } j > k \end{cases}$$

Тогда каждое базисное состояние $j \in \mathcal{B}$ имеет вид ψ_{jj} , поэтому $\mathcal{B} \subseteq \mathcal{A}$. Чтобы показать, что

$$\text{double}(\mathcal{A}) = \left\{ \left\langle \begin{array}{c} | \\ \hline \psi_{jk} \\ \hline \end{array} \right\rangle \left\langle \begin{array}{c} | \\ \hline \psi_{jk} \\ \hline \end{array} \right\rangle \right\}_{jk}$$

является базисом $A \otimes A$, достаточно показать, что любой элемент базиса произведения

$$\left\{ \left\langle \begin{array}{c} | \\ \hline j \\ \hline \end{array} \right\rangle \left\langle \begin{array}{c} | \\ \hline k \\ \hline \end{array} \right\rangle \right\}_{jk} \tag{6.12}$$

можно получить как сумму состояний вида $\lambda \psi_{jk}$ для $\lambda \in \mathbb{C}$. Оставляем это в качестве упражнения для читателя.

Итак, мы все же можем различить процессы по тому, как они воздействуют на состояния, но это далеко не так просто, как было раньше! В частности, не существует никакого способа построить ОНБ из чистых квантовых состояний.

Соглашение 6.25. Из теоремы 6.24 следует, что «размерность» (в смысле определения 5.2) квантовой системы \hat{A} равна D^2 , где D – размерность A , но, говоря о размерности квантовой системы, мы всегда имеем в виду размерность недубли-

В этом разделе мы целиком сфокусируемся на отбрасывании, рассмотрим его поведение и покажем, что это поведение заставляет нас сделать конкретный выбор. Начнем с осознания следующего факта.

6.2.1.1. Отбрасывание – не чистое квантовое отображение

Чтобы убедиться в этом, достаточно посмотреть, как процесс отбрасывания должен вести себя на состоянии одной системы. Отбрасывание не должно делать ничего, кроме удаления этого состояния с картинки:

$$\begin{array}{c} \triangle \\ \text{?} \\ \downarrow \\ \nabla \\ \psi \end{array} = \square$$

или по-другому: это испытание, которое гарантированно завершается успешно, но ничего не говорит о самом состоянии. В частности, процесс отбрасывания не может зависеть от состояния системы, которое отбрасывается.

Предложение 6.27. Для нетривиального гильбертова пространства, т. е. пространства размерности > 1 , не существует чистого квантового эффекта $\hat{\phi}$ такого, что для всех нормированных чистых квантовых состояний $\hat{\psi}$ имеет место равенство

$$\begin{array}{c} \triangle \\ \hat{\phi} \\ \downarrow \\ \nabla \\ \hat{\psi} \end{array} = \square \tag{6.13}$$

Доказательство. Предположим, что $\hat{\phi}$ – чистый эффект отбрасывания. Очевидно, что $\hat{\phi}$ не может быть нулевым. Поэтому должно существовать такое λ , что $\lambda\hat{\phi}$ нормирован. По теореме 5.79, $\lambda\hat{\phi}$ продолжается до некоторого ОНБ. Поскольку размерность пространства не меньше 2, в этом ОНБ существует отличное от $\hat{\phi}$ состояние, которое мы обозначим $\hat{\phi}'$. Оно должно быть ортогонально $\lambda\hat{\phi}$, а значит, также и $\hat{\phi}$. Следовательно,

$$\begin{array}{c} \triangle \\ \phi \\ \downarrow \\ \nabla \\ \phi' \end{array} = 0$$

и потому

$$\begin{array}{c} \triangle \\ \hat{\phi} \\ \downarrow \\ \nabla \\ \hat{\phi}' \end{array} = 0 \neq \square$$

Мы пришли к противоречию. □

Замечание 6.28. В разделе 4.3.3 мы привели убедительную причину рассматривать по умолчанию нормированные состояния, а именно тот факт, что это

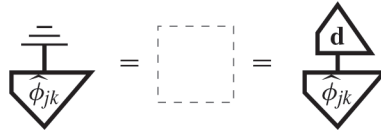
6.2.1.2. Нашим целям отвечает только одно линейное отображение

Теорема 6.31. Отображение отбрасывания из определения 6.29 – это единственное линейное отображение, которое переводит все нормированные чистые квантовые состояния в 1.

Доказательство. Предположим, что существует еще какой-то эффект:



который переводит все нормированные чистые квантовые состояния в 1. Из теоремы 6.24 мы знаем, что существует базис $\text{double}(B')$, состоящий из чистых квантовых состояний для типа $A \otimes A$ в теории **линейных отображений**. Обозначим $\text{double}(B'')$ базис, получающийся путем нормировки всех состояний в $\text{double}(B')$ (после чего он, конечно, не перестает быть базисом). Тогда для любого $\hat{\phi}_{jk} \in \text{double}(B'')$



Поскольку \mathbf{d} и отбрасывание совпадают на этом базисе, они равны. Следовательно, эффект отбрасывания единственный. \square

Теперь, зная, что отбрасывание однозначно определено своим поведением, мы можем сделать выводы о том, что это такое в отдельных частных случаях.

Упражнение 6.32. Покажите, что

$$\hat{H}_1 \otimes \dots \otimes \hat{H}_n \text{ (with bars) } := \hat{H}_1 \text{ (with bars) } \hat{H}_2 \text{ (with bars) } \dots \hat{H}_n \text{ (with bars)} \quad (6.16)$$

и

$$\hat{\mathbb{C}} \text{ (with bars) } := \text{ (dashed box) } \quad (6.17)$$

(заметим, что $\hat{\mathbb{C}}$ – система «без проводов» в теории **чистых квантовых отображений**).

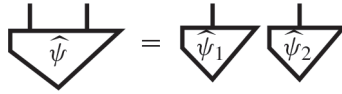
6.2.1.3. Отбрасывание не сохраняет чистые квантовые состояния

Если начать с чистого квантового состояния двух систем и отбросить одну систему, то получившееся состояние необязательно будет чистым квантовым. На самом деле есть только один случай, когда это так: если исходное состояние \otimes -разделимо.

Предложение 6.33. Для любого квантового состояния $\hat{\psi}$ редуцированное состояние:



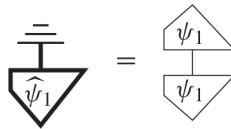
является чистым тогда и только тогда, когда $\hat{\psi} \otimes$ -разделимо:



Доказательство. В направлении \Leftarrow имеем:



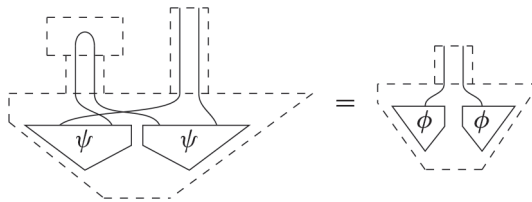
При доказательстве предложения 6.30 мы уже видели, что



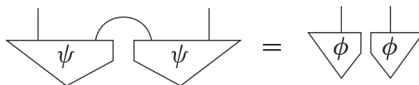
а это положительное число. Поскольку любое положительное число – чистое состояние (см. предложение 6.23), квантовое состояние (6.18) является чистым. Чтобы доказать утверждение в направлении \Rightarrow , предположим, что существует чистое состояние $\hat{\phi}$ такое, что



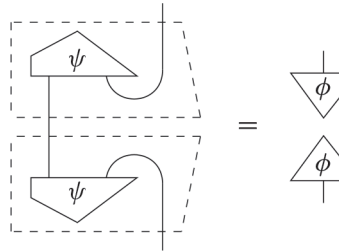
Мы воспользуемся предложением 5.74, которое утверждает, что процесс $f^\dagger \circ f$ разделим тогда и только тогда, когда разделим f . Раскрывая дублированные отображения в (6.19)



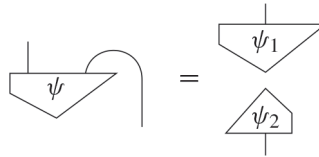
получаем



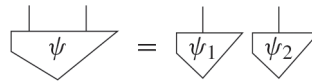
В силу двойственности процессов и состояний мы, применив транспонирование, получаем:



Тогда, в силу предложения 5.74, существуют ψ_1 и ψ_2 такие, что:



(Заметим, что изображение эффекта ψ_2 в сопряженной форме не ограничивает общность.) И снова воспользовавшись двойственностью процессов и состояний, получаем, что ψ \otimes -разделим:

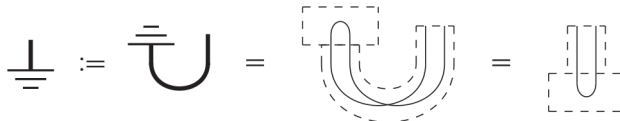


Дублирование этого равенства доказывает требуемое утверждение. □

Поскольку редуцированные состояния в общем случае не являются чистыми квантовыми состояниями, мы должны ввести более общее семейство состояний, чтобы учесть возможность отбрасывания частей системы.

6.2.2. Нечистота

При образовании композиции произвольных чистых квантовых отображений с отображением отбрасывания открывается много нового. Например, рассмотрим транспонирование (или, эквивалентно, адьюнкцию) отображения отбрасывания:



Это состояние настолько важно, что его нормированный вариант получил специальное название.

Определение 6.34. Максимально смешанным состоянием называется

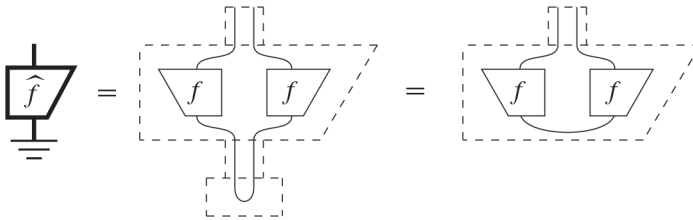
$$\frac{1}{D} \underline{\underline{\perp}}$$

Это максимально смешанное состояние – пример редуцированного состояния (см. предложение 6.33), а именно того, что остается после отбрасывания половины состояния Белла:

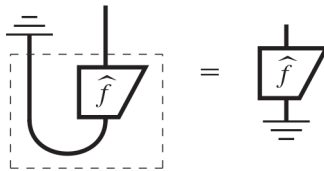
$$\frac{1}{D} \underline{\underline{=}} = \boxed{\frac{1}{D} \cup}$$

Как мы уже говорили во введении, термин «смешанное» связан с недостатком знаний о фактическом состоянии системы. В разделе 6.2.7 мы увидим, что максимально смешанное состояние означает, что у нас нет вообще никакой информации о состоянии системы.

Теперь мы можем генерировать и другие новые состояния, либо применяя чистое квантовое отображение к системе, находящейся в максимально смешанном состоянии:



либо, что эквивалентно, отбрасывая одну систему двухкомпонентного чистого состояния (которое здесь представлено, исходя из двойственности процессов и состояний):

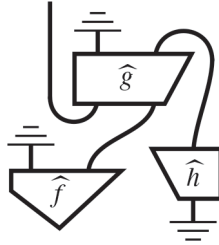


Получающаяся форма, ко всему прочему, является общей.

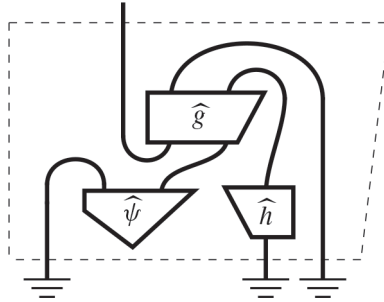
Теорема 6.35. Любое состояние, получающееся композицией чистых квантовых отображений и отбрасывания, является *квантовым состоянием*, т. е. состоянием вида

$$\downarrow \rho := \boxed{\cup} \quad (6.20)$$

Доказательство. Для диаграммы, состоящей из каких-то чистых квантовых отображений и отбрасывания:



мы всегда можем опустить все отображения отбрасывания (или максимально смешанные состояния) вниз, используя при необходимости крышки:



Затем мы можем объединить все максимально смешанные состояния в одно (см. перевернутое равенство (6.16)). Таким образом, мы получаем чистое квантовое отображение, примененное к максимально смешанному состоянию. □

Вспоминая определение \otimes -положительности из раздела 4.3.6, получаем

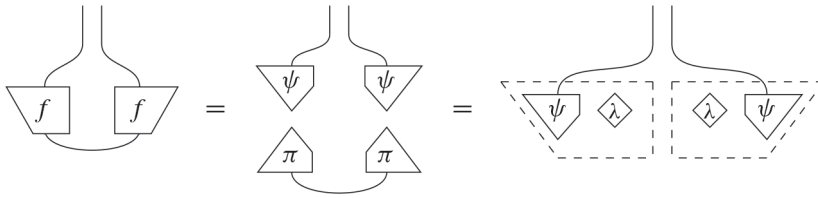
Следствие 6.36. Квантовые состояния – это \otimes -положительные состояния в теории линейных отображений.

Форма квантовых состояний является обобщением формы чистых квантовых состояний, для которых отображение f в (6.20) имеет тривиальный входной провод. В частности, не все квантовые состояния являются чистыми. Те состояния, которые не являются чистыми, называются *нечистыми*. Если раскрыть форму нечистого квантового состояния ρ и чистого квантового состояния $\hat{\psi}$, то различие сводится к наличию провода, соединяющего левую половину с правой:



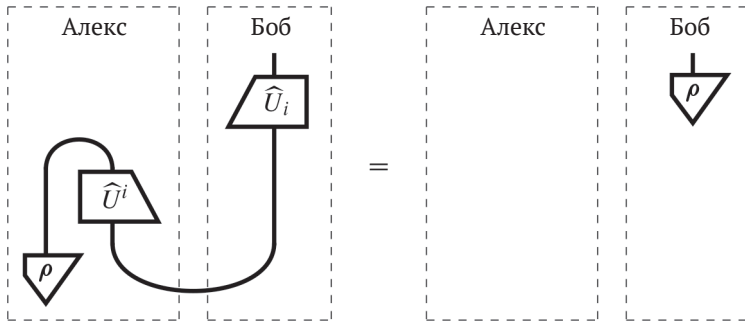
Таким образом, само понятие *чистоты* является диаграммным.

Замечание 6.37. Отметим, что мы должны принять отсутствие провода как доказательство чистоты. С другой стороны, наличие провода лишь свидетельствует о возможности нечистоты. Например, предположим, что сам процесс f несвязный:

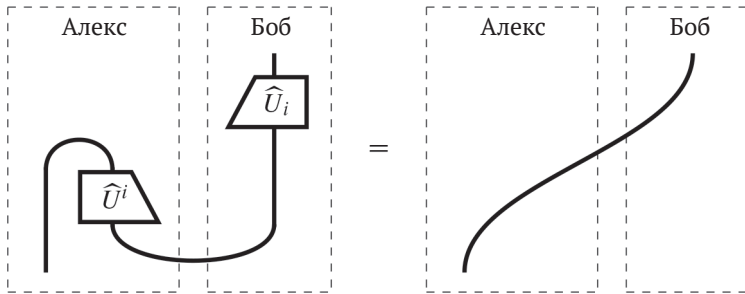


где $\lambda := \sqrt{\pi^\dagger \circ \pi}$. Тогда результирующее состояние чистое.

Пример 6.38. В квантовой телепортации не имеет значения, является ли телепортируемое состояние нечистым, поскольку картинка от этого не зависит:



Хотя это обобщение в строгом смысле, причина, по которой никакой дополнительной работы не требуется, – композиционная природа струнных диаграмм. Ключом к пониманию справедливости приведенного выше равенства является тот факт, что



А раз так, то, очевидно, не важно, подаем мы на вход $\hat{\psi}$ или ρ .

6.2.3. Вес и причинность для квантовых состояний

Внимательный читатель, возможно, обратил внимание на одну тонкость в определении 6.34, а именно что максимально смешанное состояние не является нормированным в смысле определения 4.48:

$$\begin{array}{|c|} \hline \frac{1}{D} \\ \hline \text{---} \\ \hline \text{---} \\ \hline \frac{1}{D} \\ \hline \end{array} = \frac{1}{D^2} \begin{array}{|c|} \hline \text{---} \\ \hline \text{---} \\ \hline \end{array} = \frac{1}{D} \tag{6.21}$$

поскольку кружочек равен размерности D , как мы видели в следствии 5.33. С другой стороны, если отбросить максимально смешанное состояние, то мы таки получим:

$$\begin{array}{|c|} \hline \text{---} \\ \hline \text{---} \\ \hline \frac{1}{D} \\ \hline \end{array} = \begin{array}{|c|} \hline \text{---} \\ \hline \end{array}$$

Таким образом, в отличие от случая чистых квантовых состояний, для которого мы в предложении 6.30 показали, что квадрат нормы и число, возникающее в результате отбрасывания, совпадают, для максимально смешанного состояния это уже не так, и, более того, это вообще неверно для нечистых квантовых состояний. Поэтому оправдано введение нового названия для чисел, получаемых при отбрасывании.

Определение 6.39. *Весом* квантового состояния ρ называется



а состояние ρ называется *каузальным*, если его вес равен 1, т. е.

$$\begin{array}{|c|} \hline \text{---} \\ \hline \text{---} \\ \hline \rho \\ \hline \end{array} = \begin{array}{|c|} \hline \text{---} \\ \hline \end{array} \tag{6.22}$$

Как нам следует интерпретировать эту величину? Правило Борна гласит:

$$\left. \begin{array}{l} \text{эффект} \\ \text{состояние} \end{array} \right\} \begin{array}{|c|} \hline \text{---} \\ \hline \text{---} \\ \hline \rho \\ \hline \end{array} \left. \vphantom{\begin{array}{l} \text{эффект} \\ \text{состояние} \end{array}} \right\} \text{вероятность}$$

Следовательно, вес – это результат выполнения тривиального испытания состояния (т. е. «является ли это состоянием?»). Обычно мы ожидаем, что это испытание возвращает утвердительный ответ с вероятностью 1. Однако ниже в этой главе мы увидим, что состояние может быть результатом недетерминированного процесса. В таком случае вес говорит, какова вероятность оказаться в этом состоянии. И тогда каузальные состояния – это те, которые имеют место наверняка. Иными словами, то, что мы называем квантовым состоянием, на самом деле является комбинацией двух вещей:

$$\begin{array}{c} \downarrow \\ \rho' \end{array} = p \begin{array}{c} \downarrow \\ \rho \end{array}$$

– «фактического» состояния системы (каузального состояния ρ) и вероятности p его возникновения (т. е. веса ρ'). Мы продолжим это обсуждение в разделе 6.4.1, после того как надлежащим образом определим недетерминированные квантовые процессы.

Если временно забыть про недетерминированность, то единственными «настоящими» состояниями будут каузальные. Поэтому фундаментальная интерпретация принципа причинности звучит следующим образом:

*если состояние отброшено,
то можно считать, что его никогда не существовало.*

Очевидно, что это разумное и, более того, необходимое предположение. Существует много систем (например, на Марсе), которые мы не контролируем и о которых ничего не знаем. Поэтому мы игнорируем (отбрасываем) их в своих вычислениях. Если бы это было запрещено, то ни о какой науке не было бы и речи. Тут есть и отголосок теории относительности: если нечто находится достаточно далеко (т. е. «разделено пространственно-подобным интервалом» на жаргоне теории относительности), то оно не должно оказывать влияния на происходящее локально, поскольку свет не может двигаться с достаточно большой для этого скоростью. Эта особенность, называемая «невозможностью подачи сигнала», или «несигнальностью» (non-signalling), – фундаментальная черта теории относительности. В разделе 6.3 мы увидим, что невозможность подачи сигнала и причинность тесно связаны.

На состояния каузальность налагает довольно слабое ограничение: вес должен быть равен 1. Следовательно, любое ненулевое состояние можно превратить в каузальное, просто образовав его композицию с подходящим числом. Однако в разделе 6.2.6 мы увидим, что для произвольных процессов это ограничение более серьезное, и, как будет показано в теореме 6.54, для эффектов оно прямо-таки экстремальное!

Для чистых состояний мы уже знаем, что нормированность и каузальность совпадают. Вообще, имеет место

Предложение 6.40. Для любого чистого состояния $\hat{\psi}$

$$\begin{array}{c} \hat{\psi} \\ \downarrow \\ \hat{\psi} \end{array} = \left(\begin{array}{c} \bar{\bar{\psi}} \\ \downarrow \\ \hat{\psi} \end{array} \right)^2$$

Доказательство. В этом можно убедиться, сначала раскрыв диаграмму, а затем транспонировав эффекты:

$$\begin{array}{c} \hat{\psi} \\ \downarrow \\ \hat{\psi} \end{array} = \begin{array}{c} \psi \quad \psi \\ \downarrow \quad \downarrow \\ \psi \quad \psi \end{array} = \begin{array}{c} \psi \quad \psi \\ \downarrow \quad \downarrow \\ \psi \quad \psi \end{array} = \begin{array}{c} \bar{\bar{\psi}} \quad \bar{\bar{\psi}} \\ \downarrow \quad \downarrow \\ \hat{\psi} \quad \hat{\psi} \end{array}$$

□

Тогда тот факт, что нормированность и каузальность совпадают для чистых состояний, – это просто частный случай, когда и квадрат нормы, и (возведенный в квадрат) вес равны 1.

Пример 6.41. Так как окружность равна D , состояние Белла является каузальным:

$$\frac{1}{D} \text{ (Bell state diagram) } = \frac{1}{D} \text{ (Bell state diagram) } = \text{ (empty dashed box) }$$

Учитывая, что состояние Белла еще и чистое, оно также нормированное:

$$\frac{1}{D} \text{ (Bell state diagram) } = \frac{1}{D^2} \text{ (Bell state diagram) } = \text{ (empty dashed box) }$$

Однако, как мы видели в (6.21), квадрат нормы может быть меньше квадрата веса для нечистых состояний. Тот факт, что эти две величины не всегда совпадают, на самом деле полезен, поскольку дает эффективный способ определить, является ли состояние чистым.

Предложение 6.42. Для любого квантового состояния ρ имеет место неравенство

$$\left(\text{Diagram of } \rho \right)^2 \leq \left(\text{Diagram of } \rho \right)^2 \tag{6.23}$$

причем равенство достигается тогда и только тогда, когда ρ чистое.

Доказательство. Поскольку ρ – \otimes -положительное состояние, в силу спектральной теоремы (и конкретно следствия 5.72) существует ОНБ и положительные числа r_i такие, что

$$\text{Diagram of } \rho := \sum_i r_i \text{ (Diagram of } i \text{)} \text{ (Diagram of } i \text{)}$$

Тогда не составляет труда вычислить квадрат нормы и вес:

$$\left(\text{Diagram of } \rho \right)^2 = \sum_{ij} r_i r_j \text{ (Diagram of } j \text{)} \text{ (Diagram of } i \text{)} = \sum_i r_i^2$$

$$\text{Diagram of } \rho = \sum_i r_i \text{ (Diagram of } i \text{)} \text{ (Diagram of } i \text{)} = \sum_i r_i$$

Таким образом,

$$\left(\overline{\overline{\rho}} \right)^2 = \left(\sum_i r_i \right)^2 = \sum_i r_i^2 + \sum_{i \neq j} r_i r_j$$

Из того, что все произведения $r_i r_j \geq 0$, следует первая часть утверждения. Если состояние ρ чистое, то, по предложению 6.21, квадрат нормы и квадрат веса совпадают. Обратное, предположим, что квадрат нормы и квадрат веса равны. Тогда

$$\sum_{i \neq j} r_i r_j = 0$$

а это может быть только тогда, когда для всех $i \neq j$ имеем $r_i r_j = 0$. В таком случае не более одного r_i может быть отличным от нуля, так что

$$\downarrow \rho = r_i \downarrow i \downarrow i$$

т. е. является чистым квантовым состоянием. □

Предложение 6.42 – это не просто средство обнаружения чистых состояний. По мере того как каузальное состояние становится все более и более нечистым, квадрат нормы уменьшается, до тех пор пока не достигнет $1/D$ для максимально смешанного состояния. Таким образом, эта величина фактически измеряет степень нечистоты состояния. Мы изучим эту и другие меры нечистоты в разделе 13.2.

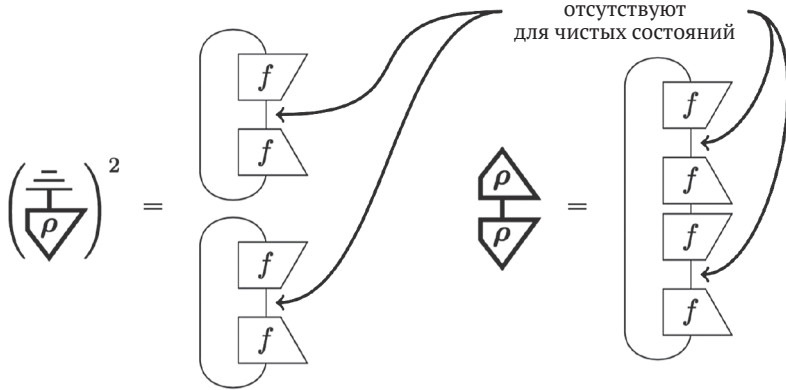
Можно также наглядно представить разность между величинами в (6.23). Для веса имеем:

(6.24)

а для квадрата нормы:

(6.25)

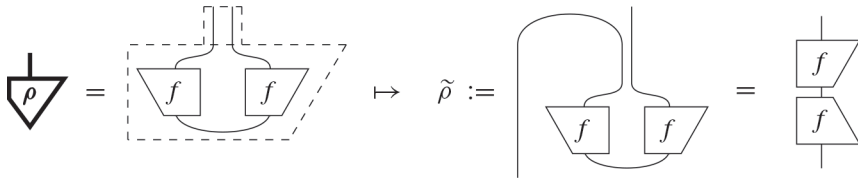
В случае чистого состояния причиной совпадения квадрата нормы и квадрата веса является отсутствие следующих проводов:



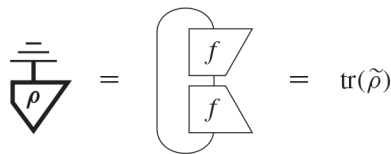
В противном случае различие чисел обусловлено различиями в проводных соединениях.

Замечание 6.43. В замечании 6.5 была отмечена возможность перейти от чистого состояния к его представлению в виде оператора плотности, который в том контексте являлся проектором. Это обобщается на (каузальные) смешанные состояния, для которых ассоциированный оператор плотности – положительное отображение со следом 1.

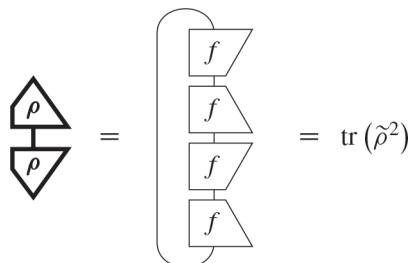
Переход между нашим дублированным представлением и представлением в виде оператора плотности возможен в силу двойственности процессов и состояний:



Для представления в виде оператора плотности из (6.24) следует, что отбрасывание состояния означает взятие его следа:



поэтому оператор плотности со следом 1 соответствует каузальному состоянию. Аналогично из (6.25) следует, что



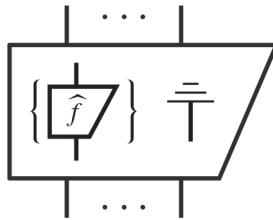
поэтому (6.23) в терминах операторов плотности принимает вид:

$$\text{tr}(\tilde{\rho}^2) \leq (\text{tr}(\tilde{\rho}))^2.$$

6.2.4. Процессная теория квантовых отображений

Мы перешли от чистых квантовых состояний к квантовым состояниям, добавив отбрасывание. На самом деле таким образом можно получить всю процессную теорию квантовых отображений.

Определение 6.44. В процессной теории **квантовых отображений** типами являются дублированные гильбертовы пространства \hat{A} , а процессами – все диаграммы, составленные из чистых квантовых отображений и отбрасывания:



Поэтому не должна вызывать удивления следующая

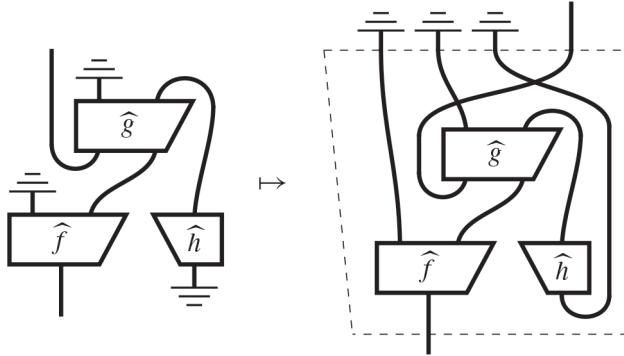
Теорема 6.45. Теория **квантовых отображений** допускает струнные диаграммы.

Доказательство. **Квантовые отображения** наследуют чашки и крышки от чистых квантовых отображений, поэтому достаточно показать, что у квантовых отображений есть адьюнкты. Адьюнктом чистого квантового отображения является другое чистое квантовое отображение, а адьюнктом отбрасывания – просто транспонированное к нему отображение:

$$\left(\overline{\overline{\top}}\right)^\dagger = \overline{\overline{\cup}}$$

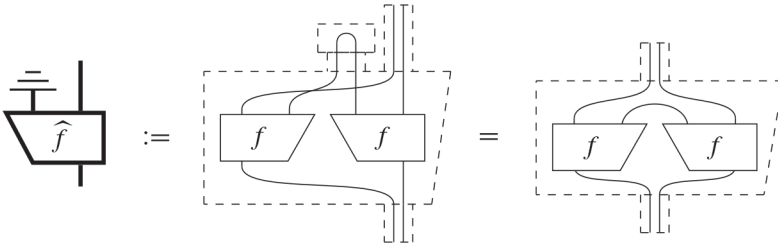
которое является композицией чистого квантового отображения (чашки) с отбрасыванием. Поэтому оно само является квантовым отображением. Поскольку адьюнкция должна сохранять диаграммы, а все диаграммы в теории **квантовых отображений** включают только чистые квантовые отображения и отбрасывание, то у каждого квантового отображения есть адьюнкт. \square

Как и квантовые состояния (см. предыдущий раздел), любое квантовое отображение можно привести к «нормальной форме», сгруппировав все отображения отбрасывания в один эффект:



Таким образом, справедливо следующее

Предложение 6.46. Все квантовые отображения имеют вид:



для некоторого линейного отображения f .

Итак, квантовые отображения – это в точности те линейные отображения, которые являются \otimes -положительными процессами (см. определение 4.66). Предложение 6.46 также показывает, что любое квантовое отображение возникает в результате игнорирования части выхода некоторого процесса. Иными словами, для любого квантового отображения Φ должно существовать чистое квантовое отображение \hat{f} такое, что

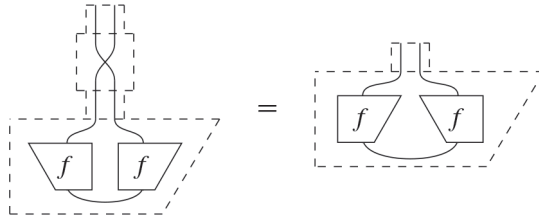
$$\Phi = \text{[Diagram of } \hat{f} \text{ gate]} \quad (6.26)$$

Определение 6.47. Чистое квантовое отображение \hat{f} в равенстве (6.26) называется *очищением* квантового отображения Φ .

Соблазнительна мысль о том, что квантовые отображения – это в точности те отображения, которые переводят квантовые состояния в квантовые состояния, но это не так. Например, линейное отображение перекоммутации, рассматриваемое как линейное отображение из типа \bar{A} в тип \bar{A} :

$$\text{[Diagram of a swap operation]} \quad (6.27)$$

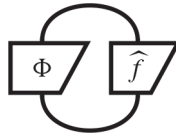
очевидно, переводит квантовые состояния в квантовые состояния:



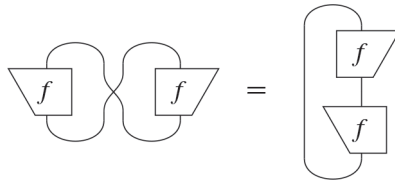
(на самом деле оно переводит состояние в сопряженное к нему!) Однако...

Предложение 6.48. Линейное отображение (6.27) не является квантовым отображением.

Доказательство. Для любого квантового отображения Φ и любого линейного отображения f число



также является квантовым отображением, а именно положительным числом. Однако если вместо Φ взять отображение (6.27), то получим:



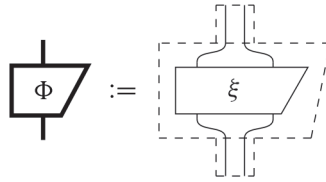
Это число не является композицией линейного отображения и его адьюнкта, поэтому оно не может быть положительно для всех f . И действительно, выбор

$$\begin{array}{c} | \\ \hline f \\ \hline | \end{array} \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

дает -2 , т. е. мы пришли к противоречию. □

Утверждение «отображение является квантовым» сильнее, чем «отображение сохраняет состояния одной системы». Причина в том, что квантовые отображения должны вести себя правильно не только в этом частном случае, но и при включении в произвольную диаграмму. Например, применение квантового отображения всего лишь к какой-то части состояния нескольких систем, как на диаграмме (6.28) ниже, должно снова давать квантовое состояние. На самом деле это (кажущееся более специфичным) условие эквивалентно тому, что отображение квантовое.

Теорема 6.49. Линейное отображение

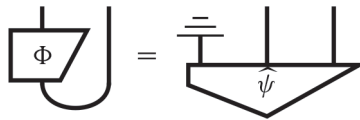


является квантовым отображением тогда и только тогда, когда для любого квантового состояния ρ состояние

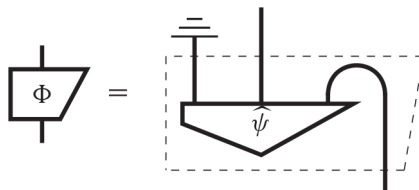


снова квантовое.

Доказательство. Если Φ – квантовое отображение, то (6.28) должно быть квантовым состоянием просто потому, что **квантовые отображения** – это процессная теория. Наоборот, пусть ρ в (6.28) – дублированное состояние-чашка. Тогда, по предположению, это квантовое состояние, поэтому, в силу предложения 6.46, существует чистое квантовое состояние $\hat{\psi}$ такое, что

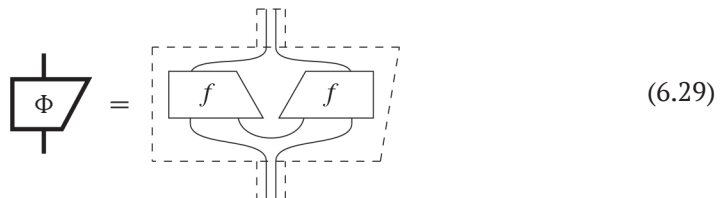


В силу двойственности процессов и состояний отсюда следует, что

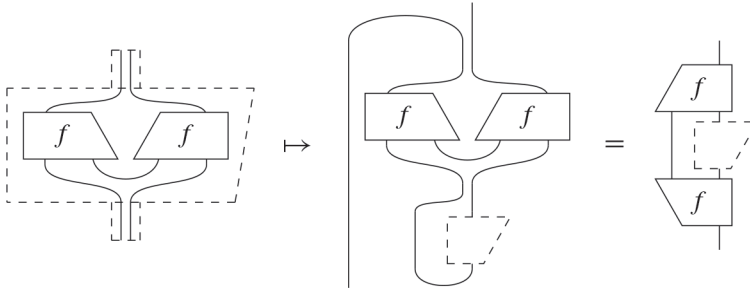


и, стало быть, Φ – действительно квантовое отображение. □

Замечание 6.50. Мы продолжаем с того места, где остановились в замечании 6.43. Прежде всего отметим, что общее квантовое отображение можно эквивалентно представить в виде:



Затем немного изменим форму этой диаграммы:



Здесь небольшой пунктирный блок представляет дырку, в которую можно вставить оператор плотности $\tilde{\rho}$, получив $\tilde{\Phi}(\tilde{\rho})$. «Супероператор» (т. е. отображение, переводящее операторы в операторы)

$$\tilde{\Phi}() := \text{[Diagram: two 'f' blocks, one above the other, with a dashed box between them]} \quad (6.30)$$

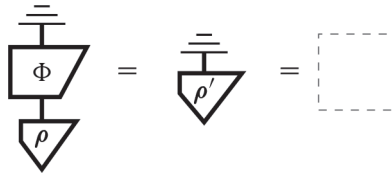
обычно называют *вполне положительным отображением* (completely positive map – CP-отображение). Они также часто встречаются в эквивалентной форме со следом:

$$\tilde{\Phi}() := \text{[Diagram: two 'g' blocks, one above the other, with a loop on the left and a dashed box between them]}$$

Слово «вполне» отражает тот факт, что CP-отображение сохраняет положительность (т. е. свойство «быть квантовым состоянием»), даже если применяется лишь к части системы, как в (6.28). Супероператор, который сохраняет положительность, только когда применяется ко всей системе, называется просто *положительным*. В случае (6.27) положительный супероператор выглядит так:



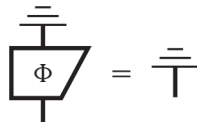
а в силу предложения 6.48 это не то же самое, что форма (6.30).



Поэтому следующий эффект



переводит все каузальные состояния (и, в частности, все нормированные чистые состояния) в 1. Тогда по теореме 6.31 о единственности отбрасывания имеем:



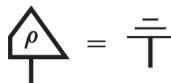
так что квантовое отображение Φ действительно каузальное. □

Равенство (6.32) можно также интерпретировать непосредственно:

если выход процесса отбрасывается, то это все равно, что его никогда и не существовало.

Это прямое обобщение интерпретации каузальных состояний в разделе 6.2.3.

Несмотря на внешнюю невинность, каузальность имеет потрясающее следствие, будучи применена к эффектам. В силу равенства (6.17) отбросить систему «без проводов» – то же самое, что ничего не сделать. Поскольку у эффектов нет выходов, каузальность сводится к такому равенству:



которое означает, что любой каузальный эффект равен отбрасыванию!

Теорема 6.54. Существует единственный каузальный квантовый эффект: отбрасывание.

Таким образом, каузальные эффекты в теории **квантовых отображений** абсолютно неинтересны. Но если каузальность (она же причинность) будет играть такую важную роль, то зачем вообще вводить эффекты? Не огорчайтесь, ваше время было потрачено не зря! Рассмотрев недетерминированные квантовые процессы, мы сможем реализовать все квантовые эффекты недетерминированно, и это окажется решающим фактором для таких приложений, как квантовая телепортация.

Замечание 6.55. Аналог каузальности для вполне положительных отображений (см. замечание 6.50) состоит в том, что они сохраняют след:

$$\text{tr}(\tilde{\Phi}(\tilde{\rho})) = \text{tr}(\tilde{\rho}),$$

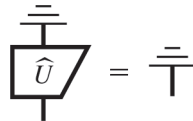
поскольку сохраняющие след CP-отображения переводят операторы плотности в операторы плотности точно так же, как каузальные квантовые отображения переводят каузальные квантовые состояния в каузальные квантовые состояния (см. предложение 6.53).

6.2.6. От каузальности к изометричности и унитарности

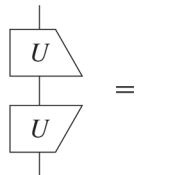
Так какое же ограничение каузальность налагает на чистые квантовые отображения? В разделе 6.2.3 мы уже видели, что для чистых состояний каузальность означает нормированность. Осознав, что нормированное состояние – это просто частный случай изометрии, когда входная система тривиальна, мы можем обобщить это утверждение.

Теорема 6.56. Для чистых квантовых отображений следующие утверждения эквивалентны.

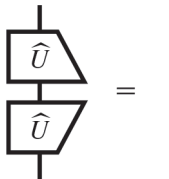
1. Отображение \hat{U} каузальное:



2. Отображение U изометрическое:



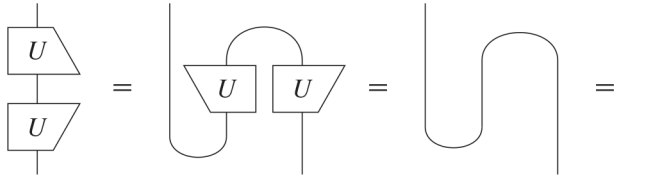
3. Отображение \hat{U} изометрическое:



Доказательство. Раскрывая условие каузальности, имеем:

(6.33)

откуда получаем условие изометричности, согнув левый вход вверх:



и, стало быть, $1 \Leftrightarrow 2$. По теореме 6.20, $2 \Leftrightarrow 3$. □

В теореме 6.54 мы уже видели, что отбрасывание, которое, конечно, не является чистым отображением, – единственный каузальный квантовый эффект. То есть чистых каузальных квантовых эффектов не существует. Из теоремы 6.56 следует более общее утверждение: не существует чистых квантовых отображений из \hat{A} в \hat{B} , если $\dim(A) > \dim(B)$, поскольку в этом случае не существует изометрии из A в B (см. предложение 5.81).

Теперь вспомним предложение 5.81, согласно которому любая изометрия гильбертова пространства в себя должна быть унитарной. Отсюда сразу вытекает следствие теоремы 6.56.

Следствие 6.57. Чистое квантовое отображение системы \hat{A} в себя является каузальным тогда и только тогда, когда оно унитарно.

Разумеется, этот факт опирается на теорему о размерности, которую мы установили только для **линейных отображений**. С другой стороны, теорема 6.56 не зависит ни от каких специальных свойств линейных отображений. Мы можем сформулировать столь же общее следствие. В силу предложения 4.58 обратимые изометрии унитарны. В сочетании с теоремой 6.56 это дает такое

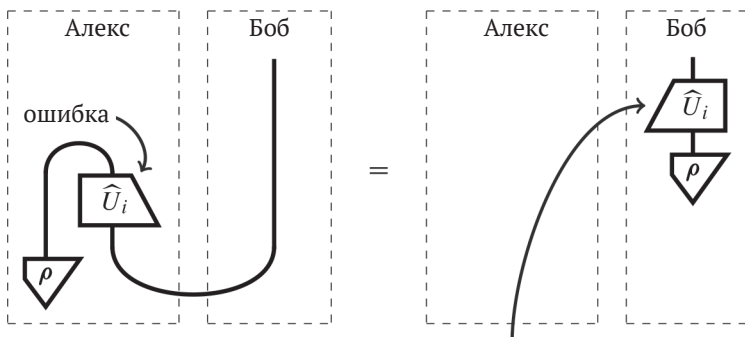
Следствие 6.58. Для любого чистого квантового отображения следующие утверждения эквивалентны:

- 1) оно каузальное и обратимое;
- 2) оно унитарное.

Замечание 6.59. Во многих учебниках унитарность предполагается с самого начала, без особых обоснований. Но причинность (каузальность) с его простой физической интерпретацией обосновать гораздо проще. Таким образом, приятное следствие дублирования состоит в том, что изометричность (а стало быть, и унитарность) так естественно возникает в равенстве (6.33).

Мы уже неявно использовали требование унитарности.

Пример 6.60. Напомним, что в разделе 4.4.4, представляя квантовую телепортацию, мы предполагали унитарность отображения \hat{U}_i в правой части равенства:



Теперь это проблема Боба!

чтобы Боб мог исправить ошибку. Теперь мы знаем, почему: чтобы исправление Боба было каузальным, оно должно быть изометрией, а чтобы отменить действие \hat{U} , оно должно быть еще и унитарным.

А как насчет нечистых процессов? Если соединить тот факт, что все каузальные чистые квантовые отображения являются изометриями, с тем фактом, что любое квантовое отображение можно очистить, то сразу становится понятно, что любое каузальное квантовое отображение можно представить в виде изометрии, один из выходов которой отброшен.

Теорема 6.61 (дилатация Стайнспринга I). Для любого каузального квантового отображения Φ существует изометрия \hat{U} такая, что

$$\text{Diagram } \Phi = \text{Diagram } \hat{U} \tag{6.34}$$

Доказательство. Из предложения 6.46 мы знаем, что всегда существует чистое квантовое отображение \hat{U} такое, что (6.34) выполняется. Из каузальности Φ следует, что \hat{U} тоже должно быть каузальным:

$$\text{Diagram } \hat{U} = \text{Diagram } \Phi = \text{Diagram } \text{---}$$

а это, по теореме 6.56, означает, что \hat{U} – изометрия.

На самом деле этот результат можно усилить, заменив изометрии унитарными отображениями, но это требует чуть больше усилий. Сначала заметим, что любую изометрию можно заменить унитарным отображением и чистым состоянием.

Лемма 6.62. Для любой изометрии U

$$\text{Diagram } U$$

существует унитарное отображение \hat{U} и чистое квантовое состояние $\hat{\psi}$ такие, что

$$\text{Diagram } \hat{U} = \text{Diagram } \hat{U}' \text{ and } \hat{\psi}$$

Доказательство. Зафиксируем ОНБ для A и B такие, что

$$\left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \\ U \\ \text{---} \\ | \\ \text{---} \\ i \\ \text{---} \end{array} \right\} \subseteq \left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \\ j \\ \text{---} \end{array} \right\}_j$$

Затем зафиксируем линейное отображение U' из $A \otimes B$ в $B \otimes A$, которое переводит

$$\mathcal{B} := \left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \\ i \\ \text{---} \end{array} \right\}_{ij} \quad \text{в} \quad \mathcal{B}' := \left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \\ j \\ \text{---} \\ | \\ \text{---} \\ i \\ \text{---} \end{array} \right\}_{ji}$$

и такое, что

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ U' \\ \text{---} \\ | \\ \text{---} \\ i \\ \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ U \\ \text{---} \\ | \\ \text{---} \\ i \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} \quad (6.35)$$

а остальные состояния базиса \mathcal{B} отображаются (инъективно) в остальные состояния базиса \mathcal{B}' . Это всегда возможно, потому что $\dim(A \otimes B) = \dim(B \otimes A)$, и тем самым определяется биективное соответствие базисов \mathcal{B} и \mathcal{B}' . Следовательно, в силу предложения 5.38 U' унитарно. Поскольку равенство (6.35) имеет место для всех белых ОНБ-состояний, то

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ U' \\ \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ U \\ \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array}$$

Дублируя это равенство и отбрасывая первый выход, получаем:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \hat{U}' \\ \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \hat{U} \\ \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \hat{U} \\ \text{---} \end{array}$$

что и завершает доказательство, если положить

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \psi \\ \text{---} \end{array} := \begin{array}{c} \text{---} \\ | \\ \text{---} \\ 0 \\ \text{---} \end{array}$$

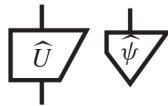
□

Теперь можно сформулировать

Следствие 6.63 (дилатация Стайнспринга II). Любое каузальное квантовое отображение Φ может быть получено из некоторого унитарного отображения \hat{U} путем размещения некоторого чистого каузального квантового состояния $\hat{\psi}$ на одном из его входов и отбрасывания одного из его выходов:

(6.36)

Замечание 6.64. Некоторые используют дилатацию Стайнспринга для обоснования точки зрения, согласно которой единственными настоящими квантовыми процессами являются чистые унитарные процессы, из которых нам доступна лишь малая часть. Эта вера иногда называется «церковью большого гильбертова пространства». Хотя эта точка зрения ничуть не противоречит квантовой теории, она не очень удобна для теоретических рассуждений о процессах. Например, невозможно построить процессную теорию, включающую как унитарные отображения, так и чистые квантовые состояния, не включив в рассмотрение также общие изометрии. Действительно, унитарные квантовые отображения U и чистые квантовые состояния ψ при параллельной композиции дают (неунитарные) изометрии:



Мы вернемся к этой точке зрения в разделе 7.3.2, когда будем обсуждать формулировку квантовой теории фон Неймана.

6.2.7. Разложение Крауса и смешивание

Один из способов понять нечистые квантовые отображения, по самому их определению, состоит в том, чтобы отбросить части большей системы. Теперь мы дадим альтернативную интерпретацию в терминах *смешивания*. Пока что мы ограничимся явными суммами. Но в разделе 8.3.4 будет описан чисто диаграммный подход к смешиванию – как часть общей стратегии избавления от сумм.

Первый шаг на пути к смешиванию – замена отображения отбрасывания суммированием по ONB. Мы можем это сделать, разложив крышку с помощью равенства (5.37):

(6.37)

Соединив это с очищением, мы сможем записать любое квантовое отображение в виде суммы чистых квантовых отображений:

$$\Phi = \widehat{f} = \sum_i \widehat{f}_i \quad (6.37)$$

где

$$\widehat{f}_i := \widehat{f} \triangleleft_i$$

Обратно, любая конечная сумма чистых квантовых отображений является квантовым отображением (напомним, что суммы определены только для процессов одного типа):

$$\sum_i \widehat{f}_i = \widehat{f}$$

где

$$f := \sum_i \triangleleft_i f_i \quad (6.38)$$

В итоге мы доказали следующую теорему.

Теорема 6.65. Сумма чистых квантовых отображений является квантовым отображением, и любое квантовое отображение Φ можно записать в виде суммы чистых квантовых отображений:

$$\Phi = \sum_i \widehat{f}_i \quad (6.39)$$

Такое представление называется *разложением Крауса*.

Замечание 6.66. Для вполне положительных отображений (см. замечание 6.50) разложение Крауса принимает вид:

$$\text{Diagram with } g \text{ and } f_i$$

который обычно встречается в следующей форме:

$$\tilde{\Phi}(\tilde{\rho}) := \sum_i f_i \tilde{\rho} f_i^\dagger$$

Сумма чистых квантовых отображений почти никогда не бывает чистой, поэтому теория **чистых квантовых отображений** не замкнута относительно сложения. Однако имеет место следующая теорема.

Теорема 6.67. Сумма любого конечного множества квантовых отображений

$$\sum_i \boxed{\Phi_i}$$

является квантовым отображением, т. е. теория **квантовых отображений** замкнута относительно сложения.

Доказательство. Поскольку у любого Φ_i имеется разложение Крауса:

$$\boxed{\Phi_i} = \sum_j \boxed{\hat{f}_{ij}}$$

то их сумму можно представить в виде:

$$\sum_i \boxed{\Phi_i} = \sum_i \sum_j \boxed{\hat{f}_{ij}} = \sum_{ij} \boxed{\hat{f}_{ij}}$$

а по теореме 6.65 это квантовое отображение. □

Разложение Крауса не единственно. Однако существуют некоторые особые случаи. Для квантовых состояний из спектральной теоремы (и конкретно из следствия 5.72) вытекает

Следствие 6.68. У любого квантового состояния ρ имеется разложение Крауса вида

$$\boxed{\rho} = \sum_i r_i \boxed{i} \tag{6.40}$$

для некоторого ОНБ и положительных вещественных чисел r_i .

Если применить следствие 6.68 к

$$\boxed{\Phi} \tag{6.41}$$

то мы сможем разложить (6.41) по ОНБ, состоящему из двухкомпонентных состояний. Эквивалентно, можно разложить само Φ по ОНБ Гильберта–Шмидта (см. определение 5.101).

Следствие 6.69. У любого квантового отображения Φ имеется разложение Крауса вида

$$\begin{array}{|c} \hline \Phi \\ \hline \end{array} = \sum_i r_i \begin{array}{|c} \hline i \\ \hline \end{array} \quad (6.42)$$

для некоторого ОНБ Гильберта–Шмидта и положительных вещественных чисел r_i .

В теореме 6.67 мы показали, что сумма квантовых отображений снова является квантовым отображением. Конечно, если сложить каузальные квантовые отображения, то сумма уже не будет каузальной:

$$\begin{array}{|c} \hline \Psi \\ \hline \end{array} + \begin{array}{|c} \hline \Phi \\ \hline \end{array} = \begin{array}{|c} \hline \\ \hline \end{array} + \begin{array}{|c} \hline \\ \hline \end{array} = 2 \begin{array}{|c} \hline \\ \hline \end{array}$$

Однако вместо обычных сумм мы можем рассматривать *выпуклые комбинации* каузальных квантовых отображений.

Определение 6.70. Выпуклой комбинацией, или смесью семейства каузальных квантовых отображений $\{\Phi_{ij}\}$, называется сумма вида

$$\sum_i p^i \begin{array}{|c} \hline \Phi_i \\ \hline \end{array} \quad (6.43)$$

где сумма чисел p^i равна 1.

В этом случае каузальность сохраняется.

Теорема 6.71. Выпуклая комбинация каузальных квантовых отображений является каузальным квантовым отображением.

Доказательство. По теореме 6.67, отображение (6.43) является квантовым, а в силу каузальности каждого из квантовых отображений Φ_i имеем:

$$\sum_i p^i \begin{array}{|c} \hline \Phi_i \\ \hline \end{array} = \sum_i p^i \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline \\ \hline \end{array} \quad \square$$

Операцию, которая порождает сумму (6.43) из $\{p^i\}$ и $\{\Phi_{ij}\}$, мы будем называть *смешиванием*. Каждое число p^i в смеси мы можем интерпретировать как вероятность процесса Φ_i . Иными словами, наличие недостатка информации – представленный распределением вероятностей $\{p^i\}$ – о том, какой именно чистый процесс Φ_i из числа $\{\Phi_{ij}\}$ действительно имеет место. Например, каузальное квантовое состояние

$$\begin{array}{|c} \hline \rho \\ \hline \end{array} = \sum_i p^i \begin{array}{|c} \hline \psi_i \\ \hline \end{array} \quad (6.44)$$

можно интерпретировать как систему, находящуюся в одном из чистых состояний $\hat{\psi}_i$, но в каком именно, мы не знаем. Нам известна только вероятность p^i ее нахождения в i -м состоянии. На самом деле любое каузальное квантовое состояние можно записать в следующей форме.

Теорема 6.72. Всякое каузальное квантовое состояние можно рассматривать как смесь чисто каузальных квантовых состояний. Более того, эти чистые каузальные квантовые состояния можно выбрать так, что они будут образовывать ОНБ.

Доказательство. Поскольку состояния, образующие ОНБ, всегда каузальные, это сразу же вытекает из следствия 6.68. \square

Возникает искушение подумать, что любую нечистоту можно свести к такой ситуации. Но стоит нам попытаться сделать это для отображений более общих, чем состояния, как мы тут же наталкиваемся на препятствие.

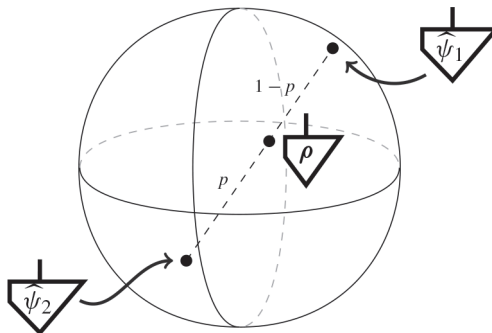
Теорема 6.73. Не всякое каузальное квантовое отображение можно представить в виде смеси чистых каузальных квантовых отображений.

Доказательство. Отбрасывание нельзя разложить в сумму чистых каузальных квантовых эффектов, потому что таких просто не существует (см. теорему 6.54). \square

Идея смешивания важна не только как концептуальная интерпретация нечистых квантовых состояний (и некоторых нечистых квантовых отображений), она еще и дает геометрическую картину таких состояний. В равенстве (6.44) ρ – выпуклая комбинация чистых состояний. В наглядных образах это естественно означает, что ρ расположено где-то между чистыми состояниями, а каждое p^i определяет степень близости к i -му чистому состоянию ($1 :=$ «точно там же», $0 :=$ «настолько далеко, насколько возможно»). Напомним (см. раздел 6.1.2), что каузальные (т. е. нормированные) чистые квантовые состояния можно изобразить в \mathbb{C}^2 как расположенные на поверхности сферы Блоха. Если допустить произвольные каузальные квантовые состояния, то будут включены все выпуклые комбинации состояний на поверхности этой сферы. Значит, мы получим не только сферу, а целый шар, который называется *шаром Блоха*. В этом шаре смешанное состояние

$$\rho := p \hat{\psi}_1 + (1-p) \hat{\psi}_2$$

изображается точкой внутри сферы:



Частным случаем смешивания является смешивание по ОНБ, что позволяет закодировать любое распределение вероятностей.

Предложение 6.74. Если задан фиксированный ОНБ, то распределения вероятностей можно эквивалентно представить как каузальные квантовые состояния вида:

$$\Downarrow_P := \sum_i p^i \Downarrow_i \quad (6.45)$$

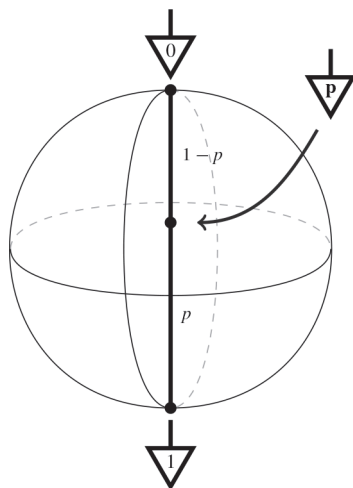
Доказательство. То, что все числа p^i положительны, вытекает из следствия 5.72. А в силу каузальности (см. пометку $(*)$ в цепочке равенств ниже) сумма этих чисел равна 1:

$$\sum_i p^i = \sum_i p^i \overline{\Downarrow_i} \stackrel{(6.45)}{=} \overline{\Downarrow_P} \stackrel{(*)}{=} 1 \quad \square$$

В двумерном случае распределения вероятностей принимают вид:

$$\Downarrow_P := p \Downarrow_0 + (1-p) \Downarrow_1$$

т. е. они зависят только от числа $p \in [0, 1]$, и внутри шара Блоха их можно наглядно представить отрезком прямой, соединяющим два дублированных базисных состояния:



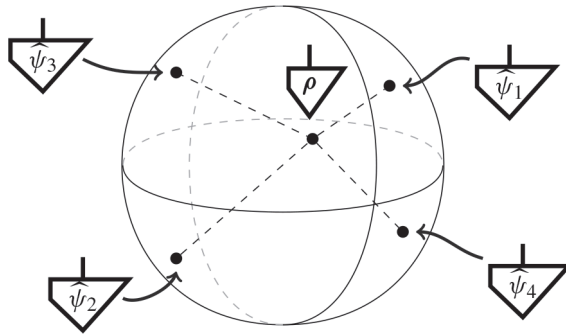
В классической теории вероятностей все на этом и закончилось бы: любое вероятностное состояние единственным образом разлагается в распределение вероятностей по чистым состояниям (т. е. тем, что соответствуют точечным распределениям), на которые натянуто все пространство распределений вероятностей. Но для квантовых состояний ситуация совершенно иная в том смысле, что такое разложение на чистые состояния обычно не единственно: квантовое состояние ρ можно представить как различные смеси чистых состояний. Самый яркий при-

мер этого явления – максимально смешанное состояние, которое можно с одинаковым успехом рассматривать как смесь чистых состояний, соответствующих любому ортонормированному базису. Действительно, в силу предложения 5.56 мы можем разложить чашку по любому ОНБ:

$$\frac{1}{D} \underline{\underline{\perp}} = \frac{1}{D} \cup = \frac{1}{D} \sum_i \nabla_i \nabla_i = \sum_i \frac{1}{D} \nabla_i \quad (6.46)$$

Это также означает, что максимально смешанное состояние «одинаково удалено» от любого чистого состояния, что и объясняет название «максимально смешанное»: оно абсолютно беспристрастно ко всем чистым состояниям.

Таким образом, у заданного смешанного состояния не существует однозначной интерпретации в терминах множества чистых состояний. Фактически нет никаких причин разлагать ρ именно в смесь по базису, а не в смесь всего по двум чистым состояниям. Или по трем, или по четырем:



А почему бы и не по миллиарду? На самом деле смешанные состояния часто используются для описания огромного числа квантовых систем, называемых ансамблями, при самых разных чистых состояниях. Такой ансамбль мог бы, например, представлять все фотоны в лазерном пучке.

Пример 6.75 (шум). Максимальное смешанное состояние можно представлять себе как шум, не похожий ни на какие осмысленные данные, т. е. ни на какое чистое состояние. Рассмотрим следующий процесс:

$$\begin{array}{l} \frac{1}{D} \underline{\underline{\perp}} \leftarrow \text{вывести чистый шум} \\ \frac{1}{D} \underline{\underline{\perp}} \leftarrow \text{отбросить любой вход} \end{array}$$

Этот процесс преобразует любой вход в шум. То, что от входа ничего не остается на выходе, ясно, поскольку диаграмма \circ -разделима. Теперь мы можем смешать это шумовое отображение с любым другим процессом:

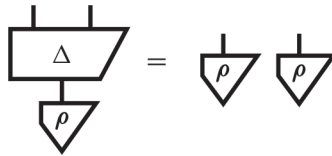
$$(1 - p) \begin{array}{|c|} \hline \Phi \\ \hline \end{array} + p \frac{1}{D} \underline{\underline{\perp}}$$

чтобы привести в него немного шума. Чем больше p , тем сильнее зашумление.

Это все, что мы можем сказать о смешивании в данный момент. В разделе 8.3.4, где приводится пикторалистский взгляд на смешивание, приведены диаграммные аналоги некоторых изложенных здесь результатов, а также ряд новых результатов. В главе 13 мы введем *ресурсную теорию*, которая позволит сравнивать и количественно выражать смешанность.

6.2.8. Теорема о нераспространении

В разделе 4.4.2 мы уже видели, что любая теория, допускающая струнные диаграммы, удовлетворяет теореме о невозможности клонирования. То есть в теории **квантовых отображений** не существует квантового отображения, которое клонировало бы все входные состояния ρ :



Даже если ограничиться чистыми состояниями $\widehat{\psi}$, все равно не существует клонирующих отображений, поскольку чистые квантовые отображения уже допускают струнные диаграммы. Ограничение каузальными состояниями тоже не помогает, т. к. некаузальное состояние всегда можно сделать каузальным, умножив на число.

Раздел 4.4, где мы впервые узнали о невозможности клонирования, был озаглавлен «От струнных диаграмм к квантовым особенностям». Но что стояло за этим названием? Говоря «квантовая особенность», обычно имеют в виду не просто то, что справедливо в квантовой теории, а то, что не имеет места в классической.

В предыдущем разделе мы видели, что распределение вероятностей можно представить в виде квантового состояния следующим образом:

$$\downarrow_p := \sum_i p^i \downarrow_i$$

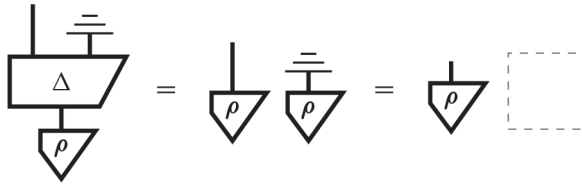
Тогда чистым квантовым состояниям соответствуют точечные распределения



тогда как все остальные распределения вероятностей являются смесями точечных распределений. Это приводит к такой аналогии:

| | Чистое | Смешанное |
|--------------------------------|------------------|---|
| Распределения вероятностей | \downarrow_j | $\downarrow_p := \sum_i p^i \downarrow_i$ |
| Каузальные квантовые состояния | $\widehat{\psi}$ | $\rho := \sum_i p^i \widehat{\phi}_i$ |

Доказательство. Для любого отображения клонирования Δ имеем:



и, из соображений симметрии, второе равенство тоже выполняется. □

Обратное неверно. В частности, мы можем распространять распределения вероятностей.

Упражнение 6.77. Покажите, что $\tilde{\Delta}$ – отображение распространения для распределений вероятностей.

Однако, несмотря на то что распространение слабее клонирования, мы все же не можем распространять квантовые состояния. Поэтому невозможность распространения – истинно квантовая особенность, которая не зависит ни от каких дополнительных предположений, например о чистоте. Чтобы доказать невозможность распространения для квантовых состояний, мы сначала обобщим предложение 6.33 с чистых состояний на любые квантовые состояния.

Предложение 6.78. Если редуцированное состояние любого квантового состояния чистое:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \rho \end{array} = \begin{array}{c} | \\ \psi \end{array} \tag{6.50}$$

то состояние ρ разделяется следующим образом:

$$\begin{array}{c} | \quad | \\ \rho \end{array} = \begin{array}{c} | \\ \rho' \end{array} \begin{array}{c} | \\ \psi \end{array}$$

для некоторого (каузального) квантового состояния ρ' .

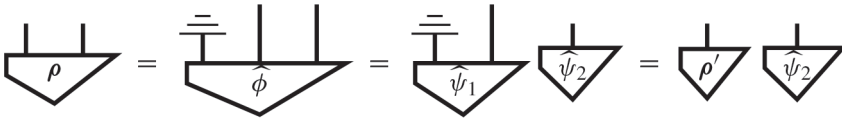
Доказательство. В предположении (6.50) мы сначала очистим ρ (см. определение 6.47):

$$\begin{array}{c} | \quad | \\ \rho \end{array} = \begin{array}{c} \text{---} \\ | \quad | \quad | \\ \hat{\phi} \end{array}$$

и подставим результат в (6.50):

$$\begin{array}{c} \text{---} \quad \text{---} \\ | \quad | \\ \hat{\phi} \end{array} = \begin{array}{c} | \\ \psi \end{array}$$

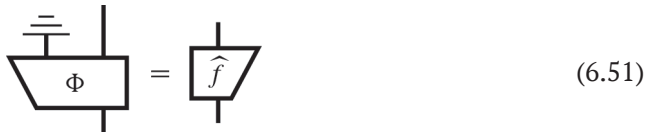
В силу предложения 6.33 $\hat{\phi}$ \otimes -разделимо, и значит:



Путем умножения $\hat{\psi}_2$ на некоторое число мы всегда можем выбрать ρ' каузальным. В таком случае из равенства (6.50) следует, что $\hat{\psi}_2 = \hat{\psi}$. Доказательство обратного утверждения тривиально. \square

И далее обобщим это утверждение на процессы.

Предложение 6.79. Если *редуцированное отображение* произвольного квантового отображения Φ чистое:



то Φ разделяется следующим образом:



для некоторого (каузального) квантового состояния ρ .
Доказательство. Согнем провод на диаграмме (6.51):



Поскольку редуцированное состояние трехкомпонентного квантового состояния чистое, то в силу предложения 6.78 оно разделяется следующим образом:



Остается разогнуть провода – и все доказано. \square

Теперь мы готовы доказать теорему о нераспространении.

Теорема 6.80. Распространение квантовых состояний невозможно.

Доказательство. По теореме 6.24, для любого типа существует базис, состоящий из квантовых состояний, поэтому равенства (6.49) эквивалентны:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \left| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \quad \stackrel{(l)}{=} \quad \left| \quad \stackrel{(r)}{=} \quad \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \quad (6.53)$$

Теперь мы покажем, что такого Δ не существует. В силу предложения (6.53) (l) редуцированное состояние для Δ чистое, поэтому, по предложению 6.79, имеем:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \left| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \quad \stackrel{(6.54)}{=} \quad \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \quad (6.54)$$

для любого состояния ρ . Отсюда следует, что

$$\left| \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right| \stackrel{(6.53)(r)}{=} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \quad \stackrel{(6.54)}{=} \quad \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}$$

Поскольку тождественный процесс \circ -разделим, то же справедливо для любого другого процесса, в котором участвует этот тип, поэтому для существования Δ система должна быть тривиальной. \square

Замечание 6.81. Хотя теорема 6.80 сформулирована конкретно для **квантовых отображений**, мы можем вывести такой же результат для многих других процессных теорий, как сделали в разделе 4.4.2 для теорем о невозможности клонирования. Действительно, если сразу определять распространение посредством равенства (6.53), то теорема о нераспространении имеет место для дублированной версии любой (нетривиальной) процессной теории, удовлетворяющей условию (5.47). С другой стороны, если мы работаем с процессной теорией, которая не является результатом дублирования, то можем определить «чистоту» квантовых процессов в виде условия (6.51), из которого следует равенство (6.52). Тогда теорема о нераспространении справедлива для любой системы, в которой тождественный процесс «чистый» в смысле определения (6.51). Однако при таком подходе возникает подводный камень, о котором мы расскажем в разделе 6.7. Можете ли вы уже сейчас догадаться, в чем дело?

6.3. ОТНОСИТЕЛЬНОСТЬ В ПРОЦЕССНЫХ ТЕОРИЯХ

К настоящему моменту должно быть ясно, что причинность играет центральную роль в квантовой теории. Например, из-за нее все чистые квантовые отображения обязаны быть изометриями, а квантовые изображения общего вида возникают как очищение изометрии посредством дилатации Стайнспринга. В обоснование причинности мы выдвигали такой лозунг:

если выход процесса отбрасывается, то это все равно, что его никогда и не существовало.

Эта мысль воплощена в равенстве

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \square \\ \Phi \\ \square \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \end{array} \quad (6.55)$$

Это также означает, что если процесс протекает где-то в другом месте и его выход до нас не доходит, то мы можем о нем и не думать. Как уже отмечалось, это необходимое условие существования науки вообще, поскольку позволяет без опаски игнорировать те части Вселенной, которые на нас не влияют.

Цель настоящего раздела – показать, что принцип причинности гарантирует совместимость квантовой теории с теорией относительности. Конкретно причинность гарантирует, что

ничто не может перемещаться быстрее света.

Это, быть может, самая неожиданная и убедительная из ее интерпретаций. На самом деле мы увидим также, что в квантовом пикторализме уже заложены релятивистские аспекты и что неотъемлемой частью принципа причинности является тот факт, что законы физики должны быть независимы от наблюдателя.

6.3.1. Причинная структура

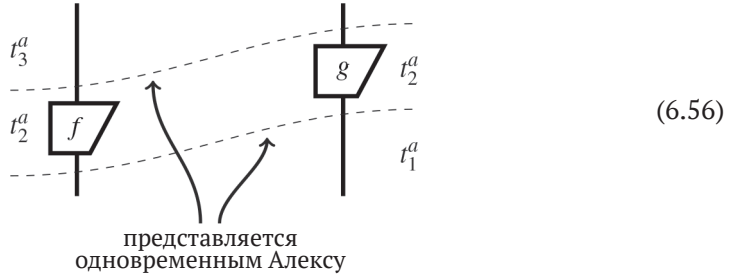
Теория относительности рассказывает нам о структуре пространства и времени, или просто *пространства-времени*. Алекс и Боб не находятся на одной арене, где все происходит по сигналам единого метронома, у каждого из них имеется собственное восприятие реальности и свое ощущение того, с какой скоростью протекают процессы. Относительность в ее простейшей форме *специальной теории относительности* вытекает из двух принципов:

- 1) для всех наблюдателей действуют одни и те же физические законы;
- 2) скорость распространения света в вакууме постоянна.

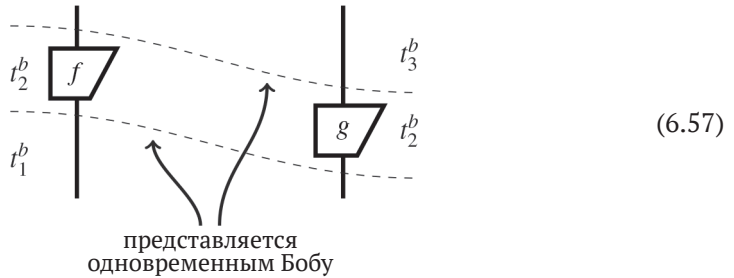
На основе этих принципов, применив немалую изобретательность, можно вывести всю теорию относительности, в т. ч. и следующие положения:

- *относительность одновременности*, означающая, что два процесса, которые Алексу кажутся одновременными, для Боба могут происходить в разное время, и наоборот;
- *невозможность перемещаться быстрее света*, т. е. никакой объект не может достичь скорости, превышающей скорость света, а эта скорость достижима, только если объект не имеет массы, поскольку иначе для перемещения потребовалась бы бесконечно большая энергия.

Первое из этих положений означает, что сценарий



эквивалентен такому:

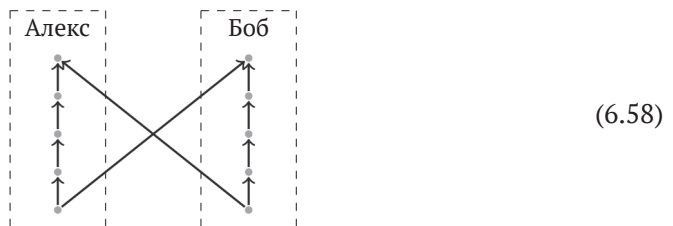


поскольку в обоих случаях по меньшей мере одному наблюдателю эти процессы представляются одновременными. Конечно, мы предполагали это с самого начала, ведь эти диаграммы равны! Следовательно, применяя диаграммный язык, мы уже включили этот важный аспект теории относительности.

Понятие одновременности, потерявшее свой абсолютный (т. е. объективный) смысл, уступает место более слабому (но все еще объективному) понятию *пространственного разделения*, которое позволяет процессам казаться одновременными одним наблюдателям и не казаться таковыми другим. Мы можем изобразить эту ситуацию в виде двух ничем не соединенных точек:



Поскольку сигнал от Алекса к Бобу не может распространяться быстрее света, в случае когда они находятся очень далеко друг от друга, сигналу, посланному Алексом, потребуется ощутимое время, чтобы дойти до Боба, и наоборот. Чтобы визуализировать этот факт, дополним картинку, показанную выше:



Точки представляют процессы, протекающие в каком-то месте пространства-времени, а стрелки показывают возможность процессов влиять друг на друга.

Из (6.58) мы видим, что Алекс и Боб вольны выполнять процессы локально, но процессы Алекса не смогут оказать влияние на процессы Боба (и наоборот) до истечения некоторого времени. Обратите внимание, что мы опустили такие детали, как «насколько далеко» отстоят друг от друга Алекс и Боб и «сколько времени» занимают процессы. Такой чертеж, состоящий из точек и стрелок, и называется *причинной структурой*.

Множество всех точек, достижимых посредством следования по стрелкам из какой-то одной точки, называется *причинным будущим* этой точки. Его следует представлять себе как все точки пространства-времени, которых можно достичь из данной точки, перемещаясь со скоростью, меньшей или равной скорости света. В терминологии теории относительности это называется *световым конусом будущего*. Точно так же существует *световой конус прошлого*, и в совокупности они образуют *световой конус* данной точки.

Разумеется, можно представить себе бесконечно много причинных структур для описания процессов, взаимодействующих во времени и в пространстве. По существу, есть только одно ограничение, выделяющее «допустимые» причинные структуры: (обычно) мы предполагаем, что они не включают ориентированных циклов, как и в случае схемных диаграмм в разделе 3.2.3.

Замечание* 6.82. Можно также определить причинную структуру как *частично упорядоченное множество*, т. е. множество, наделенное отношением \leq таким, что для любых a, b, c :

- $a \leq a$,
- $(a \leq b \text{ и } b \leq c) \Rightarrow a \leq c$,
- $(a \leq b \text{ и } b \leq a) \Rightarrow a = b$.

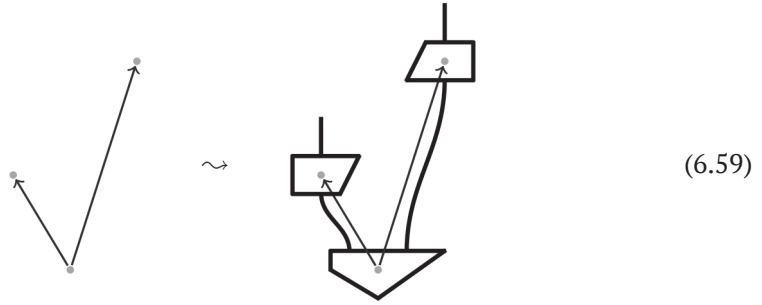
Существует тесная связь между ориентированными ациклическими графами, производными от схем (см. замечание* 3.21), и причинными структурами, и заключается она в том, что любой ориентированный ациклический граф можно превратить в частично упорядоченное множество, взяв его транзитивное замыкание. Поэтому в замечании* 6.82 мы имели право охарактеризовать схемы как диаграммы, допускающие причинную структуру.

Примеры причинных структур: V-образная и вилообразная:

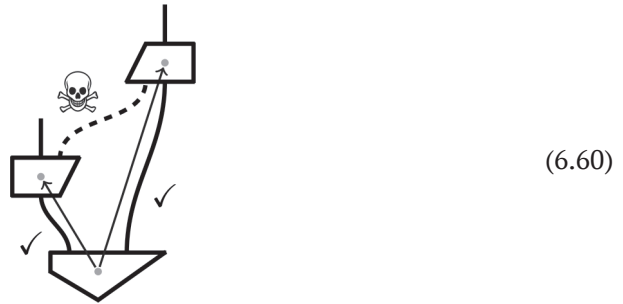


С вилообразной структурой мы встретимся в разделе 11.1, где докажем, что квантовая теория *нелокальна*, а V-образная поможет установить связь между принципом причинности и теорией относительности.

Предположим теперь, что имеется некоторая фиксированная причинная структура, представляющая пространство-время, и процессная теория, которая говорит нам, какие процессы могут иметь место (например, каузальные квантовые отображения). Мы теперь можем считать, что эти процессы протекают в определенных точках пространства-времени, наложив их на причинную структуру:

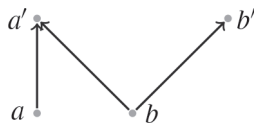


Отметим, что стрелки в причинной структуре говорят, где провода разрешены, а где запрещены:



Процессная теория называется *несигнальной* (non-signalling), если всякий процесс Ψ на диаграмме с фиксированной причинной структурой может оказывать влияние только на процессы в причинном будущем Ψ . Естественно, теория, в которой процесс может влиять на процессы, не принадлежащие своему причинному будущему, называется *сигнальной*.

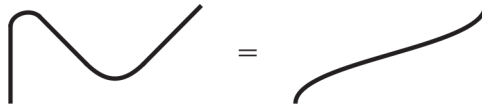
Это нетривиальное требование к процессной теории. Иначе говоря, существуют теории, в которых процессы могут влиять на другие процессы вне своего причинного будущего, даже если ограничиться диаграммами, учитывающими причинную структуру, как в (6.59). Чтобы убедиться в этом, рассмотрим следующую N-образную причинную структуру:



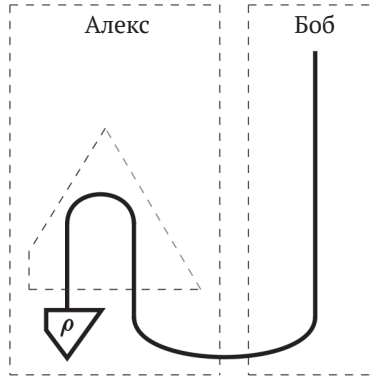
и любую процессную теорию, допускающую струнные диаграммы (например, потенциально некаузальные **квантовые отображения**). Очевидно, мы можем нарушить причинную структуру, введя чашку в точке b и крышку в точке a' :



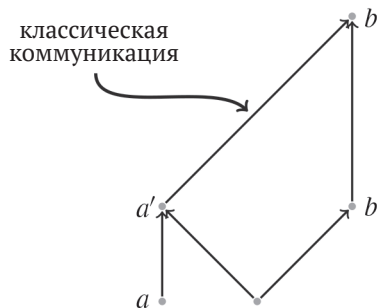
Хотя в причинной структуре не существует ребра, ведущего из a в b' , мы все равно можем передать данные из a в b , поскольку



На самом деле именно это имеет место при квантовой телепортации:



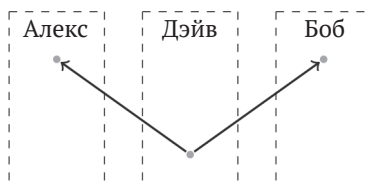
Так что же здесь происходит? Является ли квантовая теория сигнальной, потому что допускает телепортацию? Абсолютно нет! Глядя только на одну «ветвь» протокола телепортации, а именно исправленную ошибку \hat{U}_i , мы упускаем из виду важную часть: передачу Алексова значения i Бобу, что необходимо для исправления этой ошибки. Если включить в рассмотрение и эту классическую коммуникацию, то причинная структура уже не нарушается:



В разделе 6.4.4 мы увидим, что если Алекс не посылает Бобу свое значение i , то состояние, полученное в конце Бобом, будет просто шумом, без какого-либо следа ρ .

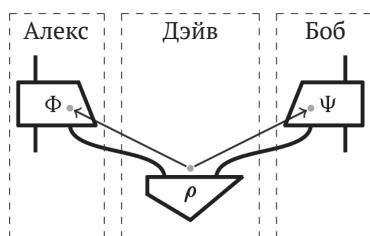
6.3.2. Из причинности следует несигнальность

Чтобы доказать это, мы воспользуемся простой V-образной причинной структурой:



То есть у Алекса и Боба может быть что-то общее, скажем, Дэйв дал им по полвинке запутанного состояния. Но они находятся так далеко друг от друга, что уже не могут общаться, не посылая сообщений со скоростью, большей скорости света, что, разумеется, невозможно.

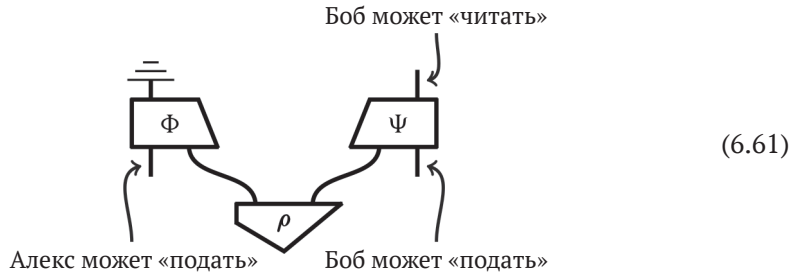
Украсим эту причинную структуру диаграммой процессов:



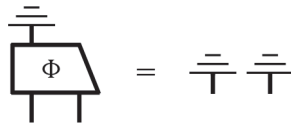
Раньше, при обсуждении телепортации, мы рассматривали весьма специфические процессы, а теперь просто предположим, что все процессы соблюдают принцип причинности. На самом деле приведенное ниже рассуждение проходит даже тогда, когда Φ , Ψ и ρ не являются квантовыми процессами, при условии что они все-таки удовлетворяют уравнению причинности относительно отбрасывания процессов.

Причинная структура позволяет Алексу и Бобу иметь локальные входы и выходы, так что они могут управлять своими процессами и получать от них данные. Технически она допускает входы-выходы и для Дэйва, но нам они не понадобятся. Важно, однако, что поскольку в причинной структуре не существует стрелки от Алекса к Бобу или в обратном направлении, ни один из них не может посылать сигнал другому. Это означает, что ни тот, ни другой не способен узнать что-нибудь о входе напарника, используя только свои собственные входы и выходы. Иначе этим можно было бы воспользоваться, чтобы передать какие-то данные, т. е. сигнал, что явилось бы нарушением причинной структуры.

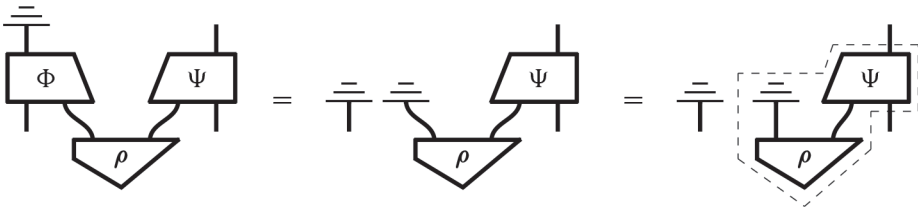
Мы утверждаем, что несигнальность вытекает прямо из принципа причинности (6.55). Начнем с рассмотрения случая, когда Боб хочет узнать что-то о входе Алекса. С точки зрения Боба, мы должны отбросить выход Алекса, потому что Бобу он недоступен:



Теперь посмотрим, может ли Боб узнать что-то о входе Алекса из своей собственной пары вход-выход. В силу принципа причинности



и отсюда следует:



Таким образом, с точки зрения Боба его пара вход-выход не соединена с входом Алекса, который отброшен. Следовательно, никакой сигнал от Алекса к Бобу невозможен. Из соображений симметрий вытекает, что и Боб не может послать сигнал Алексу. В итоге мы доказали следующую теорему.

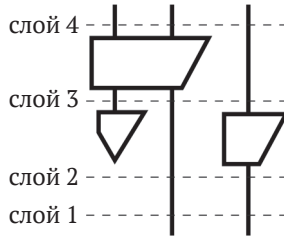
Теорема 6.83. Если в процессной теории имеется процесс отбрасывания для любого типа и она удовлетворяет принципу причинности, то она несигнальная.

Упражнение 6.84. Выше мы установили несигнальность только для V-образной причинной структуры. А что, если попробовать обобщить это на ромбовидную структуру, т. е. добавить точку в совместное будущее Алекса и Боба? Вообще, покажите, что несигнальность – свойство любой причинной структуры.

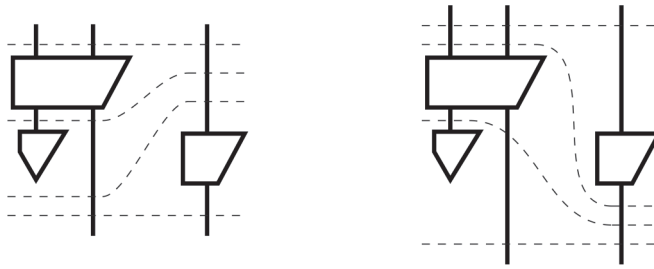
6.3.3. Причинность и ковариантность

Теперь мы покажем, что различные наблюдатели Алекс и Боб всегда будут наблюдать одинаковые физические законы. Точнее, мы покажем, что состояния, ограниченные одним местом пространства-времени (они называются локальными), выглядят одинаково для обоих. Следовательно, и физические законы, которые привели систему в это состояние, тоже должны быть одинаковыми.

Итак, что значит вопрос о том, как «выглядит» локальное состояние для данного наблюдателя? Напомним, что в разделе 6.3.1 мы сказали, что понятие одновременности зависит от наблюдателя. Предположим, что мы разрезали диаграмму на несколько слоев, показывающих, какие процессы уже произошли к моменту каждого отсчета времени с точки зрения одного наблюдателя:

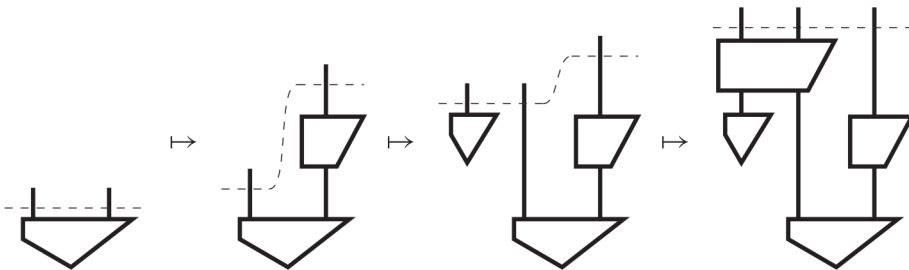


Такой способ разрезания диаграммы называется *слоением*, а поскольку понятие «одновременный» зависит от наблюдателя, то же можно сказать и о слоениях. Следовательно, одна диаграмма допускает много разных слоений:

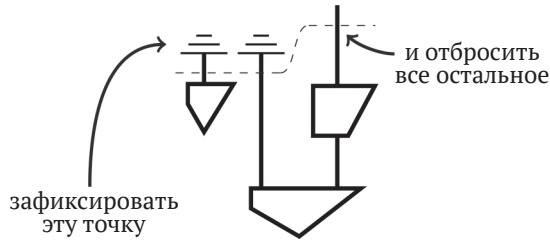


Другой способ выразить тот факт, что физические законы одинаковы для всех наблюдателей, – сказать, что они не зависят от слоения, или *ковариантны*.

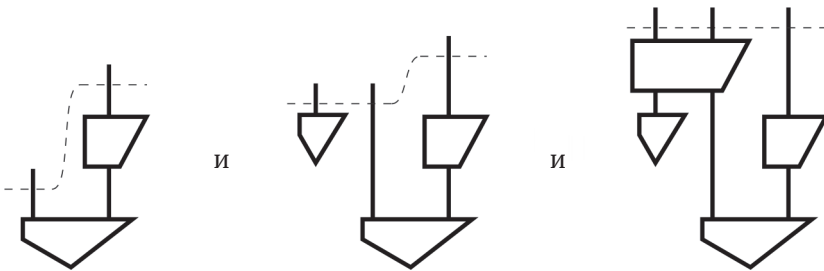
Если мы введем в расслоенную диаграмму начальное состояние, то сможем вычислить результирующее состояние в каждом слое, т. е. сможем увидеть, как происходит эволюция во времени в соответствии с конкретным слоением. Например, левое слоение на рисунке выше дает:



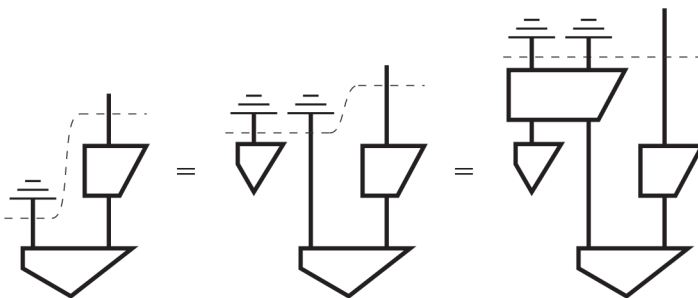
Локальное состояние получается, если зафиксировать одну точку пространства-времени и отбросить все остальные системы в одном слое, например:



Конечно, обычно существует много разных слоев, включающих одну и ту же пространственно-временную точку и происходящих из различных возможных слоений:



Но принцип причинности гарантирует, что локальное состояние не зависит от выбора слоя:



Поэтому оно не зависит и от выбора слоения.

6.4. КВАНТОВЫЕ ПРОЦЕССЫ

Во введении к этой главе мы анонсировали, что причинность станет определяющим ограничением, налагаемым на квантовые процессы общего вида. У таких квантовых процессов может быть больше одного квантового отображения, но все они, как правило, подчиняются варианту принципа причинности, обобщающему тот, что относится к квантовым отображениям. Например, по теореме 6.54 для любого типа существует только один каузальный квантовый эффект: отбрасывание. Истинный потенциал квантовых процессов раскрывается, только если включить в рассмотрение также и недетерминированные процессы. Без этого такие вещи, как телепортация, попросту невозможны, поскольку эффект-крышка, от

$$\sum_i \diamond p_i = \square$$

Мы также можем ассоциировать распределение вероятностей с квантовыми процессами, состоящими из состояний. Пусть дан такой квантовый процесс:

$$\left(\begin{array}{c} \downarrow \\ \rho_i \end{array} \right)^i$$

Тогда вес каждого состояния дает его вероятность:

$$P(\rho_i) := \overline{\overline{\begin{array}{c} \downarrow \\ \rho_i \end{array}}} \quad (6.65)$$

Как отмечалось в разделе 6.2.3, это не что иное, как правило Борна. И снова принцип причинности означает, что сумма этих вероятностей равна 1:

$$\sum_i \overline{\overline{\begin{array}{c} \downarrow \\ \rho_i \end{array}}} = \square$$

В отличие от состояний, с квантовыми процессами общего вида невозможно ассоциировать фиксированное распределение вероятностей. Это не должно вызывать удивления, поскольку если квантовый процесс применяется к системе в определенном состоянии, то вероятности, конечно, зависят от этого состояния. Например, хотя мы еще не сказали, что такое квантовое измерение, должно быть очевидно, что результат чего-либо, имеющего право называться «измерением», должен зависеть от того, что именно измеряется. Однако, применяя квантовый процесс к состоянию, мы можем назначить вероятности, и правило Борна говорит, какими они должны быть:

$$P(\Phi_i | \rho) := \left. \begin{array}{c} \overline{\overline{\begin{array}{c} \downarrow \\ \Phi_i \end{array}}} \\ \downarrow \\ \begin{array}{c} \downarrow \\ \rho \end{array} \end{array} \right\} \begin{array}{l} \text{эффект} \\ \text{состояние} \end{array}$$

а принцип причинности снова гарантирует, что их сумма равна 1:

$$\sum_i \overline{\overline{\begin{array}{c} \downarrow \\ \Phi_i \\ \downarrow \\ \rho \end{array}}} = \overline{\overline{\begin{array}{c} \downarrow \\ \rho \end{array}}} = \square$$

То есть мы можем перенести скобки изнутри наружу, как делали с суммами, и это, как мы увидим в главе 8, не случайное совпадение. Результатом снова является квантовый процесс в силу следующего предложения.

Предложение 6.89. При образовании схем, состоящих из квантовых процессов, каузальность сохраняется.

Доказательство. Мы покажем это для структуры (6.66), которая включает параллельную и последовательную композиции, а значит, произвольные схемы. В силу каузальности квантовых процессов $(\Psi_j)^i$ и $(\Psi'_l)^l$ имеем:

$$\sum_{i,j,k,l} \begin{array}{c} \overline{\overline{}} \\ \Psi_j \\ \Phi_i \end{array} \begin{array}{c} \overline{\overline{}} \\ \Psi'_l \\ \Phi'_k \end{array} = \sum_j \begin{array}{c} \overline{\overline{}} \\ \Psi_j \\ \Phi_i \end{array} \sum_l \begin{array}{c} \overline{\overline{}} \\ \Psi'_l \\ \Phi'_k \end{array} = \sum_i \begin{array}{c} \overline{\overline{}} \\ \Phi_i \end{array} \sum_k \begin{array}{c} \overline{\overline{}} \\ \Phi'_k \end{array}$$

а в силу каузальности квантовых процессов $(\Psi_i)^i$ и $(\Psi'_k)^k$ имеем:

$$\sum_i \begin{array}{c} \overline{\overline{}} \\ \Phi_i \end{array} \sum_k \begin{array}{c} \overline{\overline{}} \\ \Phi'_k \end{array} = \overline{\overline{}} \overline{\overline{}}$$

т. е. из каузальности всех четырех квантовых процессов в левой части (6.66) вытекает каузальность правой части (6.66).

Замечание 6.90. Квантовые процессы «почти» образуют процессную теорию. Определяя процессные теории в главе 3, мы говорили, что они дают интерпретацию диаграмм процессов, а не диаграмм с каким-то странными скобками $(\)^i$. Мы исправим это в главе 8, когда заменим скобки классическими проводами и получим настоящую процессную теорию. А пока не будет никакого вреда, если мы станем трактовать «почти» процессную теорию, как будто она настоящая.

Пример 6.91. Благодаря композиции квантовых процессов все три рассмотренных выше случая назначения вероятностей ветвям сводятся к первому случаю квантовых процессов, состоящих из чисел:

$$\left(\begin{array}{c} \overline{\overline{}} \\ \rho_i \end{array} \right)^i = \left(\begin{array}{c} \overline{\overline{}} \\ \rho_i \end{array} \right)^i \quad \left(\begin{array}{c} \overline{\overline{}} \\ \Phi_i \\ \rho \end{array} \right)^i = \left(\begin{array}{c} \overline{\overline{}} \\ \Phi_i \\ \rho \end{array} \right)^i$$

6.4.2. Недетерминированная реализация всех квантовых отображений

Поскольку недетерминированные квантовые процессы призваны спасти наши любимые струнные диаграммы, они, по меньшей мере, должны предоставлять какие-то эффекты, помимо отбрасывания. Ниже приведен пример как раз такого квантового процесса.

Предложение 6.92. Для любого ОНБ

$$\left\{ \begin{array}{c} | \\ \hline \nabla \\ i \end{array} \right\}_i \tag{6.67}$$

соответствующие дублированные эффекты образуют квантовый процесс:

$$\left(\begin{array}{c} \triangle \\ \hline i \\ \perp \end{array} \right)^i \tag{6.68}$$

Доказательство. Вертикальное отражение (6.46) без множителя $1/D$ дает:

$$\sum_i \begin{array}{c} \triangle \\ \hline i \\ \perp \end{array} = \overline{\overline{\perp}}$$

так что (6.68) действительно каузальный, а значит, является квантовым процессом. \square

На самом деле это один из самых важных примеров квантовых процессов, который называется *измерением ОНБ*. Мы будем подробно изучать его и родственные процессы в следующей главе. А пока он даст нам достаточную долю недетерминированности для порождения произвольных квантовых отображений.

Поскольку базис Белла ортонормирован (см. раздел 5.3.6), в силу предложения 6.92 существует соответствующий квантовый процесс:

$$\left(\begin{array}{c} \triangle \\ \hline B_i \\ \perp \end{array} \right)^i$$

который с точностью до числа включает дублированную крышку в качестве ветви:

$$\begin{array}{c} \triangle \\ \hline B_0 \\ \perp \end{array} := \frac{1}{2} \text{---} \text{---}$$

Это относится к крышке не только для кубитов, но и для произвольной размерности, что, в свою очередь, позволяет восстановить все квантовые отображения.

Лемма 6.93. Эффекты Белла можно реализовать недетерминированно. Точнее, существует квантовый процесс

$$\left(\begin{array}{c} \triangle \\ \hline \hat{\phi}_i \\ \perp \end{array} \right)^i \text{ такой, что } \begin{array}{c} \triangle \\ \hline \hat{\phi}_1 \\ \perp \end{array} := \frac{1}{D} \text{---} \text{---} \tag{6.69}$$

Доказательство. Поскольку в силу предложения 5.79 любое нормированное состояние можно рассматривать как член некоторого ОНБ, существует ОНБ, содержащий нормированную чашку:

$$\left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \phi_1 \\ \text{---} \\ | \\ \text{---} \end{array} := \frac{1}{\sqrt{D}} \text{---} \cup \text{---} , \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \phi_2 \\ \text{---} \\ | \\ \text{---} \end{array} , \dots , \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \phi_{D^2} \\ \text{---} \\ | \\ \text{---} \end{array} \right\} \quad (6.70)$$

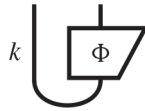
Тогда из предложения 6.92 следует, что (6.69) – квантовый процесс. □

Теорема 6.94. Любое квантовое отображение Φ можно реализовать недетерминированно с точностью до числа. Точнее, существует квантовый процесс

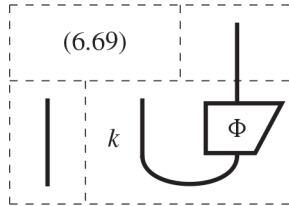
$$\left(\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Psi_i \\ \text{---} \\ | \\ \text{---} \end{array} \right)^i \text{ такой, что } \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Psi_1 \\ \text{---} \\ | \\ \text{---} \end{array} := r \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Phi \\ \text{---} \\ | \\ \text{---} \end{array} \quad (6.71)$$

для некоторого $r > 0$.

Доказательство. Выберем k , так чтобы следующее состояние было каузальным:



В результате композиции этого квантового процесса с квантовым процессом (6.69), построенным в лемме 6.93:



получается квантовый процесс

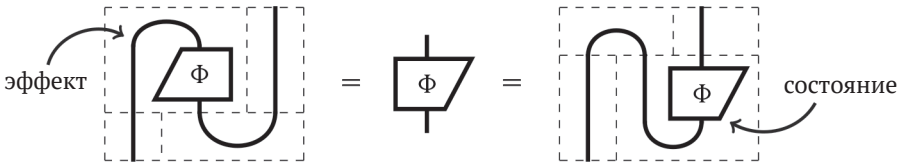
$$\left(\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Psi_i \\ \text{---} \\ | \\ \text{---} \end{array} \right)^i := \left(\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \hat{\phi}_i \\ \text{---} \\ | \\ \text{---} \\ \Phi \\ \text{---} \\ | \\ \text{---} \end{array} \right)^i$$

где

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Psi_1 \\ \text{---} \\ | \\ \text{---} \end{array} = \frac{k}{D} \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \text{---} \\ \text{---} \\ | \\ \text{---} \\ \Phi \\ \text{---} \\ | \\ \text{---} \end{array} = \frac{k}{D} \begin{array}{c} \text{---} \\ | \\ \text{---} \\ \Phi \\ \text{---} \\ | \\ \text{---} \end{array}$$

что и завершает доказательство для $r := k/D$. □

Упражнение 6.95. Квантовое отображение можно реализовать как в виде состояния, так и в виде эффекта:



Докажите теорему 6.94 по-другому, представив Φ в виде эффекта, являющегося ветвью недетерминированного процесса.

6.4.3. Очищение квантовых процессов

Из предложения 6.46 мы знаем, что любое квантовое отображение можно очистить, и, следовательно, можно очистить все детерминированные квантовые процессы. На самом деле это даже встроено в понятие квантового отображения, которое определено как результат композиции чистого квантового отображения с отбрасыванием. У очищения есть очень интересная интерпретация, состоящая в том, что любое квантовое отображение возникает из чистого путем отбрасывания выхода, и, вследствие каузальности, можно предполагать, что это чистое квантовое отображение – изометрия (дилатация Стайнспринга).

На первый взгляд кажется очевидным, что мы можем также очистить недетерминированные квантовые процессы. Действительно, каждую ветвь квантового процесса

$$\left(\begin{array}{c} | \hat{B} \\ \Phi_i \\ | \hat{A} \end{array} \right)^i$$

можно очистить, т. е. существует процесс

$$\left(\begin{array}{cc} | \hat{B} & | \hat{C}_i \\ \hat{g}_i \\ | \hat{A} \end{array} \right)^i \tag{6.72}$$

такой что

$$\begin{array}{c} | \hat{B} \\ \Phi_i \\ | \hat{A} \end{array} = \begin{array}{c} | \hat{B} & \overline{\hat{C}_i} \\ \hat{g}_i \\ | \hat{A} \end{array}$$

Однако здесь скрывается ловушка. Для всех i типы \hat{C}_i могут быть различны, а тогда процессы \hat{g}_i могут иметь разные выходные типы, так что (6.72) уже не является корректно определенным квантовым процессом.

К счастью, проблему можно решить, отыскав подходящее *совместное очищение* ветвей квантового процесса:

Лемма 6.96. Для любого квантового процесса

$$\left(\begin{array}{c} | \hat{B} \\ \hline \Phi_i \\ \hline | \hat{A} \end{array} \right)^i$$

существует единственный тип \hat{C}_i и квантовый процесс

$$\left(\begin{array}{c} | \hat{B} \quad | \hat{C} \\ \hline \hat{f}_i \\ \hline | \hat{A} \end{array} \right)^i$$

такой, что

$$\begin{array}{c} | \hat{B} \\ \hline \Phi_i \\ \hline | \hat{A} \end{array} = \begin{array}{c} | \hat{B} \quad | \hat{C} \\ \hline \hat{f}_i \\ \hline | \hat{A} \end{array} \quad (6.73)$$

Доказательство. Мы знаем, что для любого квантового отображения Φ_i существует очищение

$$\begin{array}{c} | \hat{B} \quad | \hat{C}_i \\ \hline \hat{g}_i \\ \hline | \hat{A} \end{array}$$

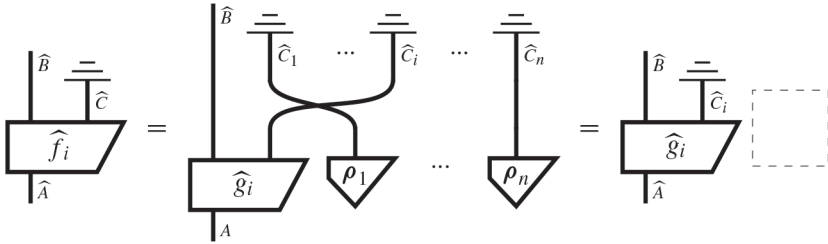
Для любого типа C_j при $j \neq i$ выберем каузальное состояние ρ_j . Затем с каждым чистым квантовым отображением \hat{g}_j ассоциируем другое чистое квантовое отображение \hat{f}_j следующим образом:

$$\begin{array}{c} | \hat{B} \quad | \hat{C} \\ \hline \hat{f}_i \\ \hline | \hat{A} \end{array} := \begin{array}{c} | \hat{B} \quad | \hat{C}_1 \quad \dots \quad | \hat{C}_i \quad \dots \quad | \hat{C}_n \\ \hline \hat{g}_i \quad \rho_1 \quad \dots \quad \rho_n \\ \hline | \hat{A} \end{array}$$

Тогда, в частности, имеем:

$$\hat{C} := \hat{C}_1 \otimes \dots \otimes \hat{C}_n,$$

где n – количество исходов квантового процесса $(\Phi_i)_i$. В силу каузальности всех состояний ρ_i имеем:



и, значит, выполняется (6.73). □

Выбор очищения и, в частности, выбор очищающей системы \hat{C} не однозначен. Хотя доказательство леммы 6.96 дает простой диаграммный способ построения \hat{C} , он не оптимален в том смысле, что размерность C в общем случае оказывается не наименьшей из возможных. В частности, если отображения Ψ_i изначально не являются чистыми, то, по лемме 6.73, размерность C экспоненциально возрастает с ростом числа отображений.

С другой стороны, мы можем найти верхнюю границу необходимой размерности C , которая зависит только от размерностей A и B . Этот результат иногда называют *теоремой Чоя*.

Упражнение 6.97. Покажите, что всегда возможно очистить квантовый процесс

$$\left(\begin{array}{c} | \hat{B} \\ \hline \Phi_i \\ \hline | \hat{A} \end{array} \right)^i$$

взяв $\hat{A} \otimes \hat{B}$ в качестве вспомогательной системы \hat{C} , для чего докажите, что линейное отображение вида

$$\begin{array}{c} | A \quad | B \quad | B \\ \hline f \\ \hline | A \end{array} = \sum_i \frac{1}{\sqrt{D}} \begin{array}{c} | A \quad | B \\ \hline i \\ \hline | A \end{array} r_i \begin{array}{c} | B \\ \hline i \\ \hline | A \end{array}$$

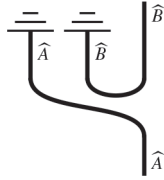
дает очищение любого квантового отображения Φ_i :

$$\begin{array}{c} | \hat{B} \\ \hline \Phi \\ \hline | \hat{A} \end{array} = \begin{array}{c} \overline{\overline{\hat{A}}} \quad \overline{\overline{\hat{B}}} \\ \hline \hat{f} \\ \hline | \hat{A} \end{array}$$

в выбранном подходящим образом базисе Гильберта–Шмидта (указание: воспользуйтесь следствием 6.69.)

Замечание 6.98. Хотя упражнение 6.97 дает верхнюю границу необходимой размерности C , в общем случае она может быть меньше. Например, даже применение леммы 6.96 к множеству чистых квантовых отображений дало бы меньшую

(в данном случае тривиальную) систему C . С другой стороны, иногда необходима полная система $\hat{A} \otimes \hat{B}$. Например, на диаграмме



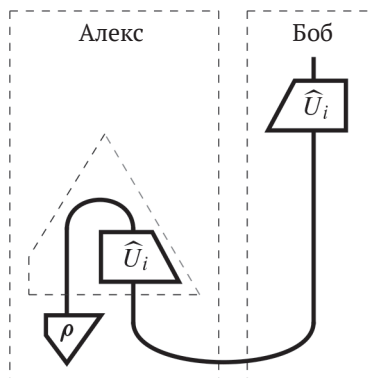
вспомогательная система \hat{C} , очевидно, должна быть не меньше $\hat{A} \otimes \hat{B}$ для любой процедуры совместного очищения.

Ну что ж, пока все недурно. Нам удалось сохранить идею очищения для случая недетерминированных квантовых процессов. Но как насчет дилатации Стайнспринга? В частности, можно задаться вопросом, есть ли возможность выбрать ветви так, чтобы все они были изометриями (быть может, умноженными на некоторую вероятность). Ответ отрицательный. В качестве контрпримера можно привести любой квантовый процесс, состоящий из эффектов (например, состоящий из эффектов ОНБ из предложения 6.92), поскольку очевидно, что не может существовать изометрии из нетривиальной системы в тривиальную.

Однако же мы можем ассоциировать с каждым квантовым процессом единственную изометрию, что, как мы увидим в разделе 7.3.4, дает вполне удовлетворительное обобщение дилатации Стайнспринга на недетерминированные квантовые процессы, называемое *теоремой Наймарка о дилатации*.

6.4.4. Для телепортации необходимо классическое взаимодействие

Пользуясь тем, что мы узнали в этой главе, попробуем наполнить диаграмму квантовой телепортации



квантовыми процессами.

Начав с ρ и половины состояния Белла, Алекс должен выполнить какой-то квантовый процесс, который порождает эффект Белла, возможно, с некоторой ошибкой (представленной чистым квантовым отображением \hat{U}_i). Затем спустя некоторое время Боб должен выполнить другой квантовый процесс, чтобы исправить эту ошибку.

В (6.62) мы установили, что для реализации телепортации обязательны недетерминированные квантовые процессы, поэтому Алекс должен выполнить недетерминированный процесс, состоящий из набора эффектов:

$$\left(\frac{1}{D} \int \widehat{U}_i \right)^i \tag{6.74}$$

и такой, что удовлетворяются условия каузальности:

$$\sum_i \frac{1}{D} \int \widehat{U}_i = \underline{\underline{\mathbb{1}}} \tag{6.75}$$

В этой точке Алекс передает значение i , порожденное своим квантовым процессом, Бобу, а Боб производит корректировку. И хотя мы знаем, как выразить недетерминированные квантовые процессы, мы еще не видели примера квантового процесса, который зависел бы от исхода другого процесса. Прежде чем тратить силы на определение такой штуки, мы должны спросить себя: а так ли необходима корректировка Боба?

Иными словами, что случится, если Алекс решит не передавать Бобу значение i ? Рассмотрим вариант телепортации без корректировки:

$$\left(\int \widehat{U}_i \right)^i = \left(\int \widehat{U}_i \right)$$

Процесс в целом находится в недетерминированном квантовом состоянии (для простоты мы опустили множитель $1/D$). Однако у Боба нет доступа к значению i . Вместо этой информации Боб видит просто смесь всех возможных ветвей. Тогда в силу каузальности квантового процесса мы получаем:

$$\sum_i \left(\int \widehat{U}_i \right)^i = \left(\sum_i \int \widehat{U}_i \right) \stackrel{(6.75)}{=} \int \underline{\underline{\mathbb{1}}} = \underline{\underline{\mathbb{1}}}$$

Таким образом, Боб получает максимально смешанное состояние, без каких-либо следов ρ . Так что мы заключаем, что без классического взаимодействия телепортировать ничего невозможно.

6.4.5. Управляемые процессы

Хорошо, мы установили, что Алекс должен не скрывать значение i , а послать его Бобу, чтобы тот мог произвести корректировку, зависящую от исхода i :



В голову приходит соблазнительная мысль рассматривать множество

$$\left\{ \hat{U}_i \right\}_i \tag{6.76}$$

как недетерминированный квантовый процесс, но это не так! На самом деле, поскольку каждый его элемент сам является квантовым процессом:

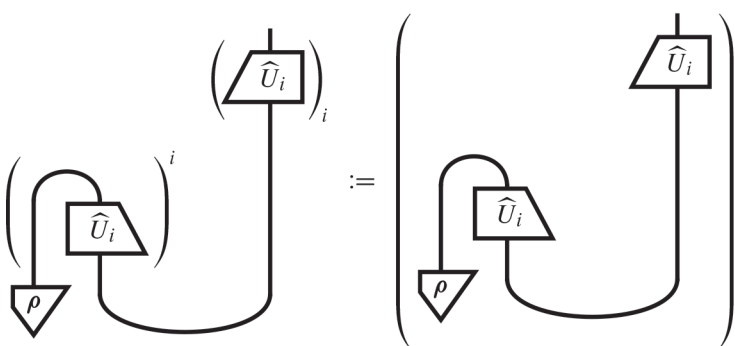
$$\forall i : \hat{U}_i = \text{---}$$

получается, что все N -элементное множество квантовым процессом быть не может:

$$\sum_i \hat{U}_i = \sum_i \text{---} = N \text{---} \neq \text{---}$$

Всего в игре участвует только один индекс i . Ключевое различие между множеством (6.76) и квантовыми процессами состоит в том, что квантовый процесс порождает значение i , тогда как (6.76) зависит от него. Вообще-то, нет никаких причин ограничиваться здесь детерминированными процессами: в зависимости от i мы можем захотеть выполнить какой-то один (недетерминированный) квантовый процесс из множества квантовых процессов. Подобное множество квантовых процессов, зависящее от некоторого классического индекса, мы будем называть *управляемым*.

Таким образом, процесс квантовой телепортации в целом должен выглядеть как-то так:



Для $1 \leq i \leq m, 1 \leq j \leq n$ в случае, когда $m = 1$, это определение сводится к предыдущему понятию неуправляемого квантового процесса. Если $n = 1$, то получается управляемый квантовый процесс, состоящий исключительно из каузальных квантовых отображений (т. е. безо всякой недетерминированности), как унитарные корректировки Боба:

$$\left(\begin{array}{c} \square \\ \hat{U}_i \end{array} \right)_i$$

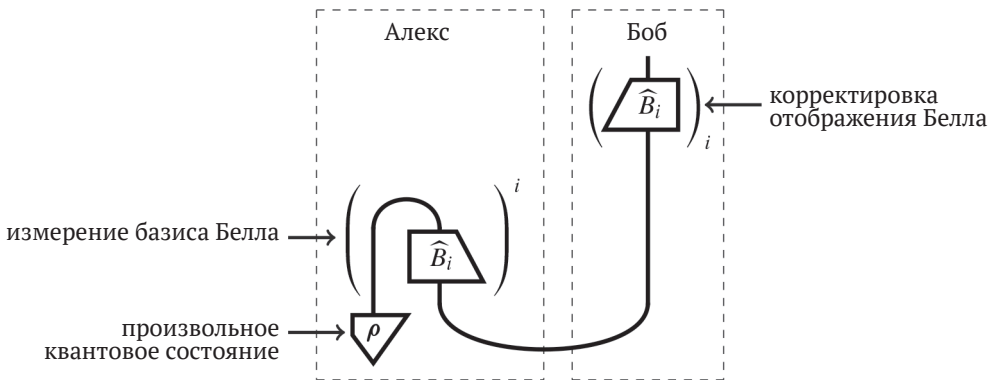
Разумеется, если и m , и n равны 1, то это просто одно каузальное квантовое отображение.

Может возникнуть вопрос, почему мы определили только отдельные квантовые процессы, а не теорию **квантовых процессов**. Сейчас индексы i для квантового процесса рассматриваются как нечто внешнее для диаграммы, а не являющееся проводом. Это не укладывается в наше определение процессной теории, чисто диаграммное по духу и букве.

Мы исправим это в главе 8, заменив индексы *классическими проводами*.

6.4.6. Квантовая телепортация в деталях

Вот и настал момент, которого вы так ждали: у нас есть все ингредиенты для полного описания квантовой телепортации. В случае кубитов квантовая телепортация реализуется следующим образом:



где B_i – i -е отображение Белла. Словами:

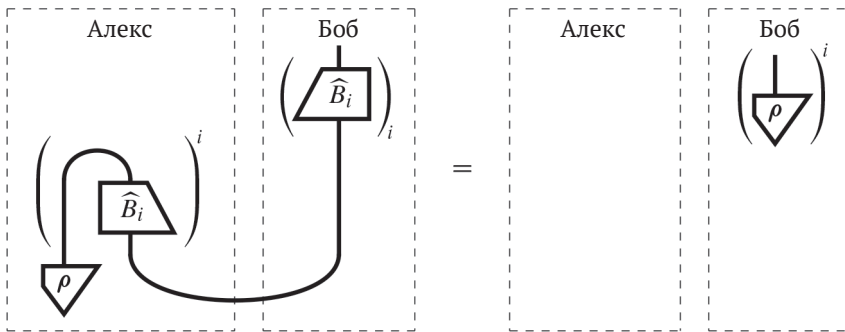
- 1) Алекс располагает произвольным квантовым состоянием ρ , которое хочет отправить Бобу, и Алекс и Боб совместно владеют некоторым состоянием Белла;
- 2) Алекс производит *измерение базиса Белла*, т. е. выполняет следующий недетерминированный квантовый процесс:

$$\left(\begin{array}{c} \square \\ \frac{1}{2} \end{array} \right)_i$$

- для ρ и своей половины состояния Белла;
- 3) Алекс отправляет исход i Бобу;
- 4) Боб выполняет корректировку Белла-отображения, т. е. следующий управляемый квантовый процесс:

$$\left(\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \hat{B}_i \right)_i$$

Как мы уже много раз видели, в результате выполнения этого протокола Боб вне зависимости от результатов измерений Алекса получит ρ :



В разделе 4.4.4 мы также подчеркивали, что телепортация не позволяет передать что-то по какому-то волшебному лучу через пространство, а лишь дает возможность использовать данные одного вида (классические) для передачи данных другого вида (квантовых). Поскольку базис Белла состоит из четырех элементов, Алекс должен передать Бобу число от 0 до 3 (т. е. два классических бита). А Боб получает кубит Алекса, который может быть одной из бесконечного множества точек в шаре Блоха.

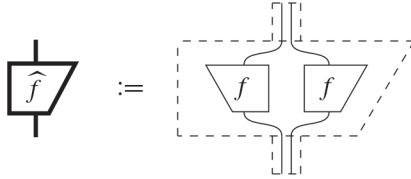
Примечательное свойство квантовой телепортации состоит в том, что хотя мы, по существу, опираемся на недетерминированный квантовый процесс, в итоге порождается детерминированный процесс. То есть как бы ни завершилось Алексом измерение, процесс всегда закончится тем, что Боб получит состояние ρ . Причина, конечно же, в том, что каждая ветвь благодаря корректировке Боба приводит к одному и тому же процессу. Это показывает, что с помощью хитроумных трюков можно «компенсировать» недетерминированность квантовых процессов.

Только что описанный протокол – простейший нетривиальный протокол квантовой телепортации, но ни в матрицах Белла, ни в кубитах нет ничего такого, что обеспечило бы им особую роль в телепортации. Для телепортации нам нужно только множество унитарных отображений

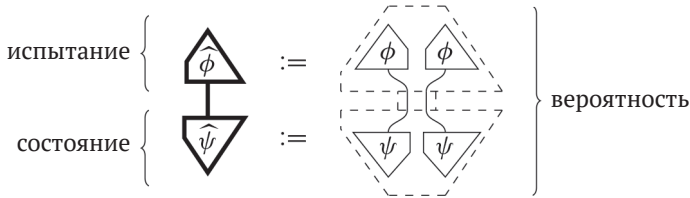
$$\left\{ \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} U_i \right\}_i$$

6.5. ИТОГИ: ЧТО СЛЕДУЕТ ЗАПОМНИТЬ

1. **Чистые квантовые отображения** получаются «дублированием» линейных отображений:



Композиция чистых квантовых состояний и эффектов



дает *правило Борна* для квантовой теории. Эта процессная теория допускает струнные диаграммы, в которых чашки и крышки имеют вид:

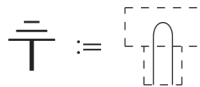


2. Пусть D и D' – произвольные диаграммы в теории **линейных отображений**, а \widehat{D} и \widehat{D}' – их дублированные версии в теории чистых квантовых отображений. Тогда

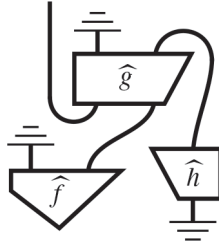
$$\left(\exists e^{i\alpha} : \begin{array}{c} \dots \\ | \\ \text{---} \\ | \\ \dots \end{array} \boxed{D} = e^{i\alpha} \begin{array}{c} \dots \\ | \\ \text{---} \\ | \\ \dots \end{array} \boxed{D'} \right) \iff \begin{array}{c} \dots \\ | \\ \text{---} \\ | \\ \dots \end{array} \boxed{\widehat{D}} = \begin{array}{c} \dots \\ | \\ \text{---} \\ | \\ \dots \end{array} \boxed{\widehat{D}'}$$

Здесь число $e^{i\alpha}$ называется *глобальной фазой*.

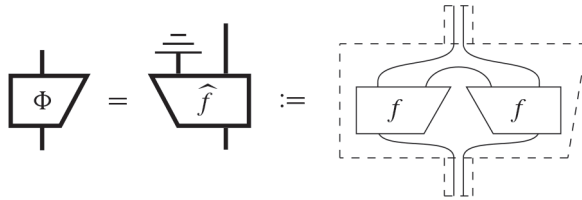
3. **Отбрасыванием** называется линейное отображение



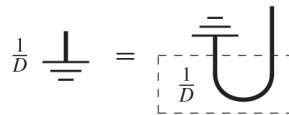
не являющееся чистым квантовым отображением. Процессная теория **квантовых отображений** получается в результате композиции чистых квантовых отображений с отбрасыванием:



Любое квантовое отображение Φ можно записать в виде:



где \hat{f} называется очищением Φ . Например, *максимально смешанное состояние* можно очистить с помощью *состояния Белла*:



4. Принцип причинности

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad (6.81)$$

является реализацией следующего очевидного (и необходимого) факта:

*если выход процесса отбрасывается,
то это все равно, что его никогда и не существовало.*

Отсюда следует, что можно отбросить все, что не «соединено» с чем-то, что нас интересует, – очевидно, что иначе никакая научная деятельность не была бы возможна. Причинность также лежит в основе совместимости с теорией относительности, а особенно со следующим фактом:

ничто не может перемещаться быстрее света.

5. Принцип причинности налагает следующие ограничения:

- все чистые квантовые отображения являются изометриями, и потому
- все чистые квантовые отображения системы в себя унитарны.

Следующий факт известен под названием *дилатации Стайнспринга*:

- для любого каузального квантового отображения Φ существует очищение в виде изометрии \hat{U} :

6. Поскольку отбрасывание следующим образом разлагается по любому ОНБ:

любое квантовое отображение Φ допускает *разложение Крауса*:

Если такое разложение к тому же имеет форму

где $\{p^i\}$ – распределение вероятностей и все \hat{f}_i каузальные, то мы называем его *смесью*. Любое каузальное квантовое состояние можно рассматривать как смесь чистых каузальных квантовых состояний. Однако это неверно для каузальных квантовых отображений общего вида.

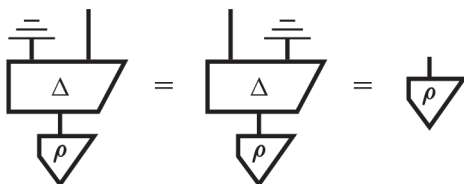
⚠ Нотация смешивания с привлечением сумм введена временно. В главе 8 мы заменим ее пикторалистской.

7. Если *редуцированный процесс* для некоторого квантового процесса является чистым:

то состояние Φ разделяется следующим образом:

для некоторого (каузального) квантового состояния ρ .

8. Квантовые состояния не допускают распространения, т. е. не существует квантового отображения такого, что для любого квантового состояния ρ имеет место равенство

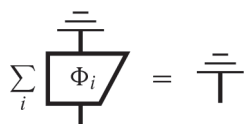


Основной вклад в доказательство этого утверждения дает 7.

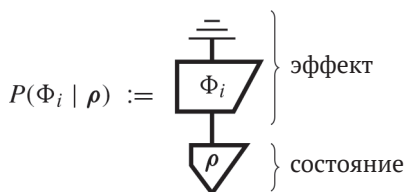
9. **Квантовые процессы** – это списки квантовых отображений:



удовлетворяющие (обобщенному) условию *каузальности*:



Квантовые отображения Φ_i называются *ветвями*, и если ветвей несколько, то квантовый процесс называется *недетерминированным*. Если квантовый процесс применяется к состоянию, то вероятность каждой ветви вычисляется по правилу Борна:



▲ Нотация с привлечением скобок и сумм введена временно. В главе 8 мы заменим ее пикторалистской.

10. Все квантовые отображения возникают как ветви квантовых процессов. Таким образом, для любого квантового отображения Ψ существует квантовый процесс



для некоторого $r \geq 0$.

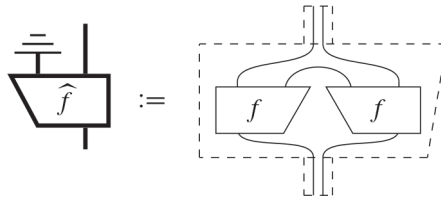
6.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

К началу этой главы у нас уже было очень сильное и по большей части необоснованное предположение: что квантовые процессы следует конструировать из **линейных отображений**. В этом разделе мы посмотрим, как можно обойти это предположение. В частности, мы более пристально рассмотрим конструкцию дублирования (на всем протяжении этого раздела считается, что она включает и отбрасывание) и ее возможную интерпретацию как конструкцию, применимую не только к **линейным отображениям**, но и к любой процессной теории, допускающей струнные диаграммы. Можно надеяться, что на этом пути удастся понять или даже воспроизвести все предсказания квантовой теории способом, полностью независимым от гильбертовых пространств и линейных отображений.

И закончим мы эту главу обращением совсем к другой теме.

6.6.1. Дублирование общих процессных теорий*

В теории **линейных отображений** нет ничего особенного, что было бы необходимо для построения дублированной процессной теории. Если дана любая процессная теория \mathbf{p} , допускающая струнные диаграммы, то мы можем получить новую процессную теорию $\mathcal{D}(\mathbf{p})$, также допускающую струнные диаграммы и составленную из всех процессов вида:



где f может быть любым процессом теории \mathbf{p} . Многие теоремы, доказанные в этой и последующих главах, не зависят от линейных отображений или допускают естественные обобщения. Например, как уже отмечалось в замечании 6.19, доказательство того, что дублирование устраняет «обобщенные глобальные фазы», было чисто диаграммным, поэтому оно допускает непосредственное обобщение.

Теорема 6.102. Пусть f и g – процессы в любой процессной теории, допускающей струнные диаграммы. Тогда

$$\widehat{f} = \widehat{g}$$

тогда и только тогда, когда существуют такие λ и μ , что

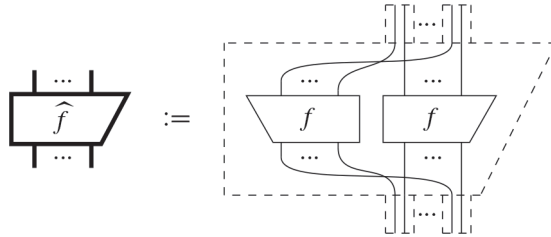
$$\lambda \begin{array}{c} | \\ \square \\ | \end{array} f = \mu \begin{array}{c} | \\ \square \\ | \end{array} g \quad \text{и} \quad \lambda \bar{\lambda} = \mu \bar{\mu}$$

Кроме того, любая процессная теория вида $\mathcal{D}(\mathbf{p})$ допускает отображение отбрасывания, поэтому такие вещи, как причинность, очищение и дилатация Стайн-спринга, по-прежнему имеют смысл.

Таким образом, многие разработанные выше концепции применимы не только к квантовой теории, но могут использоваться для изучения целого семейства «квантовоподобных» теорий. У такого подхода два достоинства. Во-первых, подчеркивая различия с другими теориями, он позволяет глубже понять истинную сущность квантовой теории. Во-вторых, как обсуждалось в разделе 1.2.4, будущие физические теории могут основываться не на **линейных отображениях**, а на чем-то совершенно ином.

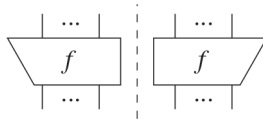
Упражнение* 6.103. Охарактеризуйте теорию $\mathcal{D}(\text{отношения})$. Каковы в ней состояния? Что представляют собой процессы общего вида? Что означает причинность?

На самом деле существует много эквивалентных способов построить такую дублированную процессную теорию. С «перекрещенной» версией, которую мы используем в этой книге:

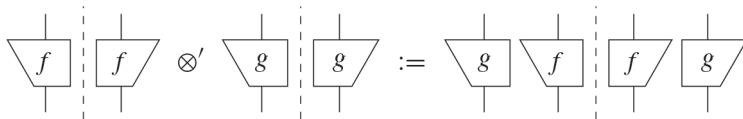


особенно легко работать с помощью диаграмм, потому что в ней применяется та же параллельная композиция, что и в исходной теории, а «две половинки» каждой системы расположены близко друг к другу. Это окажется весьма удобно в главе 8, когда мы начнем моделировать взаимодействие классических и квантовых систем.

В оригинальном варианте этой конструкции (которая обычно называется *СРМ-построением*) такого перекрещивания не было:

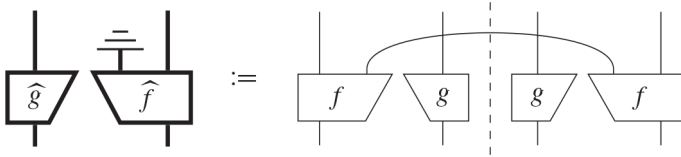


но за это приходилось расплачиваться определением новой параллельной композиции в дублированной категории:



Теперь «обе половинки» каждой системы могут находиться далеко друг от друга, но мы можем представить себе лист бумаги, сгибаемый по пунктирной линии,

чтобы показать, какие системы следует объединить для получения толстых проводов. Процесс отбрасывания в таком случае привносит соединение между левой и правой половинками:



Такой вариант дублирования проще определить с помощью теории категорий (откуда он и происходит), но его диаграммы довольно быстро становятся неудобочитаемыми.

6.6.2. Аксиоматизация дублирования*

Можно ли сказать, является ли процессная теория результатом дублирования? Вы можете воскликнуть: «Да это же просто, нужно только проверить, все ли провода толстые!» Хорошо, тогда перефразируем вопрос. Мы хотим получить аксиоматическую характеристику процессных теорий вида $\mathcal{D}(\mathbf{p})$ для некоторого \mathbf{p} .

Важнейшая черта такой теории состоит в том, что в ней имеются процессы отбрасывания, которые можно использовать для очищения любого процесса. Отметим, что поскольку мы заранее не знаем, имеет ли процессная теория \mathbf{P} вид $\mathcal{D}(\mathbf{p})$, необходимо дать такую характеристику «чистых» процессов, которая не ссылалась бы на дублирование. И вот как выглядит результат этих усилий.

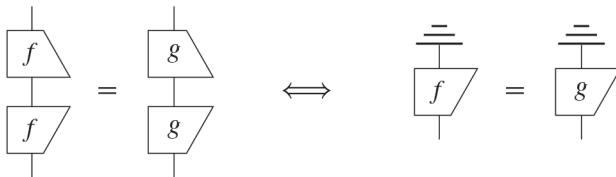
Определение 6.104. Структура отбрасывания для процессной теории \mathbf{P} , допускающей струнные диаграммы, состоит из:

- подтеории $\mathbf{p} \subseteq \mathbf{P}$ «чистых процессов», которая включает все типы из \mathbf{P} , и
- эффекта отбрасывания для каждого типа A :

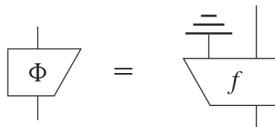


При этом имеют место следующие аксиомы:

1. Все процессы f, g в \mathbf{p} удовлетворяют условию:



2. Любой процесс Φ в \mathbf{P} можно *очистить*, т. е. существует чистый процесс f , принадлежащий \mathbf{p} и такой, что Φ получается отбрасыванием части выхода:



3. Отбрасывание двух систем означает, что отбрасывается каждая из них; при отбрасывании пустой системы не делается ничего:

$$\overline{\overline{\overline{\quad}}}_{A \otimes B} = \overline{\overline{\overline{\quad}}}_A \overline{\overline{\overline{\quad}}}_B \quad \overline{\overline{\overline{\quad}}}_I = \boxed{}$$

а транспонирование отбрасывания совпадает с его адьюнкцией:

$$\overline{\overline{\overline{\quad}}}_\cup = \overline{\overline{\overline{\quad}}}_\perp$$

Любая процессная теория со структурой отбрасывания эквивалентна теории, получаемой дублированием некоторой процессной теории.

Теорема 6.105. Если \mathbf{P} обладает структурой отбрасывания, то

$$\mathcal{D}(\mathbf{p}) \cong \mathbf{P}.$$

Доказательство. Мы докажем это утверждение, построив взаимно однозначное отображение между процессами $\mathcal{D}(\mathbf{p})$ и процессами \mathbf{P} . Поскольку типы в \mathbf{p} такие же, как в \mathbf{P} , существует очевидное соответствие между типом \hat{A} в $\mathcal{D}(\mathbf{p})$ и типом A в \mathbf{P} . Аналогично, поскольку \mathbf{p} – подтеория \mathbf{P} , существует очевидное соответствие между чистым процессом \hat{f} в $\mathcal{D}(\mathbf{p})$ и его аналогом f в \mathbf{P} . Но как быть с нечистыми процессами? Их мы сначала очистим, а затем интерпретируем (обычный) процесс отбрасывания как структуру отбрасывания, существующую в \mathbf{P} :

$$\overline{\overline{\overline{\hat{f}}}} \mapsto \overline{\overline{\overline{f}}} \tag{6.82}$$

Чтобы это отображение было корректно определено, оно не должно зависеть от конкретного выбора очищения, т. е. должна иметь место импликация:

$$\overline{\overline{\overline{\hat{f}}}} = \overline{\overline{\overline{\hat{g}}}} \implies \overline{\overline{\overline{f}}} = \overline{\overline{\overline{g}}}$$

а чтобы оно было инъективным, должна иметь место обратная импликация:

$$\overline{\overline{\overline{f}}} = \overline{\overline{\overline{g}}} \implies \overline{\overline{\overline{\hat{f}}}} = \overline{\overline{\overline{\hat{g}}}}$$

Ту и другую можно доказать, пользуясь аксиомой 1 из определения 6.104 и в полной мере задействовав двойственность процессов и состояний. Аксиома 2 гарантирует, что отображение (6.82) сюръективно. Из этих фактов и аксиомы 3

уже довольно просто показать, что это отображение также сохраняет струнные диаграммы. Детали оставляем читателю. \square

Можно было бы ожидать, что обратное тоже верно, т. е. в процессных теориях вида $\mathcal{D}(\mathbf{p})$ должна присутствовать структура отбрасывания, так что чистые процессы – это те и только те, которые имеют вид \hat{f} для некоторого f из \mathbf{p} . Оказывается, что это почти правда – при условии что чистые процессы в $\mathcal{D}(\mathbf{p})$ удовлетворяют одному дополнительному условию.

Упражнение 6.106. Покажите, что если для чистых процессов в $\mathcal{D}(\mathbf{p})$ имеет место эквиваленция

$$\begin{array}{c} \text{---} \\ | \\ \hat{f} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \hat{g} \\ | \\ \text{---} \end{array} \iff \begin{array}{c} \text{---} \\ | \\ \hat{f} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \hat{f} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \hat{g} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \hat{g} \\ | \\ \text{---} \end{array}$$

то $\mathcal{D}(\mathbf{p})$ обладает структурой отбрасывания. Это условие можно прочесть как «в дублированной теории нет глобальных фаз».

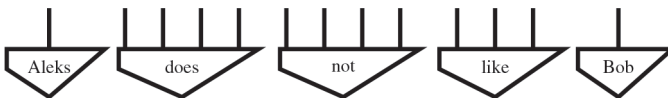
6.6.3. А теперь кое-что из другой области*

Итак, мы теперь знаем, что струнные диаграммы и дублирование – полезные инструменты для выражения квантовых процессов. Но, как ни удивительно, они нашли применение совсем в другой области: в вычислительной лингвистике!

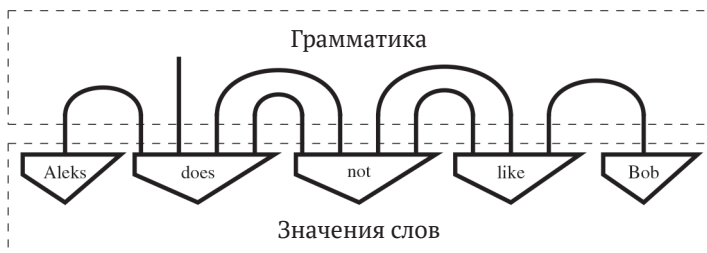
Типичная задача вычислительной лингвистики – взять пару слов и вычислить, насколько они семантически похожи. Например, «собака» и «гончая» должны быть очень похожи, «собака» и «кошка» не так похожи (но, по крайней мере, те и другие – животные), а «собака» и «налоги» совсем не похожи. Самый распространенный способ решения этой задачи – вычислить векторы для слов «собака», «гончая» и «налоги». Для этого часто производится просмотр большого корпуса текстов и автоматическое «обучение» векторов методами искусственного интеллекта. Затем, как мы видели в разделе 4.3.3, можно измерить степень схожести («общности», «перекрытия»), просто вычислив внутреннее произведение.

Этот метод теперь является стандартным, его можно найти практически в любых программах, так или иначе связанных с обработкой естественного языка (поиск в вебе, машинный перевод, таргетированная реклама и т. д.). Но по-настоящему интересные вещи начинаются при попытке обобщить его с отдельных слов на предложения.

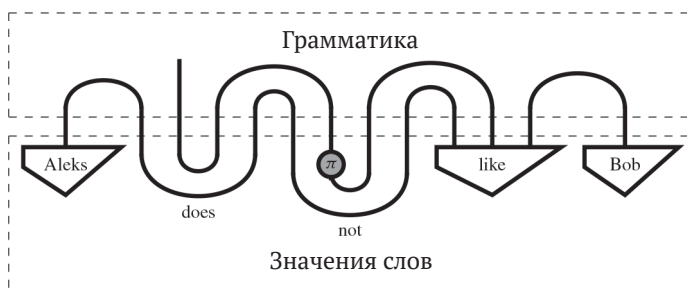
Рассмотрим следующий возможный исход совместного написания учебника двумя авторами:



Каждое слово является состоянием, а различные виды слов (существительные, переходные глаголы, непереходные глаголы и т. д.) имеют разные типы (отсюда и разное число проводов). Тогда, чтобы вычислить смысл предложения, нам нужно всего лишь соединить слова проводами. Для этого необходим набор правил комбинирования слов, но это именно то, что называется *грамматикой*:



Есть слова, которые трактуются как «черные ящики», а есть и такие, которые можно представить в виде диаграмм, показывающих, как они взаимодействуют с другими словами:



И вот теперь мы можем заняться диаграммными вычислениями, которым посвящена эта книга.

Ну а чем нам поможет дублирование? Так же, как и в квантовом случае, оно является предпосылкой «нечистоты». Есть ли место этому понятию в описанной модели языка? Еще какое! Многие слова неоднозначны; например, Bob может относиться к исполнителю фолк-музыки, к исполнителю рэги, к автору мультиков, к потребителю мультиков или к одному из авторов этой книги. Для представления неоднозначности можно воспользоваться смешиванием.

6.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Создателем квантовой теории считается Макс Планк (Max Planck, 1900). Он сделал свое открытие, изучая вопрос о том, как получить максимум света от лампы накаливания при минимальном потреблении электричества (работа выполнялась в интересах электроэнергетических компаний). Для этого он изучал излучение света абсолютно черным телом и понял, что энергия, переносимая светом, могла испускаться только порциями, которые он назвал квантами. Эти порции энергии описываются *формулой Планка*, $E = h\nu$, где h – *постоянная Планка*, ν – частота света, а E – величина порции энергии.

Затем Гейзенберг (Heisenberg, 1925) сформулировал предтечу квантовой теории, используя индексированные наборы «амплитуд перехода». Борн и Йордан (Born and Jordan, 1925) поняли, что Гейзенберг на самом деле имел в виду (бесконечные) комплексные матрицы. Шрёдингер (Schrödinger, 1926) вместо этого говорил о волнах. Дирак (Dirac, 1926) осознал, что волны и частица – одно и то же,

и, наконец, фон Нейман (von Neumann, 1932) собрал все воедино в языке гильбертовых пространств. Правило Борна было сформулировано в работе Born (1926). На этой ранней стадии исследований принимало участие немало других ученых, и многие из них получили за свой вклад Нобелевские премии, в том числе Эйнштейн, Бор, Комптон, де Бройль, Ферми и Паули. Сфера Блоха была предложена в работе Felix Bloch (1946) для представления состояний двумерных квантовых систем и, в частности, систем двух частиц со спином $1/2$.

В работе von Neumann (1927b) введены матрицы плотности для представления смешанных состояний. Квантовые отображения, которые обычно называют вполне положительными отображениями, впервые были предложены для описания общей динамики квантовых систем в работе Sudarshan et al. (1961). Как математические объекты эти отображения изучались и раньше как отображения между C^* -алгебрами (см., например, Paulsen, 2002). Именно в этом контексте впервые появилась дилатация Стайнспринга (Stinespring, 1955). Разложение Крауса можно найти в работе Kraus (1983), а теорема о нераспространении впервые появилась в работе Barnum et al. (1996). Еще одна «обобщенная теорема о нераспространении» сформулирована в работе Barnum et al. (2007), но она касается не процессных теорий, а обобщенных теорий вероятностей.

Как станет ясно в разделе 7.3.2, формулировка квантовой теории фон Неймана кардинально отличалась от ее изложения как процессной теории. Конструкция дублирования из раздела 6.1, которая преобразует линейные отображения в чистые квантовые, была введена в работе Coecke (2007) вместе с доказательством теоремы 6.17. Обобщение на любые квантовые отображения, описанное в разделе 6.2, представлено в работе Selinger (2007) под названием *СРМ-построения*. Идея о том, что это можно сделать, добавив процесс отбрасывания, была высказана в работе Coecke, а нотация «заземления» для отбрасывания введена в работе Coecke and Perdrix (2010). Аксиоматизация СРМ-построения, приведенная в разделе 6.6.2, впервые появилась в работе Coecke (2008).

Квантовые процессы без классического входа называются также *квантовыми приборами*; это понятие ввел Дэвис в работе (Davies, 1976), а дальнейшее развитие оно получило в работе Ozawa (1984).

Принцип причинности, определяющий переход от квантовых отображений к квантовым процессам в разделе 6.4, лишь недавно был признан основополагающим принципом квантовой теории – в работе Chiribella et al. (2010, 2011), где он стал одной из аксиом, на которых была заново построена квантовая теория. Фактически он определялся в терминах равенства суммы вероятностей единице, откуда была выведена единственность каузальных эффектов. Однако между терминологией, применяемой в указанных работах, и нашей имеется расхождение: в тех работах термин «детерминированный» означает «каузальный» в смысле равенства (6.64), так что он может относиться и к тому, что мы называем недетерминированными квантовыми процессами.

Характеристика всех протоколов телепортации, приведенная в разделе 6.4.6, впервые была дана в работе Werner (2001). Первое доказательство теоремы о несигнальности для квантовой теории можно найти в работе Ghirardi et al. (1980). Вывод несигнальности из принципа причинности, как в разделе 6.3.2, взят из работы Coecke (2014b). Похожий результат имеется в работах Fritz (2014) и Henson et al. (2014). Вывод ковариантности из причинности, как в разделе 6.3.3, взят из

работы Coecke and Lal (2013), в которой прежние результаты о ковариантности из работ Markopoulou (2000) и Blute et al. (2003) обобщены на каузальные процессные теории.

Работа Abramsky and Coecke (2004) положила начало аксиоматическому подходу, в которой за отправную точку принята композиция систем. И раньше были попытки взять композицию в качестве отправной точки нового аксиоматического подхода (см., например, Coecke, 2000), но они не увенчались успехом. Из недавних работ по реконструкции квантовой теории на основе диаграмм отметим Chiribella et al. (2011) и Hardy (2012). В конце главы 1 мы приводили ссылки и на более ранние аксиоматические подходы к квантовой теории. Альтернативное определение чистоты, о котором мы упомянули в замечании 6.81, заимствовано из работы Chiribella (2014). На самом деле Чирибелла определил таким образом только чистоту состояний. Как выясняется, обобщение этого определения на общие процессы имеет смысл лишь для квантовых, но не для классических систем. Поскольку классические системы допускают распространение, даже голый провод не является «чистым» в смысле этого альтернативного определения, хотя что-то более «чистое», чем «ничегонеделание», трудно вообразить!

Использование квантовых отображений для описания смысла в естественном языке впервые описано в работе Coecke et al. (2010c), прямое сравнение с квантовой телепортацией можно найти в работе Clark et al. (2014), а интерпретация неоднозначности как смешивания взята из работы Piedeleu et al. (2015).

Глава 7

Квантовые измерения

Новая научная истина торжествует не потому, что ее противники признают свою неправоту, просто ее оппоненты со временем вымирают, а подрастающее поколение знакомо с нею с самого начала.

– Макс Планк, 1936

Квантовая теория оставляет нам единственный способ взаимодействия с квантовыми системами – посредством квантовых процессов. Стало быть, есть только один способ получить информацию о состоянии квантовой системы – применить какой-то недетерминированный процесс и наблюдать, какие его ветви реализовались. Поэтому многие называют акт применения квантовых процессов *измерением*, а иногда даже *наблюдением*. У этой неудачной терминологии есть одно последствие – одну из самых разрекламированных «странностей» квантовой теории часто описывают так: «Сам акт наблюдения квантового состояния изменяет это состояние», – что лишь вводит в заблуждение.

«Вводит в заблуждение», поскольку концепция измерения, описанная в предыдущем абзаце, далека от пассивной концепции наблюдения, знакомой по нашему макроскопическому миру, на самом деле это нетривиальный процесс, который почти всегда радикально влияет на квантовое состояние. Поэтому таинственная особенность квантовой теории состоит не в том, что «наблюдение» изменяет квантовое состояние, а том, что принципиально невозможно «наблюдать» квантовую систему в классическом понимании.

При наличии столь фундаментального ограничения на способ получения информации от квантовой системы что же все-таки мы можем узнать о системе с помощью квантового процесса? На самом деле очень мало! Во-первых, выполнение конкретного измерения может для подавляющего большинства квантовых состояний дать любой исход i с ненулевой вероятностью. В таком случае получение исхода i мало что говорит о том, каким было состояние системы. Во-вторых, мы говорим «было», потому что измерение необратимо изменяет состояние в соответствии с исходом. Поэтому вместо того чтобы дать какие-то сведения о состоянии системы, квантовое измерение обычно стирает все следы этого состояния из истории!

Тем не менее квантовые измерения составляют важнейшую часть квантовой теории, поскольку это единственный интерфейс между классическим и квантовым мирами. Величайшее прозрение, озарившее сообщество квантовых вычислений, состоит в том, что недетерминированные изменения, вызванные квантовыми

измерениями, – не досадная помеха, а чрезвычайно полезный ресурс. Действительно, в предыдущей главе мы видели, что квантовое отображение можно реализовать посредством недетерминированного квантового процесса. На самом деле тот квантовый процесс, который мы использовали для демонстрации этого факта, был простейшей разновидностью квантового измерения.

В протоколе квантовой телепортации именно недетерминированная реализация крышки Алексом посредством измерения и позволяет Бобу получить состояние Алекса после корректировки. В разделе 7.2 мы увидим, что существуют и другие очень полезные протоколы, в которых используется подобный прием. Например, измерения позволяют вклеить короткие отрезки запутанности в длинные и получить важнейший ингредиент модели *квантовых вычислений, основанной на измерениях*, которую мы во всех деталях разработаем в главе 12.

При таком использовании квантовых измерений проектировщики квантового алгоритма и протокола должны проявить недюжинную изобретательность, чтобы устранить получающуюся недетерминированность (например, с помощью унитарных корректировок в случае квантовой телепортации). Это балансирование и составляет львиную долю искусства проектирования квантовых алгоритмов и протоколов.

Так что же такое измерение? С нашей точки зрения, нет никаких принципиальных отличий между измерением и любым другим недетерминированным квантовым процессом, поэтому в этой главе мы будем обсуждать три важных семейства процессов, которые были названы измерениями, а именно:

- 1) *измерения ОНБ*;
- 2) *измерения фон Неймана*;
- 3) *измерения положительной операторной меры (POVM – positive operator valued measure)*.

Каждое из них является более общим, чем предыдущее, и для каждого существуют две разновидности: возмущающее и невозмущающее.



Измерения ОНБ – самый специфичный и «самый чистый» вид измерений, тогда как измерения POVM, как и нечистые квантовые состояния, являются наиболее общими. Между этими двумя крайностями расположились измерения фон Неймана, которые вот уже примерно 80 лет являются доминирующей концепцией измерений. Как следует из названия, именно такие измерения подразумевал фон Нейман в своей формулировке квантовой теории.

Одна из основных причин включения этой главы в книгу – желание привести много конкретных примеров квантовых измерений, начиная с описания прибора Штерна–Герлаха в разделе 7.1.1. Примеров будет так много, что мы даже не станем заводить для них специальные абзацы «Пример».

7.1. ИЗМЕРЕНИЯ ОНБ

Физику, работающему в лаборатории, наверное, будет не совсем понятна вся эта дискуссия по поводу измерений. Дело в том, что хотя результат измерения состояния мало напоминает то, что принято ожидать от простого «наблюдения», в лабораторных условиях многие такие измерения сводятся к наблюдению чего-то, например положения стрелки или пятна на фотопластинке.

Поэтому существует серьезное несоответствие между воздействием на систему, с одной стороны, т. е.

○ *некто намеревается наблюдать систему,*

и тем, что происходит с системой, с другой стороны, т. е.

○ *она претерпевает недетерминированное радикальное изменение.*

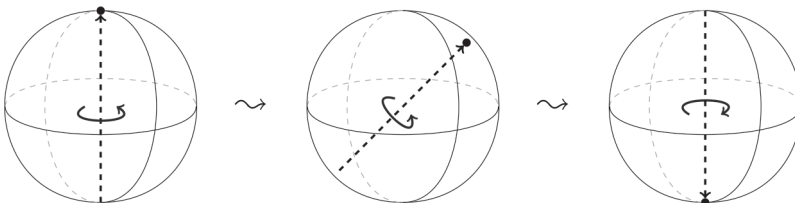
Чтобы понять природу этой нестыковки, полезно знать, с помощью каких приборов производятся реальные квантовые измерения.

7.1.1. Введение в измерительные приборы от додо

Один из самых ранних примеров квантового измерения был произведен с помощью прибора Штерна–Герлаха. Ниже мы подробно объясним, как он работает.

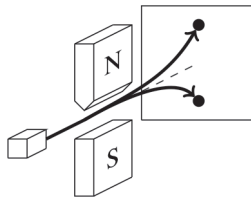
Стандартное упражнение в курсе электромагнетизма – изучить, что происходит с вращающимся магнитом при прохождении через магнитное поле. Если поле всюду одинаково, т. е. *однородно*, то все силы взаимно уравниваются, и вращающийся магнит движется по прямой. Но если в одних точках поле сильнее, чем в других, т. е. *неоднородно*, то магнит отклоняется в зависимости от направления вращения. Классическая физика говорит, что магнит отклонится в одну сторону (скажем, вверх), если вращается по часовой стрелке (относительно магнитного поля), и в другую сторону (скажем, вниз) – если против часовой стрелки. Детали этого вычисления неважны. А важно то, что состояние магнита можно закодировать одним битом информации: 0 – вращается по часовой стрелке, 1 – против часовой стрелки. Чтобы измерить это состояние, мы должны провести магнит через неоднородное магнитное поле и посмотреть, в какую сторону он отклонится.

Мы можем постепенно наклонять ось вращения вращающегося магнита, пока первоначальное направление по часовой стрелке не сменится вращением против часовой стрелки:



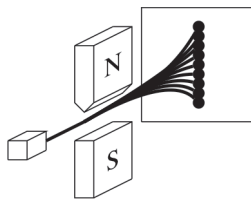
В таком случае направление отклонения в неоднородном магнитном поле постепенно будет меняться – сначала вверх, потом вниз, а в какой-то точке отклонения не будет вообще.

В начале XX века открыли, что при прохождении через магнитное поле электроны ведут себя как вращающиеся магниты. Мы можем воспользоваться этим фактом, чтобы спроектировать устройство для измерения свойства «отклонение вверх» или «отклонение вниз», оно называется прибором Штерна–Герлаха:

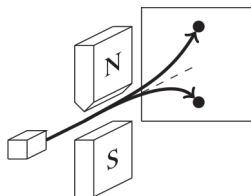


Это устройство пропускает атомы через неоднородное магнитное поле (которое создается, потому что один из магнитов, в данном случае N, заострен), а затем измеряет направление, в котором они отклонились от центра экрана. Предположим для простоты, что мы взяли атомы водорода, содержащие всего один электрон. Если пропустить атом, электрон которого находится в состоянии «отклонение вверх», то атом отклонится вверх, а если в состоянии «отклонение вниз», то атом отклонится вниз. По аналогии с классическим случаем, это свойство электронов называется *спином*, хотя никаким реальным вращением здесь и не пахнет.

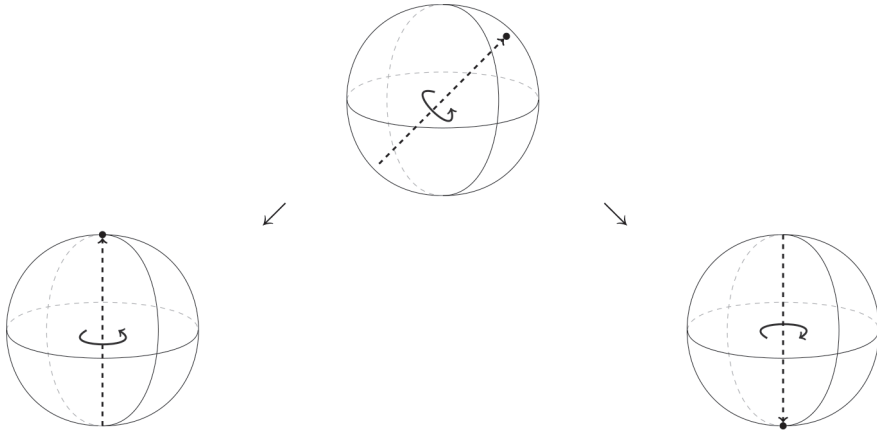
По аналогии с классическим случаем мы ожидаем, что по мере наклона оси вращения будет наблюдаться постепенный переход от отклонения вверх к отклонению вниз. То есть если мы пропустим через такое устройство поток атомов, электроны которых имеют случайно направленные спины, то получится непрерывная линия возможных отклонений:



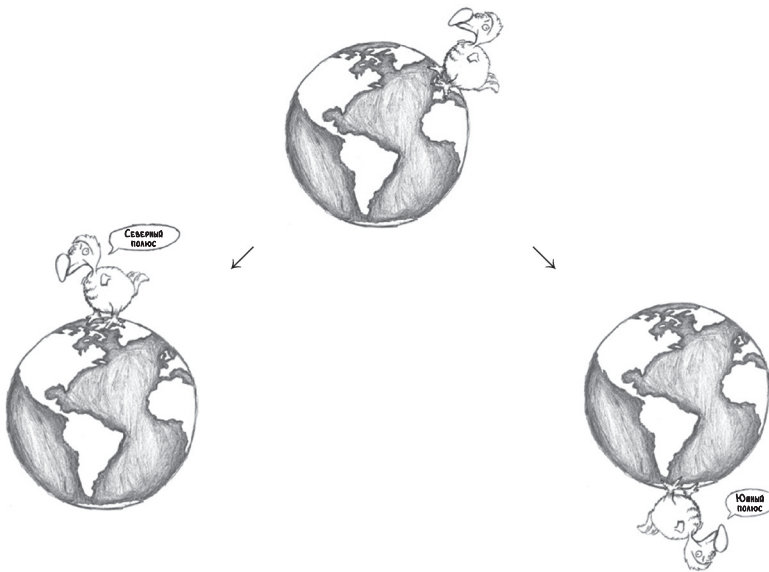
Но на самом деле Штерн и Герлах обнаружили удивительный факт – вместо непрерывной линии исходов наблюдалось ровно два исхода: спин вверх и спин вниз.



Таким образом, ось «вращения» электрона, которую можно изобразить произвольной точкой на сфере, проецируется в одну из всего двух точек:



Что-то знакомое? Ну да, прямо как драматические путешествия додо Дэйва:



Тот факт, что при измерении спина электрона с помощью прибора Штерна–Герлаха возможно всего два исхода, аналогичен открытию Макса Планка (см. раздел 6.7), касающемуся энергии, а именно: величина может принимать только дискретные значения, называемые квантами. В данном случае таких значений два: спин направлен вверх и спин направлен вниз. Этот пример – представитель простейшего семейства квантовых процессов, называемых измерениями: возмущающих измерений ОНБ.

7.1.2. Возмущающие измерения ОНБ

Предложение 6.92 из предыдущей главы гарантирует, что для любого ОНБ

$$\left\{ \begin{array}{c} \downarrow \\ i \\ \nabla \end{array} \right\}_i \quad (7.1)$$

соответствующие дублированные эффекты

$$\left(\begin{array}{c} \nabla \\ i \\ \uparrow \end{array} \right)_i \quad (7.2)$$

образуют квантовый процесс. Мы дадим ему специальное название.

Определение 7.1. *Возмущающим измерением ОНБ* называется квантовый процесс вида (7.2). Индексы i называются *исходами измерения*.

Измерение называется возмущающим, потому что после завершения процесса системы больше не существует. Конкретный физический пример такого процесса – «наблюдение» фотона с помощью старой доброй фотографической пластинки, активно-пиксельного датчика (APS), имеющегося в большинстве цифровых камер, или фотоумножителя, который часто применяется в лабораториях для обнаружения одиночных фотонов (см. рис. 7.1). Все эти устройства поглощают фотон и порождают легко обнаруживаемое подтверждение наличия фотона: пятно на фотопластинке, активированный пиксель в APS или щелчок детектора.

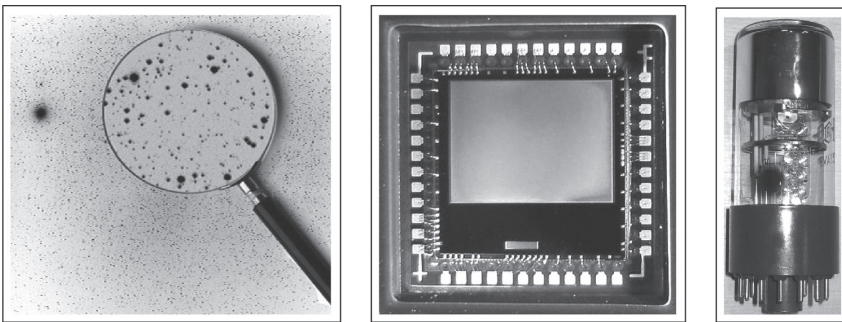


Рис. 7.1 ❖ Три устройства для измерения фотонов (слева направо): фотопластинка, активно-пиксельный датчик (APS), имеющийся в большинстве цифровых камер, и фотоумножитель

Измерение исхода i соответствует тому, что мы наблюдаем с помощью измерительного прибора. Например, в случае APS исход соответствует пикселям, которые были бы активированы при столкновении с фотоном. Количество пикселей определяет число базисных состояний, т. е. размерность квантовой системы \bar{A} . Процесс обнаружения фотона в i -м пикселе соответствует эффекту:

$$\left(\begin{array}{c} \nabla \\ i \\ \uparrow \end{array} \right)$$

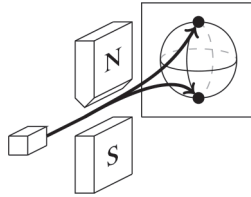
Ниже мы увидим, что любые измерения можно вывести из измерений ОНБ путем округления (раздел 7.3.1) или применения их к части большей системы (раздел 7.3.4).

В предложении 5.38 мы видели, что унитарные отображения, и только они, переводят ОНБ в ОНБ. Из него также следовало, что любой ОНБ можно получить путем применения унитарного отображения к некоторому фиксированному ОНБ. Это наводит на мысль, что множество измерений ОНБ в системе тесно переплетено с унитарными отображениями, которые можно применить к этой системе.

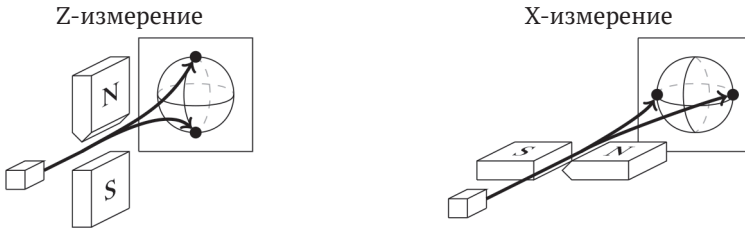
Рассмотрим измерение, выполняемое прибором Штерна–Герлаха из предыдущего раздела. Его можно смоделировать как измерение ОНБ:

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} , \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \right\}$$

Исходы можно изобразить как две точки на противоположных полюсах сферы Блоха – точно так же, как соответствующие состояния ОНБ (см. раздел 6.1.2):

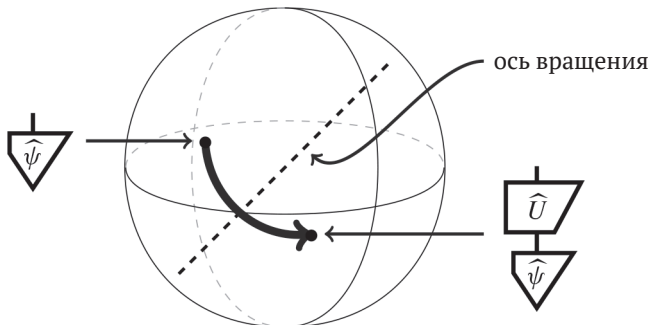


В этом конкретном измерении 0 означает «отклонение вверх», а 1 – «отклонение вниз» вдоль оси Z. Теперь мы можем варьировать измерение ОНБ, просто повернув прибор Штерна–Герлаха относительно источника частиц:

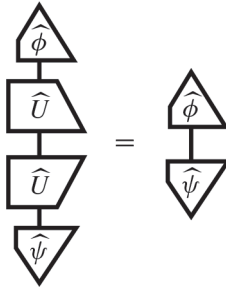


На сфере Блоха это соответствует вращению, а в нашей математической модели – унитарному отображению в силу следующего факта.

Предложение 7.2. Унитарные отображения \hat{U} из \hat{C}^2 в \hat{C}^2 в точности соответствуют вращениям сферы Блоха:

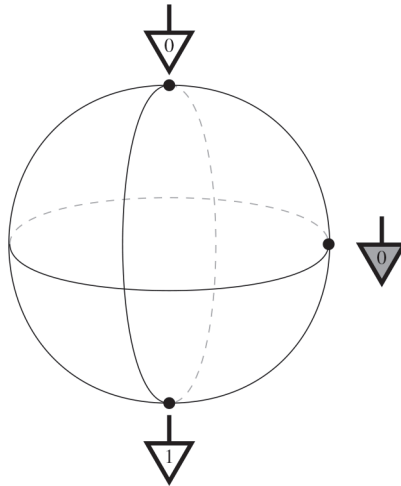


Доказательство (набросок). Это утверждение можно доказать непосредственно с помощью громоздких тригонометрических преобразований, обобщающих то, что мы проделали в разделе 6.1.2, или применив хитроумную теорию представлений групп. Однако на интуитивном уровне оно вытекает из двух фактов. Во-первых, унитарные отображения переводят чистые состояния в чистые состояния. Во-вторых, унитарные отображения сохраняют правило Борна:

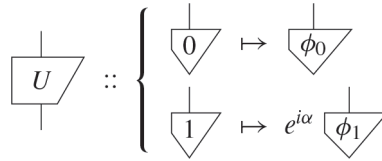


Правило Борна измеряет расстояния между точками на поверхности сферы, поэтому унитарные отображения должны сохранять эти расстояния. А единственные преобразования, сохраняющие расстояния на сфере, – это вращения и отражения. Из этих двух линейных отображений происходят только вращения.

Обратно, вращение сферы однозначно определяется образами любых трех различных точек. Например, можно взять такие:



Вращение переводит антиподы в антиподы, поэтому состояния дублированного Z -базиса переходят в другой дублированный базис $\{\hat{\phi}_i\}$. А состояние X -базиса переходит в какую-то точку на полпути между этими двумя. Очевидно, мы можем построить унитарное отображение U , так что \hat{U} будет делать это (см. следствие 5.39). Не столь очевидно, что путем выбора фазы $e^{i\alpha}$ в



мы можем перевести состояние дублированного X -базиса в любую точку на полпути между двумя антиподами, не затрагивая состояния дублированного Z -базиса.

Замечание* 7.3. Более общая формулировка предложения 7.2 называется *теоремой Вигнера*. Она утверждает, что любая функция ξ на множестве чистых квантовых состояний (без априорного требования о том, что она должна быть линейным отображением), которая сохраняет правило Борна, т. е. удовлетворяет условию

$$\begin{array}{c} \triangle \xi(\hat{\phi}) \\ \downarrow \\ \triangle \xi(\hat{\psi}) \end{array} = \begin{array}{c} \triangle \hat{\phi} \\ \downarrow \\ \triangle \hat{\psi} \end{array}$$

соответствует либо унитарному, либо так называемому *антиунитарному* отображению, являющему композицией унитарного отображения и сопряжения. Далее, на сфере Блоха правило Борна интерпретируется как расстояние между точками, а отображения, сохраняющие это расстояние, – либо вращения, либо композиции вращения с отражением. Легко видеть, что первые соответствуют унитарным отображениям, а вторые – антиунитарным.

Из этого интуитивного геометрического представления на сфере Блоха становится ясно, что все измерения ОНБ для кубитов можно получить с помощью унитарных отображений путем поворота двух противоположных полюсов в любые два других противоположных полюса. На самом деле это справедливо и в общем случае.

Предложение 7.4. Пусть дано измерение ОНБ в системе:

$$\left(\begin{array}{c} \triangle i \\ \downarrow \end{array} \right)^i \tag{7.3}$$

Тогда все остальные измерения ОНБ в этой системе можно получить следующим образом:

$$\left(\begin{array}{c} \triangle i \\ \downarrow \hat{U} \end{array} \right)^i \tag{7.4}$$

где \hat{U} – унитарное квантовое отображение.

Доказательство. Для любого такого измерения ОНБ

$$\left(\begin{array}{c} \triangle i \\ \downarrow \end{array} \right)^i$$

происходящее с измерительным прибором, то мы получаем *картину Гейзенберга*, а если нечто, происходящее с квантовым состоянием, то *картину Шрёдингера*. Разумеется, разница только в том, где «провести черту»:



7.1.3. Невозмущающие измерения ОНБ

Вместо того чтобы рассматривать дублированные ОНБ-эффекты, мы можем рассмотреть пары эффект–состояние:

$$\left(\begin{array}{c} \text{triangle } i \\ \text{trapezoid } U \\ \text{triangle } i \end{array} \right)^i \tag{7.5}$$

И снова получаем квантовый процесс:

$$\sum_i \overline{\text{triangle } i} \text{trapezoid } U \text{triangle } i = \sum_i \text{triangle } i \text{trapezoid } U = \overline{\text{triangle } i}$$

После выполнения такого процесса квантовая система остается. Поэтому мы имеем пример *невозмущающего процесса*.

Определение 7.6. *Невозмущающим измерением ОНБ* называется квантовый процесс вида (7.5). Результирующее состояние называется *состоянием исхода*.

Если дано невозмущающее измерение ОНБ, то мы можем восстановить связанное с ним возмущающее измерение, просто отбросив результирующую систему:

$$\left(\overline{\text{triangle } i} \text{trapezoid } U \text{triangle } i \right)^i = \left(\text{triangle } i \text{trapezoid } U \text{triangle } i \right)^i = \left(\text{triangle } i \right)^i \tag{7.6}$$

Обратно, любое невозмущающее измерение ОНБ можно рассматривать как возмущающее измерение ОНБ, за которым следует управляемая подготовка:

$$\begin{pmatrix} \downarrow i \\ \uparrow i \end{pmatrix}_i = \begin{pmatrix} \downarrow i \\ \uparrow i \end{pmatrix}_i$$

Следовательно, каждая ветвь невозмущающего измерения ОНБ вызывает переход состояния системы в соответствующее состояние исхода измерения (числа игнорируются):

$$\begin{pmatrix} \downarrow i \\ \uparrow i \end{pmatrix} :: \begin{pmatrix} \downarrow \psi \\ \uparrow \psi \end{pmatrix} \mapsto \begin{pmatrix} \downarrow i \end{pmatrix} \quad (7.7)$$

Таким образом, хотя невозмущающие измерения не уничтожают саму систему, они необратимо уничтожают почти все состояния системы. Единственными исключениями являются *собственные состояния* измерения.

Определение 7.7. Если дано измерение ОНБ

$$\begin{pmatrix} \uparrow i \\ \uparrow i \end{pmatrix}_i \quad \text{или} \quad \begin{pmatrix} \downarrow i \\ \downarrow i \end{pmatrix}_i$$

то состояния, принадлежащие множеству

$$\left\{ \begin{pmatrix} \downarrow i \end{pmatrix} \right\}_i$$

называются *собственными состояниями* этого измерения ОНБ. Состояние, не являющееся собственным состоянием данного измерения ОНБ, называется *суперпозиционным состоянием*.

В определении 5.42 мы определили собственные состояния общих процессов как состояния, которые процесс оставляет неизменными (с точностью до числа). По своему духу определение 7.7 очень близко – собственными называются в точности те состояния, которые достоверно переходят в себя в результате (невозмущающей формы) измерения ОНБ.

7.1.4. Суперпозиция и интерференция

Сначала посмотрим, какие исходы измерения ОНБ можно получить, когда система находится в определенном состоянии. Вероятность получить исход i , как всегда, дается правилом Борна:

$$P(i | \rho) := \begin{array}{c} \triangleup i \\ \downarrow \\ \triangleleft \rho \end{array}$$

Эта вероятность равна 0 тогда и только тогда, когда ρ и i -е состояние ОНБ ортогональны:

$$\begin{array}{c} \triangleup i \\ \downarrow \\ \triangleleft \rho \end{array} = 0$$

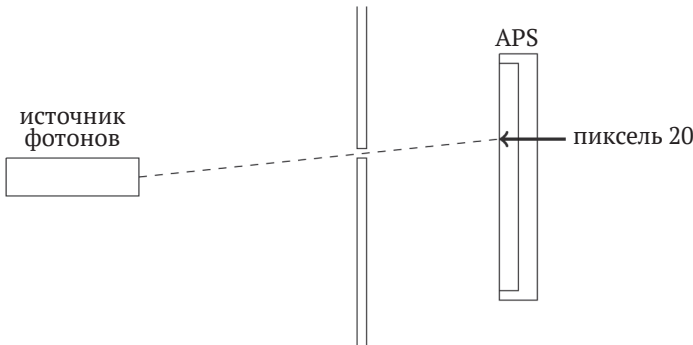
В случае кубитов есть только одно такое состояние, которое на сфере Блоха представляется антиподом. Поэтому для подавляющего большинства состояний возможны все исходы i ! Стало быть, каждое состояние может приводить к большинству исходов, а каждый исход может получиться для большинства состояний. Поэтому измерение выглядит скорее как лотерея, чем как настоящее «наблюдение».

В случае APS (рис. 7.1) это означает, что для большинства состояний фотон может быть детектирован любым пикселем. Но тогда, прежде чем фотон уничтожится, можно задать вопрос:

где был фотон?

В соответствии с вероятностями, вычисляемыми по правилу Борна, он «понемножку» находился одновременно всюду, а затем, после начала процесса измерения, лотерея решает, в каком месте он обнаружится. Но позвольте, как же тогда цифровые камеры (или наши глаза, если на то пошло!) порождают изображения действительности, а не мешанину случайных пикселей?

По счастью, хотя фотон понемножку находится всюду, «по большей части» он оказывается там, где мы ожидаем его найти. Например, рассмотрим такую установку:



Состояние фотона к моменту падения на APS можно записать в виде:

$$\begin{array}{c} \downarrow \\ \triangleleft \hat{\psi} \end{array} = \text{double} \left(\sum_j r_j e^{i\alpha_j} \begin{array}{c} \downarrow \\ \triangleleft j \end{array} \right)$$

Здесь базисное состояние j соответствует j -му пикселю APS, а комплексные числа записаны в полярной форме (см. раздел 5.3.1). Что касается $\hat{\psi}$, то вещественное число r_j велико, когда $j = 20$, но быстро падает по мере того, как j удаляется от 20. Конечно, фаза $e^{i\alpha_j}$ зависит также от j , но при вычислении вероятностей срабатывания каждого из пикселей APS фаза уничтожается:

$$P(j | \hat{\psi}) := \begin{array}{c} \triangle \\ i \\ \hline \triangle \\ \hat{\psi} \end{array} = \overline{(r_j e^{i\alpha_j})} (r_j e^{i\alpha_j}) = (r_j)^2$$

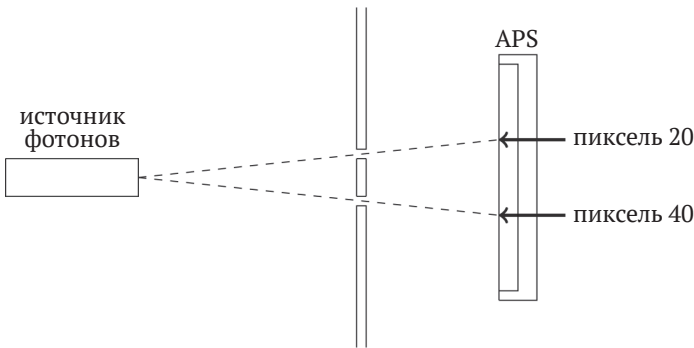
Если нанести вероятности на график, то получится нечто такое:



где белый цвет означает вероятность 1 в пикселе j , а черный – вероятность 0. Аналогично, если открыть щель перед пикселем 40, то будет порождено еще одно состояние $\hat{\phi}$. Вероятности для $\hat{\psi}$ сконцентрируются вокруг значения 40:



Так чем наблюдения (7.8) и (7.9) состояний $\hat{\psi}$ и $\hat{\phi}$ плохи? Выше мы видели, что $P(j | \hat{\psi})$ зависит только от r_j , и то же самое верно для $P(j | \hat{\phi})$. Важно, что нет и следа фаз α_j . Ну и что? Быть может, эти фазы, как и глобальные фазы, от которых мы избавились в разделе 6.1.2, вообще ни на что не влияют. Так можно было бы подумать, пока мы не откроем обе щели:



так что в результате образуется состояние

$$\text{double} \left(\begin{array}{c} \downarrow \\ \psi \\ \triangle \end{array} + \begin{array}{c} \downarrow \\ \phi \\ \triangle \end{array} \right) \tag{7.10}$$

Взгляд на вероятности пикселей APS вызывает замешательство:



Вместо двух симпатичных четких пиков мы получили чередующиеся светлые и темные полосы. Дело в том, что фазы $\hat{\psi}$ и $\hat{\phi}$, которые оставались невидимы в первых двух измерениях, в третьем измерении начинают *интерферировать*. Это приводит к результату, которого никак нельзя было ожидать, глядя на (7.8) и (7.9) по отдельности.

Замечание 7.8. Такая конфигурация, называемая *двухщелевым* экспериментом, используется для демонстрации того, что свет ведет себя одновременно как частица и как волна. Хотя мы получаем интерференционные полосы, ожидаемые при изучении волн, в каждом отдельном эксперименте фотон детектируется только в одном пикселе, что характерно для частицы (см. рис. 7.2).

Теперь предположим, что мы каждый раз можем узнать, через какую щель проходит фотон. В таком случае (игнорируя исход измерения «какая щель») мы получаем смесь вместо суперпозиции:

$$\frac{1}{2} \left(\begin{array}{c} \downarrow \\ \hat{\psi} \end{array} + \begin{array}{c} \downarrow \\ \hat{\phi} \end{array} \right) \quad (7.12)$$

Разумеется, мы еще с раздела 6.1.5.2 знали, что дублирование не сохраняет суммы, и действительно это дополнительное измерение уничтожило всю интересную интерференцию из (7.11), оставляя такие вероятности:

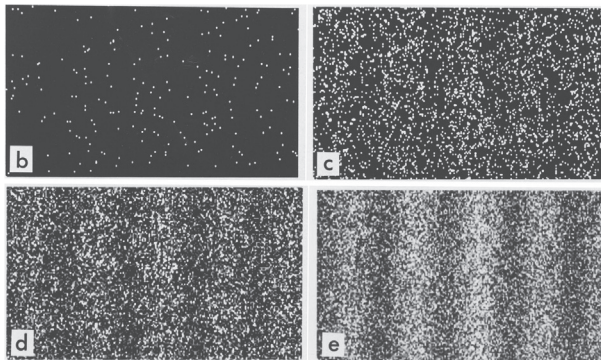


Рис. 7.2 ❖ Более традиционный двухщелевой эксперимент с участием фотографической пластинки. Обратите внимание, что интерференционные полосы появляются, даже когда фотоны подаются один за другим через двойную щель. Таким образом, волновое поведение имеет место даже для одиночных фотонов



Итак, при измерениях ОНБ, как правило, теряется очень много данных о квантовом состоянии и могут даже уничтожаться интересные виды квантового поведения. Поэтому измерения ОНБ не годятся для «наблюдения» квантовых состояний. Несмотря на это, они наилучшая из имеющихся альтернатив наблюдению.

7.1.5. Наилучшая из имеющихся альтернатив наблюдению

Подводя итоги нашим размышлениям о квантовом измерении, можно сказать, что наблюдать квантовые системы в классическом смысле принципиально невозможно.

Теорема 7.9. «Наблюдение» не является квантовым процессом.

Наполним теорему 7.9 каким-нибудь формальным содержимым. В идеале «наблюдение» было бы квантовым процессом, сообщаящим точное состояние системы. Конкретно, наблюдение

$$\left(\begin{array}{c} \triangle \\ \text{e}_{\hat{\phi}} \\ \text{T} \end{array} \right)^{\hat{\phi}}$$

должно было бы быть процессом, обладающим тем свойством, что для любого чистого состояния $\hat{\psi}$ существует соответствующий ему исход, получаемый с вероятностью 1 тогда и только тогда, когда система находится в состоянии $\hat{\psi}$:

$$\begin{array}{c} \triangle \\ \text{e}_{\hat{\phi}} \\ \text{T} \\ \triangle \\ \hat{\psi} \end{array} = \begin{cases} 1 & \text{если } \hat{\psi} = \hat{\phi} \\ 0 & \text{в противном случае} \end{cases} \quad (7.13)$$

Заметим, что мы ограничиваемся только чистыми состояниями. Мы не ожидаем, что это должно быть справедливо для нечистых состояний, потому что некоторая (возможно, важная) часть состояния уже отброшена. Однако даже при таком ограничении можно доказать следующую лемму.

Лемма 7.10. Никакой квантовый процесс не удовлетворяет условию (7.13).

Доказательство. Пусть

$$\left\{ \begin{array}{c} \text{T} \\ \triangle \\ 0 \end{array}, \begin{array}{c} \text{T} \\ \triangle \\ 1 \end{array} \right\} \quad \text{и} \quad \left\{ \begin{array}{c} \text{T} \\ \triangle \\ 0 \end{array}, \begin{array}{c} \text{T} \\ \triangle \\ 1 \end{array} \right\}$$

– чистые состояния, полученные из двух различных (и непересекающихся) ОНБ, например Z- и X-базиса из раздела 5.3.4. Отразив (6.37), получим:

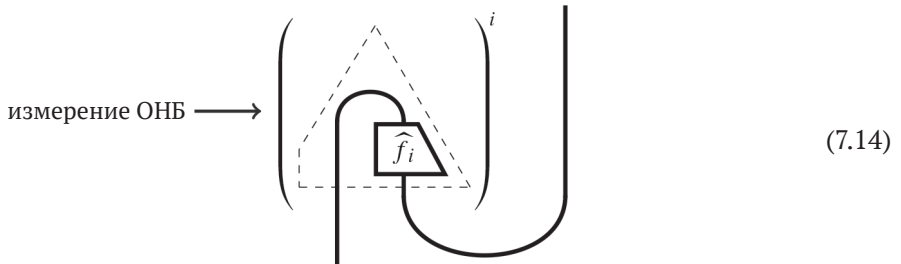
$$\begin{array}{c} \text{T} \\ \triangle \\ 0 \end{array} + \begin{array}{c} \text{T} \\ \triangle \\ 1 \end{array} = \underline{\underline{\text{T}}} = \begin{array}{c} \text{T} \\ \triangle \\ 0 \end{array} + \begin{array}{c} \text{T} \\ \triangle \\ 1 \end{array}$$

Теперь предположим, что имеется эффект \mathbf{e}_0 , который идентифицирует белое 0-состояние. Применив \mathbf{e}_0 к каждому состоянию в левой и правой частях, получим:

Но что в данном контексте означает слово «работа»? Здесь под работой понимается воздействие на системы, приводящее к радикальным, часто нелокальным изменениям. Употребление слова «радикальный» – отнюдь не преувеличение, учитывая, что физической системе для динамического эволюционного перехода из одного состояния в другое требуется время, тогда как изменения, вызванные измерением, происходят мгновенно. Мы увидим, что короткие отрезки запутывания могут мгновенно становиться длинными и что произвольные линейные отображения могут применяться мгновенно – и все это благодаря квантовым измерениям.

7.2.1. Индуцированная измерением динамика I: обратное действие

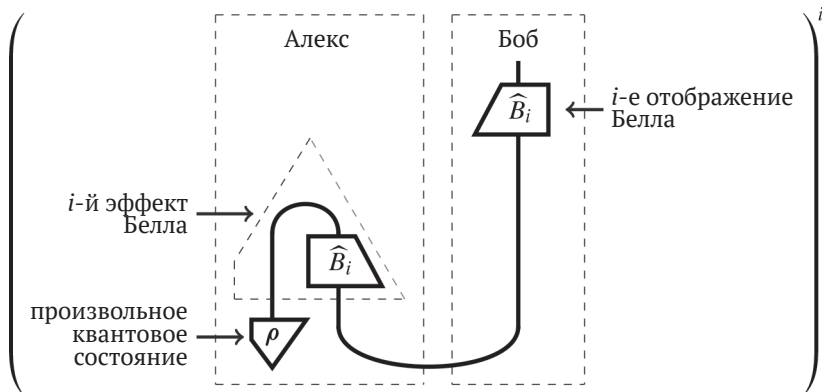
В примере из раздела 6.4.2 мы уже видели, как измерения ОНБ изменяют состояние системы полезными способами. Тогда мы использовали измерение ОНБ (теперь мы знаем, что это было именно оно), чтобы недетерминированно реализовать произвольное квантовое отображение:



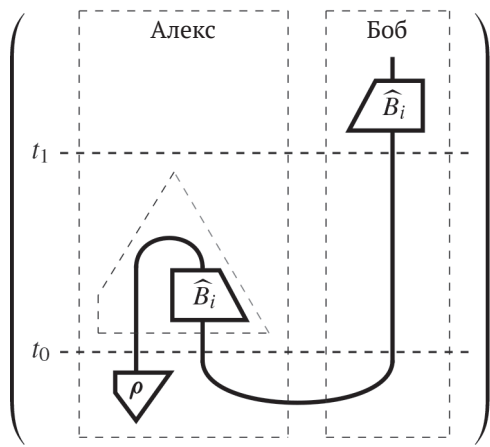
Аналогично в случае кубитов мы можем реализовать квантовую телепортацию с помощью *возмущающего измерения Белла*:



Так как все B_i унитарны, можно соответственно скорректировать ошибку:



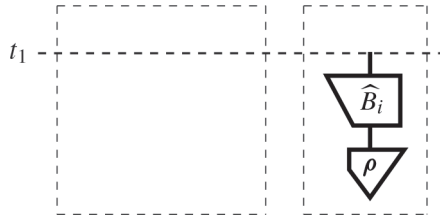
Разобьем это на более мелкие шаги и посмотрим, как состояние изменяется со временем. При выполнении измерения полное состояние в моменты t_0 и t_1 на этой диаграмме



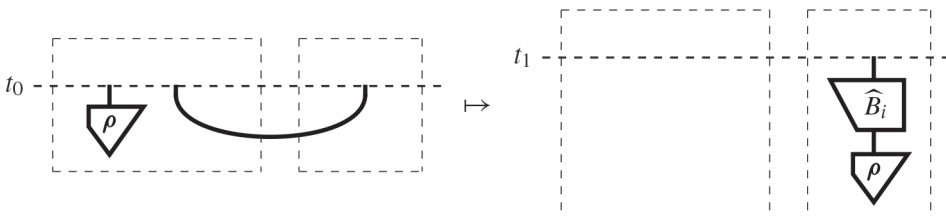
изменяется радикально. В момент t_0 имеем:



а в момент t_1 :



То есть имеет место мгновенный переход

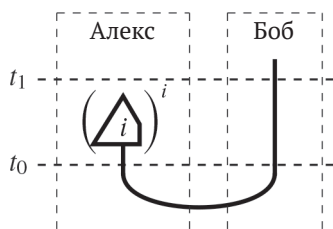


когда состояние ρ «перескакивает» от Алекса к Бобу и возникает ошибка.

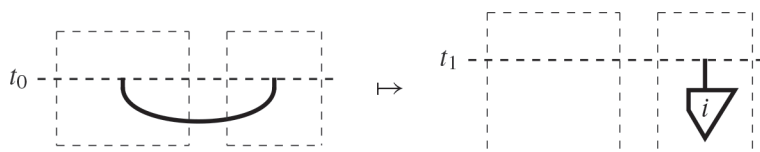
Однако в разделе 6.3.2 мы уже узнали, что благодаря тонкому акту балансирования между квантовой теорией и теорией относительности подобные мгновенные

переходы невозможно использовать для передачи сигнала со скоростью, большей скорости света. Тем не менее они обеспечивают возможность телепортации и, как мы скоро увидим, очень полезны и для других вещей.

Описанный выше сценарий не самое простое проявление феномена мгновенного перехода. Более простой вариант, в котором участвуют всего две системы, состоит из измерения ОНБ, выполняемого для одной из двух систем в состоянии Белла:



Тогда мы имеем следующий мгновенный переход:



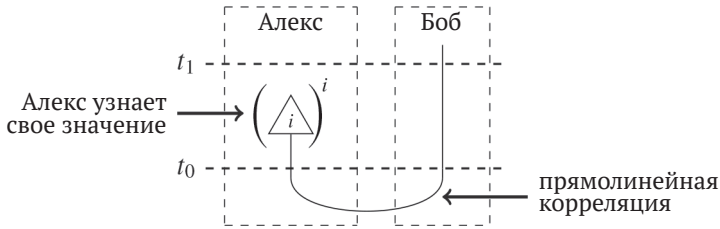
Здесь исход измерения Алекса определяет результирующее состояние Боба. Поэтому сам факт выполнения измерения изменяет состояние системы настолько радикально, что любой наблюдаемый Алексом эффект оказывается состоянием на стороне Боба.

Определение 7.12. Мгновенный переход, вызванный возмущающим измерением части составной системы, называется его *обратным действием*.

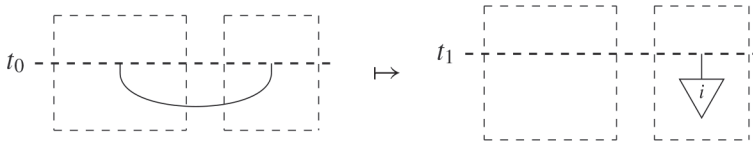
Мы употребляем термин «обратное действие» (backaction), потому что складывается впечатление, будто влияние измерения распространяется обратно во времени, согласно порядку «логического прочтения» диаграмм, который обсуждался в разделе 4.4.3. Важно, что это индуцированное измерением обратное действие – не просто «незначительный аспект» динамики, а целая умопомрачительная динамика, у которой нет аналогов ни в какой другой области физики!

Тем не менее мы можем сравнить эту ситуацию с куда менее удивительной, возникающей в классической теории вероятностей. Теорию вероятностей можно рассматривать как способ моделирования наших знаний о системе. Стоит некоторой части системы (например, какой-то случайной величине) стать известной, как это может привести к глобальному изменению наших знаний о системе (например, когда эта величина коррелирует с другими). Такое изменение состояния наших знаний называется *байесовским выводом*.

Рассмотрим ситуацию, аналогичную встретившейся в примере 4.91, когда у Алекса и Боба имеется по запечатанному конверту, содержащему одно и то же сообщение, случайно выбранное из множества возможных сообщений $\{1, \dots, n\}$. Тогда открывание Алексом своего конверта можно трактовать как недетерминированный процесс:



Поскольку содержимое обоих конвертов совпадает, то содержимое конверта Боба становится известно в тот момент, когда Алекс выполняет свой процесс «измерения»:

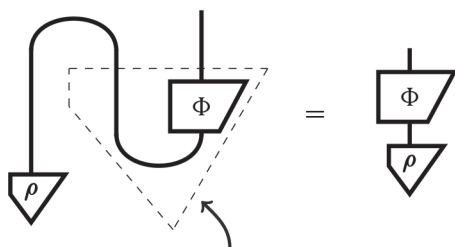


Однако принципиальная разница между квантовой теорией и классической теорией вероятностей заключается в том, что во втором случае изменяется только наше знание о содержимом конверта, а не само содержимое. С другой стороны, в квантовой теории, согласно стандартной концепции, изменяется само (чистое) состояние системы, а не просто наше знание о нем. Многие ученые пытались дать похожее объяснение для квантового случая в терминах знания. Однако в разделе 11.1 мы покажем, что квантовая нелокальность запрещает любой такой модели быть *локальной*. Иными словами, между Алексом и Бобом что-то должно происходить мгновенно, даже если они далеко друг от друга.

7.2.2. Пример: вентиляная телепортация

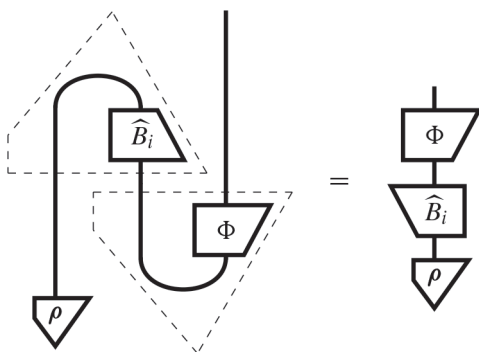
В телепортации обратное действие измерения ОНБ используется для передачи состояния из одного места в другое в неизменном виде, т. е. путем применения к нему тождественного процесса. А нельзя ли примерить к этому состоянию какое-нибудь другое квантовое отображение Φ ? Иначе говоря, можно ли закодировать все «вычисление» в квантовом состоянии, а затем «выполнить» это вычисление посредством всего лишь измерения? Поразительно, но ответ утвердительный, хотя требуется некоторая изобретательность.

Ключ к решению этой проблемы – двойственность процессов и состояний. Квантовое отображение Φ можно закодировать как двухкомпонентное состояние. Затем мы можем модифицировать протокол квантовой телепортации, воспользовавшись этим двухкомпонентным состоянием вместо состояния Белла:

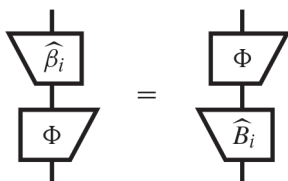


квантовое отображение Φ закодировано как двухкомпонентное состояние

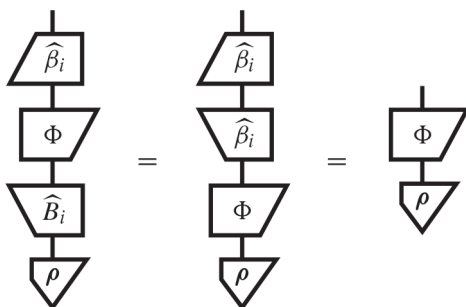
С учетом ошибки это равенство принимает вид:



Таким образом, мы почти применили квантовое отображение Φ , закодированное в квантовом состоянии. Но есть небольшая проблема: ошибка \widehat{B}_i застряла позади Φ , поэтому напрямую ее исправить нельзя. Однако если существует другой унитарный процесс $\widehat{\beta}_i$ такой, что:



ТО МЫ СНОВА НА КОНЕ:

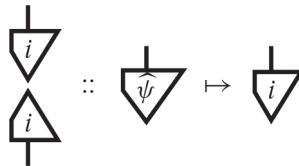


Может показаться, что это серьезное ограничение на то, какие отображения можно реализовать таким образом, но в действительности этого приема достаточно, чтобы породить универсальную квантовую вычислительную модель, называемую *квантовым вычислением, основанным на измерениях*, в которой «динамика» индуцирована всецело измерениями. В разделе 12.3 мы точно опишем, как работает эта модель вычислений.

7.2.3. Индуцированная измерением динамика II: коллапс

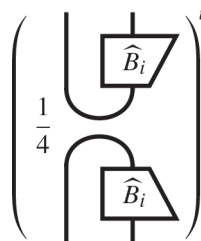
По сравнению с возмущающими, невозмущающие измерения ОНБ демонстрируют два вида индуцированной измерением динамики:

- обратное действие, обсуждавшееся в разделе 7.2.1, и
- *коллапс*, который мы видели в (7.7):



и который можно было бы назвать «прямым действием».

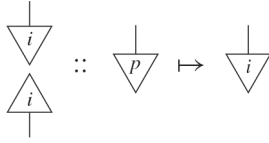
Например, *невозмущающее измерение Белла*



имеющее такое же обратное действие, как его возмущающая версия, приводит к тому, что две незапутанные системы становятся одной запутанной (числа снова игнорируются):

(7.16)

Как мы знаем, обратному действию есть аналог в классической теории вероятностей, и то же самое справедливо для коллапса. В классической теории вероятностей коллапс



просто означает, что ранее неизвестное содержимое конверта (т. е. выбираемое из какого-то распределения вероятностей p) становится известным (т. е. точкой i в распределении вероятностей). Как и в случае обратного действия, в момент коллапса не изменилось ничего, кроме нашего знания, тогда как в квантовом случае коллапс куда более разрушителен. Например, подумайте, что произойдет, если после открывания запечатанного конверта мы решим снова запечатать его и забыть, какое значение видели. Забывание исхода недетерминированного процесса просто соответствует смешиванию ветвей:

$$\left(\begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \end{array} \right)^i \mapsto \sum_i \begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \end{array} = \left| \right. \quad (7.17)$$

Поскольку наше знание не изменилось, не меняется ничего. Но если то же самое проделать для квантового измерения, получится нечто совершенно иное:

$$\left(\begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \end{array} \right)^i \mapsto \sum_i \begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \end{array} \neq \left| \right. \quad (7.18)$$

Результирующий квантовый процесс переводит любое квантовое состояние в смесь базисных состояний. В частности, чистое состояние $\hat{\psi}$ действительно становится смесью базисных состояний:

$$\sum_i \begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \\ \triangle \hat{\psi} \\ \downarrow \end{array} = \sum_i \begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle \hat{\psi} \\ \downarrow \end{array} \triangle i$$

с соответствующими вероятностями в качестве весов. Процесс

$$\sum_i \begin{array}{c} \downarrow \\ \triangle i \\ \uparrow \\ \triangle i \\ \downarrow \end{array}$$

называется *декогеренцией*, мы будем подробно изучать его в разделе 8.3.2, когда приведем для него простое (не содержащее сумм) диаграммное представление.

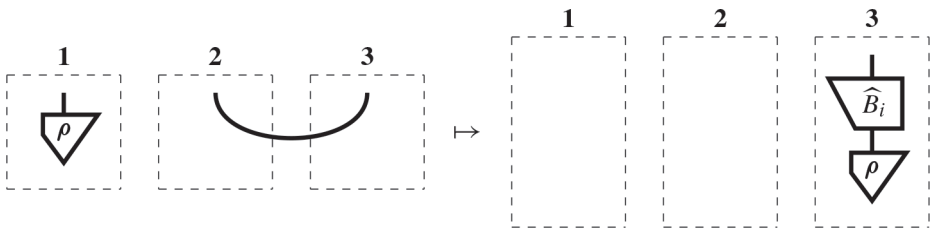
Упражнение 7.13. Покажите, что декогеренция не является тождественным процессом, для чего запишите тот и другой в виде суммы состояний, принадлежащих ОНБ.

Несмотря на свое разрушительное воздействие на квантовые состояния, коллапс может быть весьма полезен. Одно из его применений – *подготовка состояния*, когда состояние $\hat{\psi}$ получается просто путем измерения ОНБ, для которого состояние $\hat{\psi}$ является одним из возможных состояний исхода. Если выполнить такое измерение достаточно много раз в состоянии, для которого возможно состояние исхода $\hat{\psi}$, то в какой-то момент получится состояние $\hat{\psi}$. Именно так, например, поляризационный фильтр дает поляризованный свет.

Далее мы рассмотрим протокол, в котором используется как обратное действие, так и коллапс невозмущающего измерения базиса Белла.

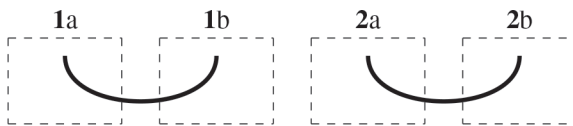
7.2.4. Пример: перекоммутация запутывания

В разделе 7.2.1 мы видели, что телепортация зависит от обратного действия (возмущающего) измерения базиса Белла. То есть когда измерение применяется к системам **1** и **2**:

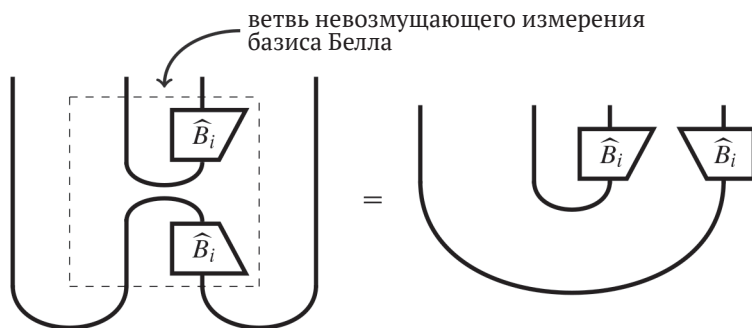


ρ сдвигается из системы **1** в систему **3**, несмотря на то что на систему **3** не оказывалось прямого воздействия (разве что позже, для корректировки). Мы также видели в (7.16), что прямое действие невозмущающего измерения Белла позволяет запутать две системы, которые до того не были запутаны.

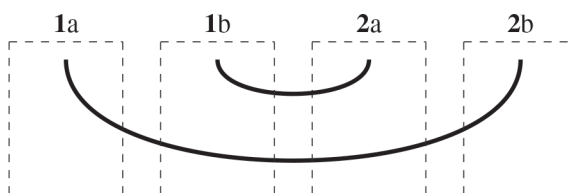
Попробуем объединить обе идеи. Начнем с пары состояний Белла:



и применим невозмущающее измерение базиса Белла к системам **1b** и **2a**. Тогда получится следующее состояние:



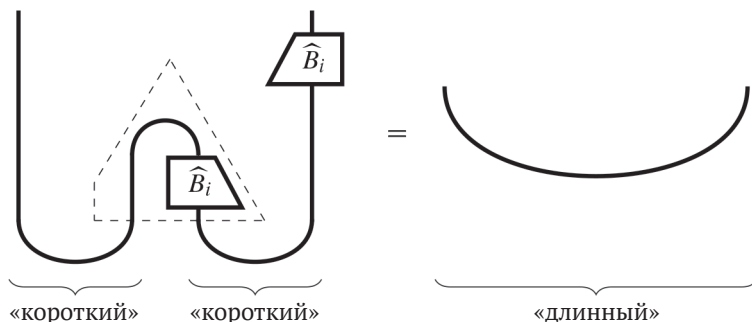
После необходимых корректировок остается вот что:



Хотя первоначально система **1a** была запутана с **1b**, а **2a** с **2b**, в конечном состоянии **1a** запутана с **2b**, а **1b** с **2a**. Иными словами, запутывания «поменялись местами». Мы называем эту процедуру *перекоммутацией запутывания*. Удивительно, что **1a** стала запутанной с **2b**, хотя на эти системы не оказывалось совместного воздействия, т. е. квантовая теория допускает

запутывание без прикосновения.

На практике эта процедура используется в квантовых технологиях, чтобы создать запутывание на большом расстоянии, при условии что в нашем распоряжении имеются запутанные состояния на меньших расстояниях:



Устройство, осуществляющее перекоммутацию запутывания для этой конкретной цели, иногда называют *квантовым повторителем*, оно совершенно необходимо для создания высококачественных запутанных состояний на больших расстояниях. Повторителем оно называется по аналогии с классическими повто-

рителями сигналов, которые позволяют посылать сообщения на дальнее расстояние посредством перехвата сигнала и «повторной» передачи его в усиленном виде в линию передачи.

Упражнение 7.14. Пусть дано n коротких отрезков запутывания. Спроектируйте протокол, который порождает «длинный» отрезок запутывания, минимизируя в то же время количество необходимых корректировок.

Замечание 7.15. Протокол телепортации улавливает суть определяющего равенства струнных диаграмм:

$$\text{Cup} \text{---} \text{Cap} \text{---} \text{Line} = \text{Line}$$

которое включает чашку и крышку в левой части, а перекоммутация запутывания – следующий шаг. Она отражает равенство, содержащее три чашки (крышки) в левой части:

$$\text{Cup} \text{---} \text{Cup} \text{---} \text{Cup} = \text{Cup}$$

7.3. БОЛЕЕ ОБЩИЕ ВИДЫ ИЗМЕРЕНИЯ

В этом разделе мы поговорим о более общих видах измерений, которые возникают, если рассматривать измерения ОНБ в более широком контексте процессной теории. Например, что случится, если измерить лишь одну подсистему квантового состояния или произвести композицию измерения ОНБ с другими процессами?

7.3.1. Измерения фон Неймана

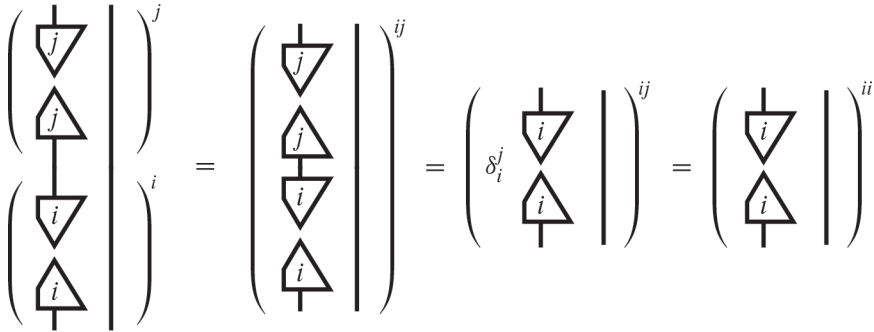
Рассмотрим квантовый процесс, полученный, когда для одной системы выполняется невозможное измерение ОНБ, а для другой не делается ничего:

$$\left(\begin{array}{c} \text{Triangle } i \\ \text{Triangle } i \end{array} \right) \text{---} \text{Line} = \left(\text{Triangle } i \right) \text{---} \text{Line}$$

Сам этот процесс не может быть измерением ОНБ просто потому, что его ветви не \circ -разделимы:

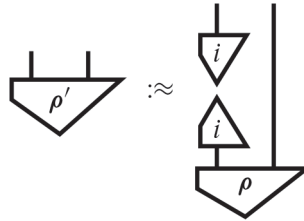
$$\left(\begin{array}{c} \text{Triangle } i \\ \text{Triangle } i \end{array} \right) \text{---} \text{Line} \neq \left(\widehat{\text{Triangle } \phi_i} \right) \text{---} \text{Line}$$

Однако он обладает важной характеристикой измерения ОНБ, что станет заметно, если выполнить этот процесс дважды:

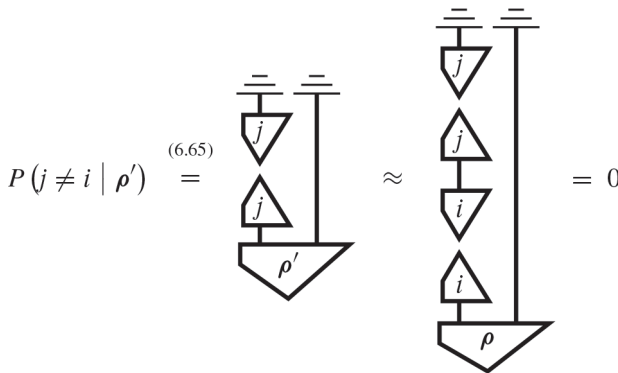


Мы могли здесь положить $i = j$, потому что для $i \neq j$ получается невозможный процесс, который, конечно же, никогда не произойдет. Следовательно, два последовательных процесса дают один и тот же исход, т. е. итог такой же, как если бы мы выполнили этот процесс только один раз.

Полезно посмотреть, что происходит при применении этих процессов к состоянию. Допустим, что мы выполнили процесс для состояния ρ и получили исход i . Тогда новым состоянием будет



Если затем сразу же применить этот же процесс еще раз, то вероятность всех ветвей, для которых $j \neq i$, равна 0:



поэтому мы гарантированно получим исход i снова. И не имеет значения, сколько раз выполнить этот процесс: 1, 2 или 100. После первого же измерения ущерб уже причинен, поэтому в дальнейшем состояние не меняется.

Идею о том, что процесс может привести к такому «коллапсу» состояния, при котором повторение процесса всегда дает один и тот же результат, фон Нейман считал характерной особенностью квантовых измерений и формулировал следующий

Постулат редукции фон Неймана. После того как выполнено невозмущающее измерение и получен исход i , повторное измерение дает тот же самый исход с вероятностью 1 и не влияет на состояние системы.

Это можно выразить на языке квантовых процессов.

Определение 7.16. Измерением фон Неймана (невозмущающим) называется квантовый процесс:

$$\left(\begin{array}{c} | \\ \hline \hat{P}_i \\ \hline | \end{array} \right)^i$$

такой, что

$$\begin{array}{c} \hat{P}_j \\ \hline \hat{P}_i \\ \hline | \end{array} = \delta_{ij} \begin{array}{c} \hat{P}_i \\ \hline | \end{array} \tag{7.19}$$

Измерения фон Неймана иногда называют *проекционными измерениями* по следующей причине.

Предложение 7.17. Для любого измерения фон Неймана ветви \hat{P}_i являются проекторами.

Доказательство. Из (7.19) мы уже знаем, что ветви \hat{P}_i идемпотентны, поэтому остается только показать, что они самоадьюнкты. Совокупный набор квантовых отображений \hat{P}_i образует квантовый процесс, поэтому он является каузальным. Раскрывая условие каузальности, получаем:

$$\sum_i \left(\begin{array}{c} \\ \hline P_i \quad P_i \\ \hline \end{array} \right) = \left(\begin{array}{c} \\ \hline \quad \\ \hline \end{array} \right)$$

откуда

$$\sum_i \left(\begin{array}{c} | \\ \hline P_i \\ \hline P_i \\ \hline | \end{array} \right) = | \tag{7.20}$$

По теореме 6.17, дублированные равенства (7.19) можно заменить недублированными с точностью до глобальной фазы $e^{i\alpha_{jk}}$ для всех значений j и k :

$$\begin{array}{c} \diagup \\ P_k \\ \diagdown \\ \diagup \\ P_j \\ \diagdown \end{array} = e^{i\alpha_{jk}} \delta_j^k \begin{array}{c} \diagup \\ P_j \\ \diagdown \end{array} \quad (7.21)$$

Поэтому

$$\begin{array}{c} \diagup \\ P_j \\ \diagdown \end{array} \stackrel{(7.20)}{=} \sum_k \begin{array}{c} \diagup \\ P_k \\ \diagdown \\ \diagup \\ P_k \\ \diagdown \\ \diagup \\ P_j \\ \diagdown \end{array} \stackrel{(7.21)}{=} \sum_k e^{i\alpha_{jk}} \delta_j^k \begin{array}{c} \diagup \\ P_k \\ \diagdown \\ \diagup \\ P_j \\ \diagdown \end{array} = e^{i\alpha_{jj}} \begin{array}{c} \diagup \\ P_j \\ \diagdown \\ \diagup \\ P_j \\ \diagdown \end{array}$$

Дублирование устраняет глобальную фазу:

$$\begin{array}{c} \diagup \\ \widehat{P}_i \\ \diagdown \end{array} = \begin{array}{c} \diagup \\ \widehat{P}_i \\ \diagdown \\ \diagup \\ \widehat{P}_i \\ \diagdown \end{array}$$

Следовательно, по предложению 4.70, каждое отображение \widehat{P}_i является проектором. □

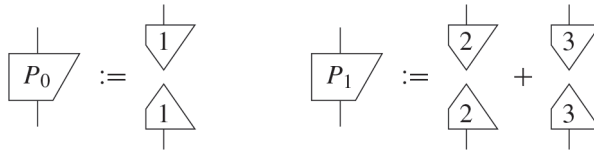
Проекторы называются *ортогональными* именно потому, что удовлетворяют условию (7.19), поэтому с тем же успехом измерение фон Неймана можно было бы определить как квантовый процесс, состоящий из взаимно ортогональных проекторов. Кроме того, поскольку мы имеем дело с проекторами, условие каузальности (7.20) упрощается – исходные проекторы (см. предложение 6.21) должны образовывать разрешение единицы:

$$\sum_i \begin{array}{c} \diagup \\ P_i \\ \diagdown \end{array} = \left| \right.$$

Альтернативно измерение фон Неймана можно получить из измерения ОНБ, объединив исходы нескольких измерений в один, т. е. произведя *огрубление*. Например, предположим, что имеется трехмерная квантовая система, тогда, быть может, вместо измерения, призванного показать, в каком из трех состояний



находится система, мы сможем придумать измерение, проверяющее, находится ли система в состоянии 1. Это можно сделать, зафиксировав проекторы



а затем измерив

$$\left(\begin{array}{c} \downarrow \\ \boxed{\hat{P}_i} \\ \downarrow \end{array} \right)^i \tag{7.22}$$

Вообще, зафиксируем любое разбиение множества исходов:

$$I := \{1, \dots, D\},$$

т. е. набор подмножеств I :

$$\{I_1, \dots, I_n\}$$

удовлетворяющий условиям

$$I_1 \cup \dots \cup I_n = I \quad \text{и} \quad \forall i \neq j : I_i \cap I_j = \emptyset.$$

Тогда измерение фон Неймана можно получить следующим образом:

$$\left(\begin{array}{c} \downarrow \\ \boxed{\hat{P}_i} \\ \downarrow \end{array} \right)^i, \quad \text{где} \quad \begin{array}{c} \downarrow \\ \boxed{P_i} \\ \downarrow \end{array} := \sum_{j \in I_i} \begin{array}{c} \downarrow \\ \downarrow \\ j \\ \downarrow \\ \downarrow \\ j \\ \downarrow \end{array} \tag{7.23}$$

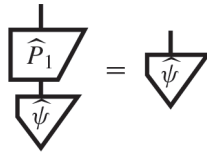
Очевидно, что все \hat{P}_i являются проекторами, а их взаимная ортогональность следует из того, что множества I_i не пересекаются.

Упражнение 7.18. Покажите, что для любого разбиения ОНБ (7.23) является квантовым процессом и, следовательно, измерением фон Неймана. Обратно, пользуясь спектральной теоремой из раздела 5.3.3.1, покажите, что любое измерение фон Неймана можно выразить в виде (7.23) для некоторого разбиения ОНБ.

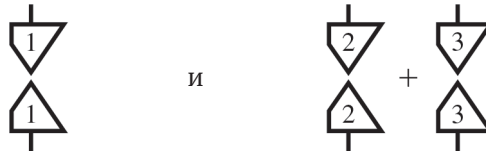
Огрубленное измерение сообщает меньше, чем измерение ОНБ, но и наносит меньший ущерб. Например, любое состояние вида

$$\begin{array}{c} \downarrow \\ \psi \\ \downarrow \end{array} = \text{double} \left(\lambda_2 \begin{array}{c} \downarrow \\ 2 \\ \downarrow \end{array} + \lambda_3 \begin{array}{c} \downarrow \\ 3 \\ \downarrow \end{array} \right)$$

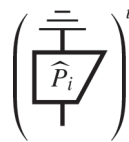
сохраняется измерением (7.22), потому что \widehat{P}_0 никогда не произойдет и



Это объясняется тем, что мы намеренно производили огрубление на уровне недублированных процессов P_i . Если бы вместо этого мы выполнили квантовый процесс, состоящий из



то $\widehat{\psi}$ не переходило бы даже в чистое состояние (если только λ_2 или λ_3 не равны 0), а не то что в себя. С другой стороны, если рассмотреть *возмущающее измерение фон Неймана*, т. е. квантовые процессы вида:

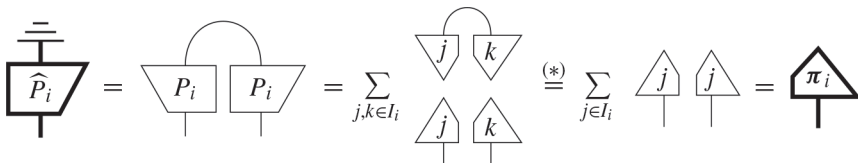


для которых выполняется условие (7.19), то это различие исчезает. Следовательно, в отличие от возмущающих измерений ОНБ, ветви возмущающего измерения фон Неймана не обязаны быть чистыми.

Предложение 7.19. Квантовый процесс является возмущающим измерением фон Неймана тогда и только тогда, когда он имеет вид:



Доказательство. Пусть проекции P_i определены как в (7.23). Тогда



где в равенстве, помеченном (*), мы воспользовались ортонормированностью базисных состояний. □

И последнее: как для возмущающих, так и для невозмущающих измерений фон Неймана это огрубление не единственно. То есть одно и то же измерение фон Неймана можно получить путем огрубления различных ОНБ.

Упражнение 7.20. Для ОНБ

$$:= \left\{ \begin{array}{c} | \\ \hline \triangle \\ \hline 1 \end{array}, \begin{array}{c} | \\ \hline \triangle \\ \hline 2 \end{array}, \begin{array}{c} | \\ \hline \triangle \\ \hline 3 \end{array}, \dots, \begin{array}{c} | \\ \hline \triangle \\ \hline D \end{array} \right\}$$

положим:

$$\begin{array}{c} | \\ \hline \triangle \\ \hline + \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle \\ \hline 1 \end{array} + \begin{array}{c} | \\ \hline \triangle \\ \hline 2 \end{array} \right) \quad \text{и} \quad \begin{array}{c} | \\ \hline \triangle \\ \hline - \end{array} = \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \hline \triangle \\ \hline 1 \end{array} - \begin{array}{c} | \\ \hline \triangle \\ \hline 2 \end{array} \right)$$

Для получения другого ОНБ:

$$\mathcal{B}' := \left\{ \begin{array}{c} | \\ \hline \triangle \\ \hline + \end{array}, \begin{array}{c} | \\ \hline \triangle \\ \hline - \end{array}, \begin{array}{c} | \\ \hline \triangle \\ \hline 3 \end{array}, \dots, \begin{array}{c} | \\ \hline \triangle \\ \hline D \end{array} \right\}$$

Покажите, что

$$\begin{array}{c} | \\ \hline \triangle \\ \hline + \end{array} + \begin{array}{c} | \\ \hline \triangle \\ \hline - \end{array} = \begin{array}{c} | \\ \hline \triangle \\ \hline 1 \end{array} + \begin{array}{c} | \\ \hline \triangle \\ \hline 2 \end{array}$$

и, следовательно, измерение

$$\left(\begin{array}{c} \triangle \\ \hline | \\ \hline 1 \end{array} + \begin{array}{c} \triangle \\ \hline | \\ \hline 2 \end{array}, \begin{array}{c} \triangle \\ \hline | \\ \hline 3 \end{array}, \dots, \begin{array}{c} \triangle \\ \hline | \\ \hline D \end{array} \right)$$

получается путем огрубления измерений ОНБ \mathcal{B} или \mathcal{B}' . Сможете ли вы охарактеризовать все ОНБ, огрублением которых получается это измерение?

7.3.2. Квантовый формализм фон Неймана

Измерения фон Неймана лежат в основе квантового формализма в том виде, в каком он до сих пор описывается в большинстве учебников, т. е. совершенно отличным от нашего изложения. Прежде всего обычно различают *квантовую теорию чистых состояний* и *квантовую теорию смешанных состояний*. Чистые состояния считаются примитивами, а смешанные – (факультативным) производным понятием. Квантовая теория чистых состояний опирается на три постулата.

Постулат 1: системы. *Квантовая система* представляется гильбертовым пространством. *Состояние* квантовой системы тогда соответствует классу эквивалентности нормированных векторов, равных с точностью до глобальной фазы (см. раздел 6.1.2). *Составные системы* представляются тензорным произведением гильбертовых пространств, представляющих подсистемы (см. раздел 5.4.2).

Постулат 2: эволюция. Детерминированные обратимые квантовые процессы представляются унитарными отображениями гильбертова пространства (см. следствие 6.58).

Постулат 3: измерения. Квантовые измерения представляются самоадьюнктными линейными отображениями гильбертова пространства.

Однако минуточку. Третий постулат совсем не похож на то, что мы называли измерением, а уж тем более на измерение фон Неймана, которое, по идее, должно быть сердцевинной формализма фон Неймана. Но, применив спектральную теорему (раздел 5.3.3.1), мы увидим, что различия не так уж велики. Начав с измерения фон Неймана, мы сможем обернуть набор проекторов одним отображением:

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline f \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} = \sum_i r_i \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline P_i \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \quad (7.24)$$

где r_i – различные вещественные числа. Получающееся отображение самоадьюнктное, и мы всегда можем восстановить проекторы P_i , поскольку спектральная теорема гарантирует существование такого ОНБ, что:

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline f \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} = \sum_i r_i \begin{array}{|c} \hline i \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline i \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array}$$

В общем случае некоторые r_i могут повторяться. Это индуцирует разбиение $\{I_1, \dots, I_n\}$, в котором каждому уникальному r_i соответствует множество I_i . Затем мы можем воспользоваться (7.23), чтобы восстановить разложение (7.24).

Пример 7.21. Отображения Паули

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_X \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_Y \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_Z \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

матрицы которых впервые встретились нам в замечании 5.99, являются самоадьюнктными линейными отображениями, представляющими измерения для X-базиса, Y-базиса (см. упражнение 6.7) и Z-базиса соответственно:

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_X \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline 0 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 0 \\ \hline \end{array} + (-1) \begin{array}{|c} \hline 1 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 1 \\ \hline \end{array}$$

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_Y \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline 0 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 0 \\ \hline \end{array} + (-1) \begin{array}{|c} \hline 1 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 1 \\ \hline \end{array}$$

$$\begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline \sigma_Z \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline 0 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 0 \\ \hline \end{array} + (-1) \begin{array}{|c} \hline 1 \\ \hline \end{array} \begin{array}{|c} \hline \\ \hline \end{array} \begin{array}{|c} \hline 1 \\ \hline \end{array}$$

Таким образом, результирующее самоадъюнктное линейное отображение следует рассматривать не как процесс сам по себе, а как способ представления настоящих процессов, т. е. проекторов.

Постулат 3: измерения (продолжение). После измерения состояние системы изменяется (т. е. «коллапсирует») под действием одного из проекторов, причем вероятность выбора конкретного проектора определяется правилом Борна:

$$P(i | \hat{\psi}) := \begin{array}{c} \overline{\overline{}} \\ \hat{P}_i \\ \downarrow \\ \hat{\psi} \end{array} = \begin{array}{c} \text{---} \\ P_i \quad P_i \\ \downarrow \quad \downarrow \\ \psi \quad \psi \end{array} \stackrel{(*)}{=} \begin{array}{c} \psi \\ \downarrow \\ P_i \\ \downarrow \\ \psi \end{array} \quad (7.25)$$

где равенство, помеченное (*), следует из того, что P_i – проектор.

Замечание 7.22. В случае нечистых состояний правило Борна принимает вид:

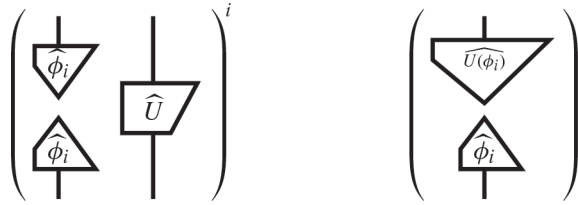
$$P(i | \rho) := \begin{array}{c} \overline{\overline{}} \\ \hat{P}_i \\ \downarrow \\ \rho \end{array} = \begin{array}{c} \text{---} \\ P_i \quad P_i \\ \downarrow \quad \downarrow \\ g \quad g \end{array} \stackrel{(*)}{=} \begin{array}{c} \text{---} \\ P_i \\ \downarrow \\ \tilde{\rho} \end{array}$$

где $\tilde{\rho} := g \circ g^\dagger$ – оператор плотности, ассоциированный с ρ (см. замечание 6.43). В более традиционной нотации вероятности, которые правило Борна дает для чистых и смешанных состояний соответственно, равны:

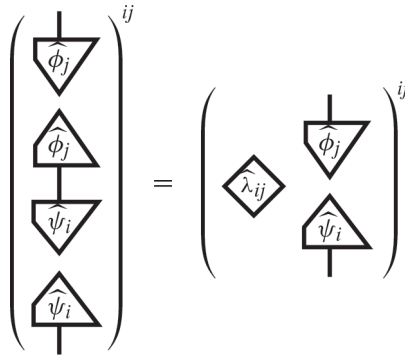
$$\langle \psi | P_i | \psi \rangle \quad \text{и} \quad \text{tr}(P_i \tilde{\rho}).$$

В этой формулировке чистой квантовой теории самое примечательное то, что унитарные отображения и измерения фон Неймана выделены как очень специальные процессы. Одна из причин выделения унитарных отображений – теорема о дилатации Стайнспринга в форме следствия 6.63, которая утверждает, что любой детерминированный квантовый процесс можно реализовать с помощью состояния, унитарного отображения и отбрасывания. Более того, в следующем разделе мы увидим, что можно реализовать все квантовые процессы, если дополнительно включить в рассмотрение измерения ОНБ (см. раздел 7.3.4).

С другой стороны, чтобы получить квантовую процессную теорию, мы обязаны рассматривать не только унитарные отображения и измерения фон Неймана, но и более общие процессы, потому что эти операции попросту не замкнуты относительно композиции. Например, параллельная композиция состояния и унитарного отображения дает изометрию. Аналогично композиция – последовательная или параллельная – невозмущающего измерения фон Неймана с унитарным отображением дает квантовый процесс, уже не являющийся измерением фон Неймана, например:



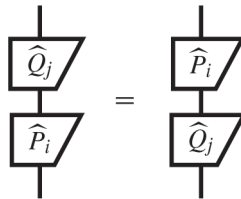
Кроме того, результатом последовательной композиции двух невозмущающих измерений фон Неймана обычно не является измерение фон Неймана. Например, композиция двух разных измерений ОНБ дает:



Упражнение 7.23. Докажите, что результатом последовательной композиции двух невозмущающих измерений фон Неймана



снова является измерение фон Неймана тогда и только тогда, когда измерения коммутируют, т. е. для любых i и j имеет место равенство



Поэтому справедлива

Теорема 7.24. Формулировка квантовой теории фон Неймана не замкнута относительно построения диаграмм. В частности, она не замкнута относительно параллельной и последовательной композиций процессов.

Замечание 7.25. Одно из преимуществ представления измерений фон Неймана как самоадьюнктных линейных отображений заключается в том, что в качестве чисел r_i можно взять реальные физические величины, ассоциированные с проектором, например положение или импульс. Если заменить P_i в правой части (7.25) самоадьюнктным линейным отображением

$$\begin{array}{|c} \hline f \\ \hline \end{array} := \sum_i r_i \begin{array}{|c} \hline P_i \\ \hline \end{array}$$

вместо вероятности, то получим взвешенное среднее чисел r_i :

$$E_f(\hat{\psi}) := \begin{array}{|c} \hline \psi \\ \hline \begin{array}{|c} \hline f \\ \hline \end{array} \\ \hline \psi \\ \hline \end{array} = \sum_i r_i \begin{array}{|c} \hline \psi \\ \hline \begin{array}{|c} \hline P_i \\ \hline \end{array} \\ \hline \psi \\ \hline \end{array} = \sum_i r_i P(i | \hat{\psi})$$

которое называется *ожидаемым значением*.

Замечание* 7.26. Фон Нейман рассматривал проекторы в гильбертовом пространстве как квантовый аналог более знакомого понятия «высказывания» из классической логики. Благодаря этой идее он стал сооснователем *квантовой логики*, которую мы рассмотрим в разделе* 7.6.2.

7.3.3. Измерения POVM

Самый общий вид возмущающих измерений – это просто произвольный квантовый процесс, отображающий в тривиальную систему, т. е. набор эффектов, ограниченный только условием совместной каузальности:

Определение 7.27. Любой квантовый процесс вида

$$\left(\begin{array}{|c} \hline \psi_i \\ \hline \end{array} \right)^i$$

называется *возмущающим измерением POVM*.

Аббревиатура «POVM» означает «positive operator-valued measure» – положительная операторная мера. Мы вкратце объясним смысл этого термина, поскольку это находится несколько в стороне от терминологии, используемой в книге.

- При чем тут «положительный оператор»? Если для проекционных измерений мы имеем

$$\begin{array}{|c} \hline \pi_i \\ \hline \end{array} = \begin{array}{|c} \hline \text{проектор} \\ \hline \begin{array}{|c} \hline P_i \\ \hline \end{array} \\ \hline \end{array}$$

то теперь имеем:

$$\begin{array}{c} \triangle \\ \uparrow \\ \varphi_i \end{array} = \begin{array}{c} \text{⊗-положительный} \\ \curvearrowright \\ \text{положительный} \end{array} \begin{array}{c} \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \\ f_i \\ \diagdown \\ \text{---} \\ \diagup \end{array} \quad (7.26)$$

Так что это всего лишь дань тому факту, что элементы этого квантового процесса представляются положительными операторами, или положительными линейными отображениями.

- А почему «мера»? В теории вероятностей конечной «вероятностной мерой» называется сопоставление положительных чисел $P(i)$ каждому элементу $i \in \{1, \dots, D\}$ конечного множества таким образом, что сумма всех этих чисел равна 1. «Положительная операторная мера» – обобщение этого понятия в том смысле, что каждому i сопоставляется положительное отображение, так что сумма этих отображений – тождественное отображение. Иными словами, это просто означает каузальность, поскольку мы имеем:

$$\sum_i \begin{array}{c} \curvearrowright \\ \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \\ f_i \\ \diagdown \\ \text{---} \\ \diagup \end{array} = \curvearrowright \iff \sum_i \begin{array}{c} \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \\ f_i \\ \diagdown \\ \text{---} \\ \diagup \end{array} = \text{---} \quad (7.27)$$

Замечание 7.28. Как и для измерений фон Неймана, мы можем записать правило Борна в терминах матрицы плотности и следа:

$$P(i | \rho) = \begin{array}{c} \triangle \\ \uparrow \\ \varphi_i \\ \text{---} \\ \rho \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ E_i \\ \diagup \\ \text{---} \\ \tilde{\rho} \\ \diagdown \\ \text{---} \\ \diagup \end{array} \quad (7.28)$$

где

$$E_i := \begin{array}{c} \text{---} \\ \diagdown \\ f_i \\ \diagup \\ \text{---} \\ f_i \\ \diagdown \\ \text{---} \\ \diagup \end{array} \quad (7.29)$$

В неграфической нотации (7.28) принимает вид:

$$P(i | \rho) = \text{Tr}(E_i \tilde{\rho}),$$

а это и есть правило Борна для POVM, встречающееся в стандартной литературе.

Мы можем также рассмотреть понятие «невозмущающего» измерения POVM, хотя оно и нестандартно. То есть берется семейство квантовых процессов такое, что можно получить любое возмущающее измерение POVM путем отбрасывания выхода. Такое семейство может быть получено с помощью очищения (см. раздел 6.4.3):

$$\left(\begin{array}{c} \triangle \\ \varphi_i \\ \uparrow \end{array} \right)^i = \left(\begin{array}{c} \overline{\overline{\square}} \\ \widehat{f}_i \\ \uparrow \end{array} \right)^i$$

Таким образом, чтобы восстановить все возмущающие измерения POVM, достаточно рассмотреть только квантовые процессы с чистыми ветвями, так что фраза «невозмущающее измерение POVM» – просто синоним чистого квантового процесса:

$$\left(\begin{array}{c} \square \\ \widehat{f}_i \\ \uparrow \end{array} \right)^i$$

Замечание 7.29. Хотя ниже нам это и не потребуется, но для того чтобы процесс действительно можно было назвать невозмущающим измерением, отображения \widehat{f}_i должны иметь на выходе такой же системный тип, как на входе. Иначе говоря, для измерения POVM на \widehat{A} должна быть возможность выбрать \widehat{f}_i с выходным типом \widehat{A} :

$$\left(\begin{array}{c} \triangle \\ \varphi_i \\ \uparrow \widehat{A} \end{array} \right)^i = \left(\begin{array}{c} \overline{\overline{\square}} \\ \widehat{A} \\ \square \\ \widehat{f}_i \\ \uparrow \widehat{A} \end{array} \right)^i$$

В силу упражнения 6.97 это всегда возможно.

Разумеется, существует много невозмущающих измерений POVM, которые дают одно и то же возмущающее измерение POVM после отбрасывания выхода. Это следует из того, что существует много способов разложить φ_i , как в равенстве (7.26). Поэтому судьба квантового состояния зависит от самих \widehat{f}_i , а не только от φ_i . Отсюда можно сделать вывод, что многие невозмущающие измерения POVM могут породить одни и те же вероятности исходов, но при этом они по-разному воздействуют на саму квантовую систему.

7.3.4. Теоремы Наймарка и Озавы о дилатации

Теперь вспомним, что по теореме о дилатации Стайнспринга (см. теорему 6.61) любое каузальное квантовое отображение Φ (т. е. любой детерминированный квантовый процесс) получается из некоторой изометрии \widehat{U} путем отбрасывания одного из ее выходов:

$$\begin{array}{c} | \\ \hline \Phi \\ \hline | \end{array} = \begin{array}{c} | \\ \hline \hat{U} \\ \hline | \end{array} \quad (7.30)$$

Аналогичный результат о дилатации имеет место для измерений POVM. Мы уже упоминали, что с любым квантовым процессом можно однозначно ассоциировать изометрию. Сначала докажем это для чистых квантовых процессов, этот результат называется *теоремой Наймарка о дилатации*.

Лемма 7.30. Для любого чистого квантового процесса с D ветвями

$$\left(\begin{array}{c} | \\ \hline \hat{f}_i \\ \hline | \end{array} \right)^i$$

и для любого ОНБ с D базисными состояниями

$$\left\{ \begin{array}{c} | \\ \hline i \\ \hline | \end{array} \right\}_i$$

следующее отображение является изометрией:

$$\begin{array}{c} | \\ \hline U \\ \hline | \end{array} := \sum_i \begin{array}{c} | \\ \hline f_i \\ \hline | \end{array} \begin{array}{c} | \\ \hline i \\ \hline | \end{array}$$

а значит, изометрией является и квантовое отображение, полученное его дублированием.

Доказательство. Имеем:

$$\begin{array}{c} \sum_j \begin{array}{c} | \\ \hline f_j \\ \hline | \end{array} \begin{array}{c} | \\ \hline j \\ \hline | \end{array} \\ \sum_i \begin{array}{c} | \\ \hline f_i \\ \hline | \end{array} \begin{array}{c} | \\ \hline i \\ \hline | \end{array} \end{array} = \sum_i \begin{array}{c} | \\ \hline f_i \\ \hline | \end{array} \begin{array}{c} | \\ \hline f_i \\ \hline | \end{array} = \left| \right.$$

где последнее равенство справедливо в силу каузальности, как в (7.27). □

Теорема 7.31 (Наймарка о дилатации). Любое неразрушающее измерение POVM получается как изометрия \hat{U} , одним из выходов которой является измерение ОНБ.

$$\left(\begin{array}{c} | \\ \hline \hat{f}_i \\ \hline | \end{array} \right)^i = \begin{array}{c} | \\ \hline \hat{U} \\ \hline | \end{array} \begin{array}{c} | \\ \hline i \\ \hline | \end{array} \quad (7.31)$$

Следовательно, любое разрушающее измерение POVM получается как изометрия \hat{U} , один из выходов которой отбрасывается, а другим является измерение ОНБ:

$$\left(\begin{array}{c} \triangle \\ \varphi_i \\ \uparrow \end{array} \right)^i = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \hat{U} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \left(\begin{array}{c} \triangle \\ i \\ \uparrow \end{array} \right)^i \quad (7.32)$$

Доказательство. Для изометрии, построенной в лемме 7.30, получаем:

$$\begin{array}{c} \triangle \\ j \\ \uparrow \\ U \\ \text{---} \end{array} = \sum_i \begin{array}{c} \triangle \\ j \\ \uparrow \\ f_i \\ \text{---} \end{array} \begin{array}{c} \triangle \\ i \\ \uparrow \end{array} = \begin{array}{c} \triangle \\ j \\ \uparrow \\ f_j \\ \text{---} \end{array}$$

Дублирование этого равенства дает (7.31). □

Замечание 7.32. Мы можем получить (7.30) из (7.31), просуммировав по всем ветвям измерения ОНБ:

$$\sum_i \begin{array}{c} \triangle \\ \hat{f}_i \\ \uparrow \end{array} = \sum_i \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \hat{U} \\ \text{---} \\ \text{---} \\ \text{---} \\ \triangle \\ i \\ \uparrow \end{array}$$

что соответствует измерению с последующим забыванием исхода:

$$\begin{array}{c} \triangle \\ \Phi \\ \uparrow \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \hat{U} \\ \text{---} \\ \text{---} \\ \text{---} \end{array}$$

Таким образом, мы видели, что «возмущающие POVM» – это просто произвольные квантовые процессы, отображающие в тривиальную систему, а «невозмущающие POVM» – чистые квантовые процессы, отображающие систему в себя. Стало быть, введя POVM, мы в действительности не получили ничего, кроме затейливого названия того, что нам и так было известно. Однако кое-что важное мы все же установили, а именно что все вероятности, порождаемые произвольными квантовыми процессами, можно воспроизвести в терминах изометрии, измерения ОНБ и ничего более. Это важный урок, который следует запомнить.

Объединяя это с дилатацией Стайнспринга, получаем общую формулировку для всех квантовых процессов.

Теорема 7.33 (Озавы о дилатации). Любой квантовый процесс получается как изометрия \hat{U} , один из выходов которой отбрасывается, а другой является измерением ОНБ:

$$\left(\begin{array}{|c|} \hline \Phi_i \\ \hline \end{array} \right)^i = \begin{array}{|c|} \hline \hat{U} \\ \hline \end{array} \begin{array}{|c|} \hline \begin{array}{|c|} \hline i \\ \hline \end{array} \\ \hline \end{array} \quad (7.33)$$

Упражнение 7.34. Докажите теорему 7.33.

Итак, одна из причин для рассмотрения общих измерений POVM – тот факт, что они естественно возникают при рассмотрении измерения ОНБ для части большей системы, как в теореме 7.31. Приведем еще две причины.

- Измерения POVM возникают из-за несовершенства процедуры измерения вследствие шума или ограниченного доступа к физической системе. С этой точки зрения, естественно интерпретировать (настоящие) измерения POVM как *смешанные измерения*.
- Измерения POVM могут решать задачи, недоступные измерениям фон Неймана. Пример мы увидим в разделе 7.4.2, где специальные измерения, называемые *информационно полными* измерениями POVM, применяются для *томографии квантовых состояний*.

7.4. Томография

Одинокое измерение обычно уничтожает квантовое состояние, давая взамен мало информации. Но если имеется много идентичных копий квантового состояния, то открываются новые возможности. Выполнив серию тщательно подобранных измерений, мы сможем вывести состояние системы из распределения вероятностей всех исходов. Эта процедура называется *томографией*. В этом разделе мы рассмотрим, как работает томография и какие измерения необходимы для ее реализации.

7.4.1. Томография состояния

Очевидно, что «наблюдение» в смысле раздела 7.1.5 – высшая форма томографии. Поэтому для процессных теорий, в которых доступен процесс наблюдения, понятие томографии более-менее избыточно. С другой стороны, в квантовой теории «одинокое наблюдение» недоступно, поэтому концепция томографии очень кстати.

Так как одинокое наблюдение – не вариант, следующий наш шаг – попробовать многократно выполнить одно и то же измерение ОНБ. Но эта идея тоже не работает. Поскольку результат дублирования ОНБ уже не является ОНБ (см. раздел 6.1.5.3), вероятностей

$$P(i | \rho) = \begin{array}{|c|} \hline i \\ \hline \rho \\ \hline \end{array}$$

никогда не хватит для однозначного определения состояния ρ .

Однако существуют более крупные наборы состояний, которые служат (неорто-нормированными) базами квантовых систем. Мы даже явно построили такой набор в теореме 6.24:

$$\left\{ \text{double} \left(\begin{array}{c} \downarrow \\ j \end{array} + \begin{array}{c} \downarrow \\ k \end{array} \right) \right\}_{j \leq k} \cup \left\{ \text{double} \left(\begin{array}{c} \downarrow \\ j \end{array} + i \begin{array}{c} \downarrow \\ k \end{array} \right) \right\}_{j > k}$$

Иными словами, существует набор квантовых состояний

$$\left\{ \begin{array}{c} \downarrow \\ \hat{\phi}_i \end{array} \right\}_i$$

такой, что

$$\left(\forall i : \begin{array}{c} \begin{array}{|c|} \hline \Phi \\ \hline \end{array} = \begin{array}{|c|} \hline \Phi' \\ \hline \end{array} \\ \downarrow \\ \begin{array}{|c|} \hline \hat{\phi}_i \\ \hline \end{array} \end{array} \right) \Rightarrow \begin{array}{|c|} \hline \Phi \\ \hline \end{array} = \begin{array}{|c|} \hline \Phi' \\ \hline \end{array}$$

Отсюда следует, что ассоциированного набора квантовых эффектов

$$\mathcal{E} := \left\{ \begin{array}{|c|} \hline \hat{\phi}_i \\ \hline \uparrow \end{array} \right\}_i$$

достаточно для различения состояний

$$\left(\forall i : \begin{array}{c} \begin{array}{|c|} \hline \hat{\phi}_i \\ \hline \end{array} = \begin{array}{|c|} \hline \hat{\phi}_i \\ \hline \end{array} \\ \uparrow \\ \begin{array}{|c|} \hline \rho \\ \hline \end{array} \end{array} \right) \Rightarrow \begin{array}{|c|} \hline \rho \\ \hline \end{array} = \begin{array}{|c|} \hline \rho' \\ \hline \end{array}$$

Зафиксировав вероятности

$$\begin{array}{|c|} \hline \hat{\phi}_i \\ \hline \uparrow \\ \begin{array}{|c|} \hline \rho \\ \hline \end{array} \end{array}$$

(7.34)

для всех $\hat{\phi}_i$ из \mathcal{E} , мы тем самым зафиксируем состояние ρ . Конечно, мы не можем реализовать эффекты детерминированно, но для любого квантового отображения можно найти реализующий его недетерминированный процесс. Так, в частности, можно найти набор измерений, включающий в себя все эффекты из \mathcal{E} .

Пример 7.35. Для кубитов следующие четыре эффекта однозначно определяют любое состояние:

$$\begin{array}{|c|} \hline 0 \\ \hline \uparrow \end{array} \quad \begin{array}{|c|} \hline 1 \\ \hline \uparrow \end{array} \\ \begin{array}{|c|} \hline 0 \\ \hline \uparrow \end{array} := \text{double} \left(\begin{array}{|c|} \hline 0 \\ \hline \uparrow \end{array} + \begin{array}{|c|} \hline 1 \\ \hline \uparrow \end{array} \right) \quad \begin{array}{|c|} \hline 0 \\ \hline \uparrow \end{array} := \text{double} \left(\begin{array}{|c|} \hline 0 \\ \hline \uparrow \end{array} + i \begin{array}{|c|} \hline 1 \\ \hline \uparrow \end{array} \right)$$

поэтому томографию состояний кубитов можно выполнить, проведя измерения в базисах X , Y и Z (определены в упражнении 6.7):

$$\left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\} \quad \left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\} \quad \left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\}$$

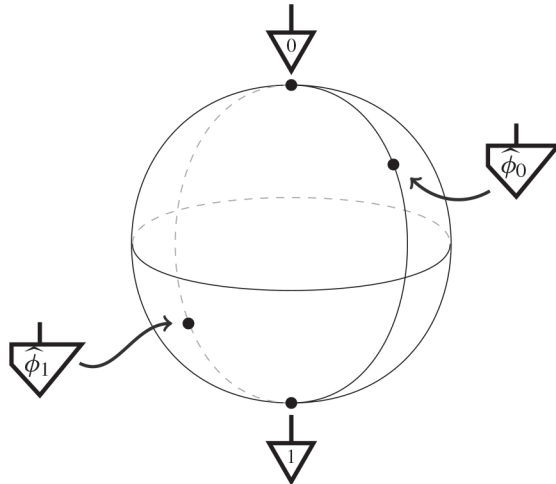
На самом деле никакого меньшего набора измерений ОНБ, чем приведенный в примере 7.35, для решения этой задачи недостаточно. Чтобы доказать это, снова воспользуемся геометрией сферы Блоха.

Предложение 7.36. Для томографии состояний кубитов с помощью измерений ОНБ необходимо выполнить измерения по меньшей мере в трех разных ОНБ.

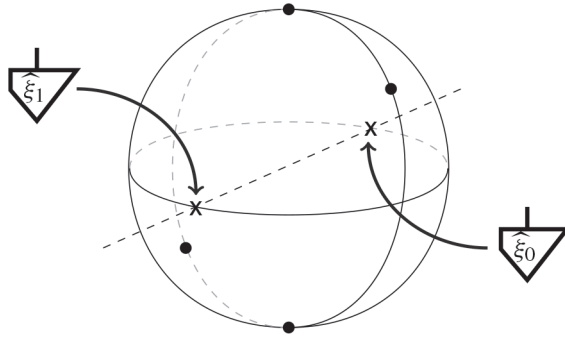
Доказательство. Мы дадим геометрическое доказательство, вспомнив (см. раздел 6.1.2), что внутреннее произведение (7.34) определяет расстояние между двумя состояниями на сфере Блоха. Достаточно показать, что для любых двух измерений ОНБ существует хотя бы два состояния ρ и ρ' , которые невозможно различить. Без ограничения общности предположим, что первым является ОНБ

$$\left\{ \begin{array}{c} \downarrow \\ 0 \end{array}, \begin{array}{c} \downarrow \\ 1 \end{array} \right\}$$

поскольку в противном случае мы бы просто выразили все последующее в терминах какого-то другого базиса, а не Z -базиса. Зафиксируем второй ОНБ $\{\phi_0, \phi_1\}$. Тогда $\hat{\phi}_0$ – произвольная точка на сфере Блоха, а $\hat{\phi}_1$ – ее антипод:



Чтобы найти два неразличимых состояния, достаточно найти два состояния, которые были бы равноудалены от всех четырех базисных состояний. Для этого проведем прямую, перпендикулярную плоскости, образованной этими четырьмя точками, и отметим точки, в которых эта прямая пересекает сферу Блоха:



Тогда измерение ξ_i в любом ОНБ дает любой исход с вероятностью $1/2$. Следовательно, проведя измерения всего в двух базисах, мы не сможем различить ξ_0 и ξ_1 . \square

7.4.2. Информационно полные измерения

Чтобы реализовать томографию состояний кубита, необходимы измерения в трех разных ОНБ. Удивительно, что можно добиться лучшего результата, если не ограничиваться измерениями ОНБ, а допустить общие измерения POVM. На самом деле существует вид измерения POVM, *симметричное информационно полное* (SIC) измерение, которое способно реализовать томографию состояний само по себе. Быть может, идея о том, что «смешанный» процесс может оказаться в чем-то лучше чистого, противоречит интуиции, но факт налицо.

Чтобы понять, как такое возможно, рассмотрим все три измерения ОНБ, необходимых для томографии кубитов, и определим новый квантовый процесс следующим образом. Бросим игральную кость. Если выпадет 1 или 2, выполним первое измерение ОНБ, если 3 или 4 – второе, если 5 или 6 – третье. Очевидно, что если повторить этот квантовый процесс много раз, то количества выполненных измерений ОНБ каждого из трех видов будет достаточно для целей томографии кубитов. Измерение SIC-POVM улучшает этот процесс тем, что проделывает ту же работу более непосредственным и геометрически изящным способом.

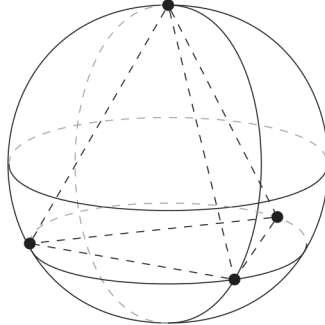
Измерение SIC-POVM состоит из чистых (но ненормированных) квантовых эффектов. Чтобы обеспечить *информационную полноту*, т. е. достаточность для томографии, мы должны потребовать, чтобы у этого квантового процесса было по крайней мере D^2 ветвей, т. к. таково число квантовых состояний, необходимых для образования базиса дублированной системы (см. теорему 6.24). Если множество состоит из D^2 эффектов:

$$\left\{ \begin{array}{c} \triangle \\ \phi_i \\ \uparrow \end{array} \right\}_{i=1}^{i=D^2}$$

то все они не могут быть попарно ортогональны. Для кубитов это все равно, что найти на сфере Блоха четыре точки, каждые две из которых были бы антиподами! Поэтому мы согласимся на меньшее и потребуем, чтобы все эффекты перекрывались на одну и ту же величину:

$$\begin{array}{c} \triangle \\ \hat{\phi}_j \\ \hline \triangle \\ \hat{\phi}_i \end{array} = \begin{cases} 1 & \text{если } i = j \\ \lambda & \text{если } i \neq j \end{cases} \quad (7.35)$$

для некоторого числа λ . Геометрически это означает, что эффекты равномерно распределены в пространстве состояний. На сфере Блоха четыре равномерно расположенные точки всегда находятся в вершинах тетраэдра:



Это условие выражает *симметрию* в термине «симметричное информационно полное». Чтобы это множество эффектов было также каузальным, необходимо умножить каждый эффект на коэффициент, получив тем самым квантовый процесс:

$$\left(\frac{1}{D} \begin{array}{c} \triangle \\ \hat{\phi}_i \\ \hline \triangle \end{array} \right)^i \quad (7.36)$$

и тогда условие каузальности принимает вид:

$$\sum_{i=1}^{i=D^2} \frac{1}{D} \begin{array}{c} \triangle \\ \hat{\phi}_i \\ \hline \triangle \end{array} = \overline{\overline{\mathbb{I}}} \quad (7.37)$$

Определение 7.37. Измерением SIC-POVM называют каузальный квантовый процесс вида (7.36), удовлетворяющий условию (7.35) для некоторого числа λ .

Наконец, и это самое важное, можно доказать, что измерения SIC-POVM информационно полны. Это означает, что вероятности, порождаемые таким измерением, однозначно характеризуют квантовое состояние.

Упражнение* 7.38. Покажите, что для любого измерения SIC-POVM вероятности

$$\left(\frac{1}{D} \begin{array}{c} \triangle \\ \hat{\phi}_i \\ \hline \triangle \\ \rho \end{array} \right)^i$$

полностью характеризуют состояние ρ . Указание: поскольку измерение SIC-POVM состоит из D^2 эффектов, условие «является базисом» можно эквивалентно сформулировать в следующем виде, для которого применяется термин «линейная независимость»:

$$\sum_i c_i \begin{array}{c} \triangle \\ \hat{\phi}_i \\ | \\ \hline \end{array} = 0 \quad \implies \quad \forall i : c_i = 0$$

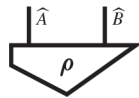
Чтобы показать, что все c_i должны быть равны нулю, для начала покажите, что все они должны быть одинаковы.

Если вам удастся решить следующее упражнение, сообщите нам!

Упражнение* 7.39. Существует ли (изящное) диаграммное представление измерений SIC-POVM?

7.4.3. Локальная томография = процессная томография

Квантовая теория допускает достаточное количество измерений ОНБ для идентификации квантовых состояний. С этим связан другой вопрос: можно ли идентифицировать квантовые состояния нескольких систем, используя только *локальные измерения*? То есть можно ли идентифицировать состояние



ограничившись лишь измерениями отдельных систем? С учетом материала предыдущего раздела это сводится к вопросу о том, существуют ли наборы эффектов

$$\left\{ \begin{array}{c} \triangle \\ \varphi_i \\ | \\ \hat{A} \end{array} \right\}_i \quad \text{и} \quad \left\{ \begin{array}{c} \triangle \\ \varphi'_j \\ | \\ \hat{B} \end{array} \right\}_j$$

такие, что

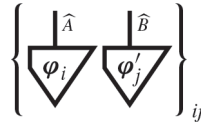
$$\left(\forall i, j : \begin{array}{c} \varphi_i \quad \varphi'_j \\ | \quad | \\ \hline \triangle \\ \rho \end{array} = \begin{array}{c} \varphi_i \quad \varphi'_j \\ | \quad | \\ \hline \triangle \\ \rho' \end{array} \right) \implies \begin{array}{c} | \quad | \\ \hline \triangle \\ \rho \end{array} = \begin{array}{c} | \quad | \\ \hline \triangle \\ \rho' \end{array}$$

Обычно это свойство называют *локальной томографией*.

Для квантовой теории ответ – «безусловно, да». Такие локальные измерения существуют, и очень легко понять, почему. Раз можно найти базисы

$$\left\{ \begin{array}{c} \hat{A} \\ | \\ \hline \triangle \\ \varphi_i \end{array} \right\}_i \quad \text{и} \quad \left\{ \begin{array}{c} \hat{B} \\ | \\ \hline \triangle \\ \varphi'_j \end{array} \right\}_j$$

то требуемые локальные измерения можно определить в терминах базиса произведения:



В разделе 5.2 мы показали, что произведение ОНБ – снова ОНБ, но в случае **линейных отображений** это справедливо и для произвольных базисов. Поэтому имеем следующую теорему.

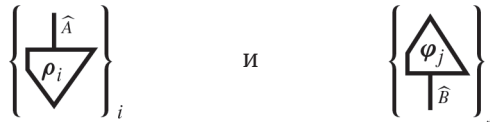
Теорема 7.40. Квантовая теория обладает свойством локальной томографии.

Стоит привыкнуть к концепции базисов произведений, как локальная томография начинает казаться настолько естественным предположением, что даже не понятно, как оно может не выполняться. Однако если немного отклониться в сторону от квантовой теории, то это предположение перестает быть справедливым. Например, как показано в разделе* 7.6.3, это свойство не имеет места в варианте квантовой теории, основанном на матрицах вещественных, а не комплексных чисел.

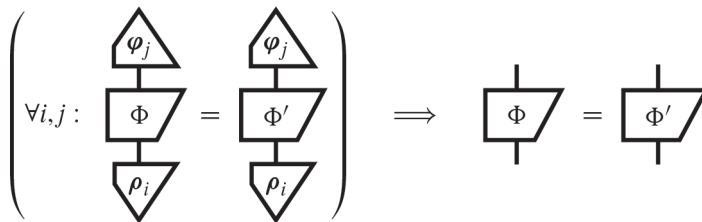
Родственное, но, на первый взгляд, совершенно иное понятие – *процессная томография*. Это процедура, с помощью которой мы пытаемся идентифицировать процесс, представляющий собой черный ящик:



подавая на вход состояния и производя измерения. Она сводится к нахождению таких состояний и эффектов:



что



Для процессных теорий, описываемых струнными диаграммами, эти два понятия томографии эквивалентны.

Теорема 7.41. Процессная теория, допускающая струнные диаграммы, обладает свойством локальной томографии тогда и только тогда, когда она обладает свойством процессной томографии.

Доказательство. Это следует из двойственности процессов и состояний. Предположим, что процессная теория обладает свойством локальной томографии. Тогда для любых процессов f и g имеем:

$$\left(\forall i, j : \begin{array}{c} \psi_i \quad \phi_j \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ f \end{array} = \begin{array}{c} \psi_i \quad \phi_j \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ g \end{array} \right) \Rightarrow \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ f \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ g \end{array}$$

откуда получаем:

$$\left(\forall i, j : \begin{array}{c} \phi_j \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ f \\ \text{---} \\ \psi_i \end{array} = \begin{array}{c} \phi_j \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ g \\ \text{---} \\ \psi_i \end{array} \right) \Rightarrow \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ f \end{array} = \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ g \end{array}$$

Следовательно, процессы f и g различимы с помощью следующих состояний и эффектов:

$$\left\{ \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ \psi_i \end{array} \right\}_i \quad \text{и} \quad \left\{ \begin{array}{c} \phi_j \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \end{array} \right\}_j$$

Обратное утверждение доказывается аналогично. □

7.5. Итоги: что следует запомнить

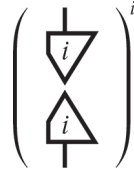
1. «Наблюдение» не является квантовым процессом.
2. Некоторые виды квантовых процессов называются *квантовыми измерениями*.
 - *Возмущающее измерение ОНБ* – это квантовый процесс вида

$$\left(\begin{array}{c} \triangle \\ \text{---} \\ i \\ \text{---} \\ \uparrow \end{array} \right)_i$$

где

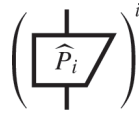
$$\left\{ \begin{array}{c} \text{---} \\ \diagdown \quad \diagup \\ \text{---} \\ \diagup \quad \diagdown \\ i \end{array} \right\}_i$$

– произвольный ОНБ, а соответствующее *невозмущающее измерение ОНБ* – квантовый процесс вида

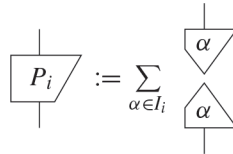


Любое состояние дублированного ОНБ называется *собственным состоянием*, а любое другое состояние – суперпозиционным состоянием этого измерения.

○ *Измерением фон Неймана* называется квантовый процесс вида:



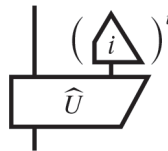
ветвями которого являются взаимно ортогональные проекторы. Эквивалентно измерения фон Неймана можно определить как огрубленные измерения ОНБ:



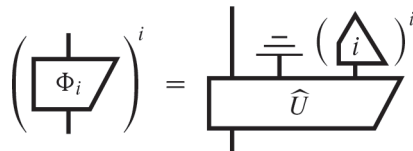
○ *Измерением POVM* называется квантовый процесс вида:



Распределение вероятностей, порождаемое измерением POVM, можно получить также с помощью изометрии и измерения ОНБ:

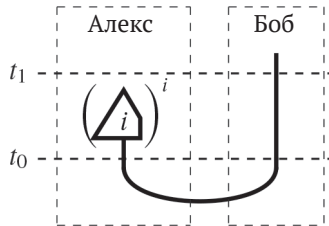


Это утверждение называется *теоремой Наймарка о дилатации*. Вообще, любой квантовый процесс получается из некоторой изометрии \hat{U} , один выход которой отброшен, а другой является измерением ОНБ:

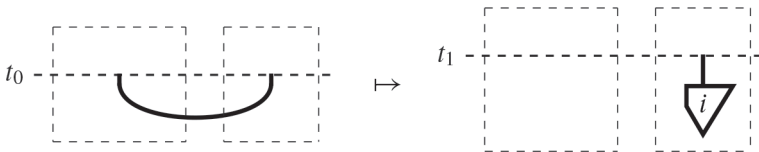


3. Квантовые измерения индуцируют два вида «динамики»:

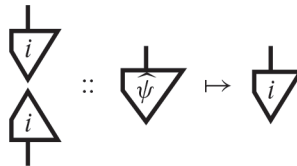
- 1) *обратное действие*, вызывающее мгновенные и радикальные изменения состояния системы, в результате чего оно отличается от измеренного. Например, в ситуации



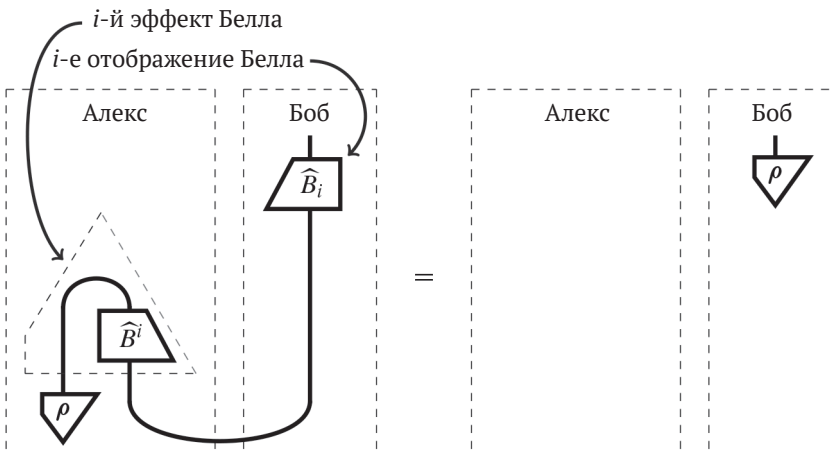
имеет место следующая динамика между моментами времени t_0 и t_1 :



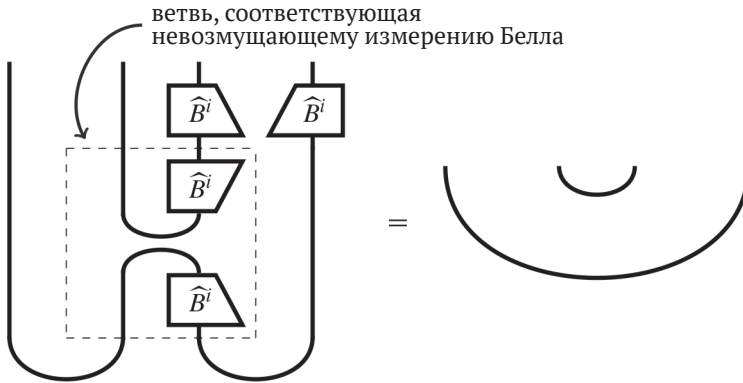
- 2) *коллапс*, вызывающий мгновенный переход из измеренного состояния в собственное состояние измерения:



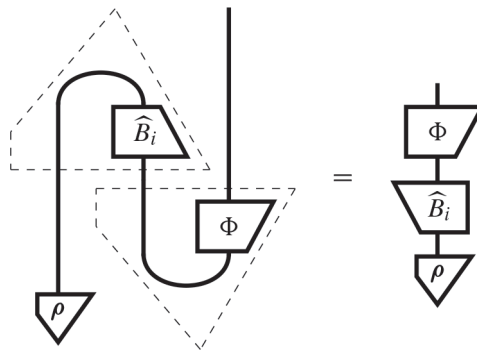
4. Эти динамики используются в квантовых протоколах, включая *квантовую телепортацию*:



перекоммутацию запутывания:

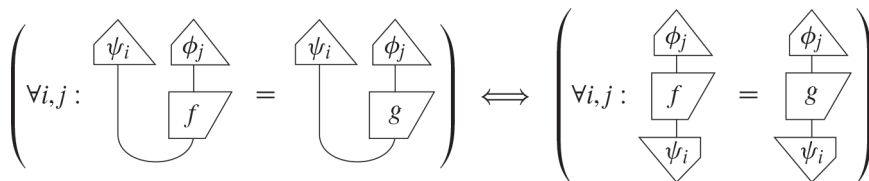


которое позволяет создавать длинные отрезки запутывания из коротких, и *вентильную телепортацию*:



которая позволяет применить к ρ произвольное квантовое отображение Φ , закодированное в двухкомпонентном состоянии. Этот последний прием лежит в основе *квантовых вычислений, основанных на измерениях*.

5. Если имеется много копий системы и все они находятся в одном и том же квантовом состоянии, то мы можем вывести это состояние с помощью *томографии*. Специальный вид измерений POVM – измерения SIC-POVM – дает возможность сделать это, полагаясь только на одно конкретное измерение. Для процессных теорий, допускающих струнные диаграммы, локальная и процессная томографии эквивалентны:



7.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

Теперь мы рассмотрим некоторые фундаментальные вопросы, окружающие квантовые измерения. Начнем с философского обсуждения *проблемы измерения*. Как следует из самого названия, тут есть непростые аспекты. И, кроме того, именно здесь впервые появляется так называемая *квантовая логика*, которая берет начало в идее о том, что проекторы (используемые в измерениях фон Неймана) следует рассматривать как аналог высказываний в обычной логике. Мы сравним эту «логику» с нашей «логикой взаимодействия» (см. раздел 1.2.3). И закончим примером, взятым из работы по основаниям квантовой теории, – покажем, что нечто, столь практичное, как томография, позволяет выявить фундаментальное различие между теориями, основанными на комплексных и вещественных числах.

7.6.1. А существуют ли вообще квантовые измерения?*

Квантовые измерения поистине незаменимы, потому что это единственный способ доступа к квантовому миру. Но что это такое по сравнению с классическим аналогом? В частности, оправдано ли употребление слова «измерение»? В разделе 7.3.4 мы видели, что все квантовые процессы можно рассматривать как некий вид измерения, так что введение специального названия «измерение» выглядит избыточным. Однако в этом разделе мы примем более философскую точку зрения и поразмышляем об истинной сути квантового измерения.

Почему в квантовой теории нет процесса наблюдения? В разделе 7.1.5 мы уже видели доказательство того, что ничего подобного не существует, но тогда нам пришлось в полной мере воспользоваться математической структурой квантовой теории. А хотелось бы иметь концептуальное обоснование того, почему не следует рассчитывать на процесс «наблюдения». Ответ восходит к временам зарождения квантовой теории и связан в основном с именами Нильса Бора и Вернера Гейзенберга:

любая попытка наблюдения обязательно приводит к возмущению.

Многие возразят, что до появления квантовой теории наблюдениям ничто не мешало, и, следовательно, отсутствие процесса наблюдения в квантовой теории – очевидный отход от привычных интуитивных представлений. Но действительно ли в прежних теориях наблюдение было таким уж свободным? Рассмотрим самую обычную ньютонову механику, еще до добавления такой экзотики, как электромагнетизм (и в особенности свет!). Раз нет света, то нет и камер (да и глаз тоже!) для выполнения наблюдений. Если такая вот упрощенная версия ньютоновой механики допускает процесс наблюдения, то мы должны иметь возможность найти предмет в темной комнате, не потревожив его. Очевидно, что если предмет очень легкий, например воздушный шарик, то практически невозможно найти его и при этом не сместить. Точнее, чтобы мы могли найти объект, он должен воздействовать на нас, а согласно закону действия и противодействия, он также будет испытывать воздействие и, значит, немного сдвинется.

Конечно, если восстановить в правах электромагнетизм, т. е. свет и глаза, то мы сможем наблюдать воздушный шарик, не оказывая на него заметного воздействия. Но в квантовых системах, увы, нет аналога той роли, которую свет и гла-

за играют в случае механических объектов. Это печально, но уже неудивительно. Можно сказать, что мы страдаем *квантовой слепотой* и что единственный способ познания квантового мира подразумевает некоторое возмущающее взаимодействие, подобное тому, что имеет место при поиске предмета в темной комнате.

Многим ученым стоит больших усилий отказаться от идеи, что измерение по существу представляет собой наблюдение, и от отчаяния они даже сознательно принимают по-человечески понятное решение производить наблюдения в квантовой теории. Так появляются парадоксы: знаменитый *кот Шрёдингера* и не столь известный *друг Вигнера*.

Раз в квантовой теории не существует процесса наблюдения и доступ к квантовому состоянию сильно осложнен, то возникают вопросы о том, что же на самом деле представляет квантовое состояние. Например, представляет ли квантовое состояние реальные свойства системы или оно ближе к распределению вероятностей, т. е. всего лишь отражает состояние наших знаний о системе? Во многих отношениях вторая интерпретация более привлекательна, потому что распределения вероятностей, как и квантовые состояния, невозможно наблюдать непосредственно, и они могут даже «коллапсировать» при получении новой информации – посредством *байесовского вывода* (раздел 7.2). Однако ряд теорем о невозможности стоит на пути такой интерпретации квантового состояния. Самая известная из них, *теорема Пюзи–Барретта–Рудольфа*, утверждает, что при некоторых предположениях о квантовых системах (которые многие считают разумными) интерпретация на основе «состояния знаний» абсолютно некорректна.

С интерпретацией квантового состояния тесно связана еще одна проблема.

Определение 7.42. *Проблема измерения* состоит из двух вопросов, касающихся измерения (обычно фон Неймана):

m1 В силу какой причины имеет место процесс измерения и, в частности, коллапс квантового состояния?

m2 Что «определяет» исход i этого процесса?

Попытки ответить на эти вопросы обычно называются *интерпретациями*. Некоторые из них отрицают факт изменения состояния, тем самым отвергая постулат редукции фон Неймана, в попытке спасти идею о существовании процесса наблюдения. Как правило, за это приходится платить очень высокую цену: например, в случае *многомировой интерпретации Эверетта* приходится принять существование огромного количества совершенно независимых параллельных Вселенных. В разделе 7.7 мы дадим ссылки на обширную литературу по этим интерпретациям. А сейчас ограничимся тем, что переформулируем проблему измерения в случае, когда квантовая теория рассматривается как процессная теория, и опишем некоторые естественные подходы к ее решению.

Ранние решения проблемы **m1** включали идею о том, что коллапс вызывается подключением к *измерительному прибору* или, более общо, к любой *макроскопической системе*. Однако для этого необходимо четко определить, что такое измерительный прибор и где кончается микромир и начинается макромир. Дать исчерпывающие ответы на эти вопросы оказалось очень трудно, а то и невозможно. Ничто в нашем опыте не предполагает существования «стены», разделяющей микро- и макроуровни, и уж совсем нелепо думать, будто какая-то изготовленная человеком машина сможет играть определяющую роль в фундаментальной физике, которая существовала задолго до появления человечества.

Альтернативно можно было бы сказать, что процесс измерения имеет место, когда система находится в среде, которая вызывает осуществление этого процесса. Не больше, не меньше. Если занять такую позицию, то ответ на вопрос **m1** сводится к явному описанию такой среды. Эта точка зрения особенно хорошо стыкуется с описанием квантовых систем как проводов на диаграмме, где система характеризуется своим поведением в контексте. Также она тесно связана с позднейтеитенштейновской концепцией *значения в контексте*, которая говорит, что значение чего-либо раскрывается только при условии учета контекста, в котором это что-то рассматривается. В переводе на язык квантовой теории это означает, что квантовые системы следует рассматривать не как изолированные сущности, а как сущности во взаимодействии с контекстом, т. е. с остальной частью диаграммы, которая включает и измерение.

Сюда же примыкает вопрос о концептуальном месте ОНБ в процессе измерения. Что-то узнать о квантовой системе можно только в терминах понятий, которые мы способны воспринять, например положений в пространстве-времени. Но, быть может, пространство-время не является естественной средой для квантовой системы, и тогда, вероятно, процесс измерения заключается в «принудительной доставке» системы в пространственно-временной театр действий. Такой процесс можно было бы назвать *оклассичиванием*. Идея о том, что пространство-время может и не быть тем театром, на котором разворачивается наша реальность, а лишь формой человеческого опыта, восходит к философу Иммануилу Канту, и впоследствии была развита математиком Анри Пуанкаре, который зашел настолько далеко, что роль геометрии в физике приписывал отчасти человеческой интуиции.

Теперь перейдем к проблеме **m2** – что приводит к определенному исходу i измерения. Первые попытки решения, предпринятые под влиянием знаменитого высказывания Эйнштейна «Бог не играет в кости», предполагали, что квантовая система не сводится к одному лишь квантовому состоянию, а есть в ней что-то еще. Это «что-то» получило название *скрытых параметров*. Основная идея заключалась в том, что дополнительные параметры, связанные с квантовой системой, могли бы определять результаты измерения. Известная *теорема Белла–Кохена–Спекера* запрещает *бесконтекстные* скрытые параметры, значения которых в некотором смысле «реальны» и не зависят от измерения. Существуют скрытые параметры, которые не противоречат теоремам о невозможности, и в особенности *модель скрытых параметров Боба*. Однако эти скрытые параметры сильно отличаются от того, что имел в виду Эйнштейн. В частности, они обязательно нелокальны, как будет показано в разделе 11.1.

С другой стороны, если ассоциировать дополнительные параметры не с самим состоянием, а с контекстом состояния, который включает взаимодействие между квантовой системой и ее окружением, то можно будет беспрепятственно связать исходы с парой, состоящей из квантового состояния и этих дополнительных параметров. Удивительно, что эта возможность никогда по-настоящему не рассматривалась. Хотя мы, движимые все тем же желанием спасти процесс наблюдения, считаем это вполне разумным, многие ученые отказываются принять идею о том, что окружение может оказывать влияние на информацию, получаемую о системе.

Основное препятствие, мешающее смириться с этой идеей, – тот факт, что наука традиционно строилась на предположении о том, что любую систему, являющуюся предметом исследования, следует как можно сильнее изолировать от окружения в процессе изучения. Быть может, главный урок, который преподает нам квантовая теория, в том и заключается, что эту позицию невозможно сохранить и следует искать что-то другое на путях *реляционализма* – представления о том, что ткань реальности состоит из связей между вещами, а не из их отдельных атрибутов. Диаграммы, конечно, предлагают естественный язык для описания такой реляционной Вселенной.

7.6.2. Проекторы и квантовая логика*

В замечании 7.26 мы упомянули о том, что проекторы можно интерпретировать как высказывания относительно квантовых систем, что приводит к появлению *квантовой логики*. Отправная точка квантовой логики состоит в том, что верна не точка зрения Шрёдингера, согласно которой сердцевина квантовой механики – это способ композиции систем, а точка зрения фон Неймана, заключающаяся в том, что ключом является понимание природы квантовых измерений.

В классической логике система обычно рассматривается как множество состояний X . Тогда *высказывание* – это просто подмножество состояний $P \subseteq X$, которое следует интерпретировать как множество всех состояний, удовлетворяющих P . Например, если системой является картошка, а P – «сварена», то формально это высказывание представляется как множество всех возможных состояний картошки, в которых она сварена.

На высказываниях, являющихся подмножествами, определено естественное отношение порядка – включение множеств. Так, если Q означает «приготовлена», то поскольку сваренная картошка является также приготовленной, имеем:

$$P \subseteq Q.$$

Иными словами, мы можем вывести Q из P . Это отношение порядка, представляющее собой «дедукцию», – краеугольный камень любой логической системы. Мы также можем представить конъюнкцию (« P и Q »), дизъюнкцию (« P или Q ») и отрицание («не P ») как операции над множествами:

$$P \cap Q, \quad P \cup Q, \quad P^\perp := X \setminus P. \quad (7.38)$$

Эти операции наделяют множество высказываний математической структурой *булевой решетки*, т. е. множества с операциями \cup , \cap , $()^\perp$, обладающими различными свойствами. Самое важное из них – *дистрибутивность*:

$$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R).$$

Проекторы в некотором смысле играют роль высказываний в квантовой теории, будучи «верифицируемыми высказываниями». А именно для любого \hat{P} мы можем найти измерение фон Неймана, проверяющее, выполняется ли \hat{P} . Как и в случае высказываний, на множестве проекторов можно определить «дедуктивный» порядок:

$$\left(\begin{array}{c} \diagdown \\ \hat{P} \\ \diagup \end{array} \leq \begin{array}{c} \diagdown \\ \hat{Q} \\ \diagup \end{array} \right) := \left(\begin{array}{c} \begin{array}{c} \diagdown \\ \hat{Q} \\ \diagup \end{array} \\ \text{---} \\ \begin{array}{c} \diagdown \\ \hat{P} \\ \diagup \end{array} \end{array} = \begin{array}{c} \diagdown \\ \hat{P} \\ \diagup \end{array} \right) \quad (7.39)$$

И в чем же сходство этого порядка на множестве высказываний с предыдущим? Мы можем ассоциировать с каждым проектором \hat{P} множество состояний, для которых \hat{P} достоверно выполняется:

$$S_{\hat{P}} := \left\{ \begin{array}{c} \downarrow \\ \psi \\ \downarrow \end{array} \mid \begin{array}{c} \begin{array}{c} \diagdown \\ \hat{P} \\ \diagup \end{array} \\ \text{---} \\ \begin{array}{c} \diagdown \\ \psi \\ \downarrow \end{array} \end{array} = \begin{array}{c} \downarrow \\ \psi \\ \downarrow \end{array} \right\}$$

Легко проверить, что (7.39) эквивалентно включению

$$S_{\hat{P}} \subseteq S_{\hat{Q}}.$$

Поэтому для любого состояния ψ из свойства «удовлетворяет» \hat{P} следует свойство «удовлетворяет» \hat{Q} . Однако эти $S_{\hat{P}}$ – не произвольные множества, а *подпространства*.

Упражнение 7.43. Покажите, что для любого проектора \hat{P} в квантовой системе \hat{H} существует подпространство $H_P \subseteq H$ такое, что $S_{\hat{P}}$ является множеством всех состояний $\hat{\psi}$ для $\psi \in H_P$. Обратно, покажите, что любое подпространство H соответствует проектору, который однозначно определяется подобным образом.

Мы можем извлечь отсюда кое-что полезное. Например, множеству

$$S_{\hat{P}} \cap S_{\hat{Q}}$$

также соответствует подпространство, поэтому можно назвать « \hat{P} and \hat{Q} » ассоциированный с ним проектор, который будем обозначать

$$\hat{P} \wedge \hat{Q}.$$

Однако

$$S_{\hat{P}} \cup S_{\hat{Q}}$$

не является подпространством, поэтому придется проявить изобретательность. Полагая

$$\begin{array}{c} \diagdown \\ P^\perp \\ \diagup \end{array} := \left| - \begin{array}{c} \diagdown \\ P \\ \diagup \end{array} \right.$$

мы получим отрицание. Тогда, в силу закона де Моргана, «not (not P and not Q)», это выражение должно совпадать с « P or Q », поэтому положим

$$\widehat{P} \vee \widehat{Q} := (\widehat{P}^\perp \wedge \widehat{Q}^\perp)^\perp.$$

К сожалению, операции \wedge и \vee не дистрибутивны.

Упражнение 7.44. Покажите, что

Поэтому вместо дистрибутивности в квантовой логике используется значительно более слабое свойство, называемое *ортотомодулярностью*:

$$\widehat{P} \leq \widehat{Q} \implies \widehat{Q} = \widehat{P} \vee (\widehat{P}^\perp \wedge \widehat{Q}).$$

Цель квантовой логики – изучение квантовых систем в той мере, в какой это возможно с использованием только этой, очень слабой логической структуры.

При таком подходе убирается «шум», связанный с гильбертовыми пространствами, и открывается возможность для новых идей, что вполне созвучно целям этой книги. Однако, как мы подчеркивали в разделе 1.2.4, квантовая логика стремится охарактеризовать квантовую теорию с точки зрения *отсутствия* чего-либо, что и объясняет провал этой программы исследований. Интересно, что проблема, на которой квантовая логика потерпела самое сокрушительное поражение, – описание составных систем, т. е. ровно то, с чего мы начали эту книгу, и, быть может, это самый важный урок, который стоит извлечь из квантовой логики.

7.6.3. Невозможность локальной томографии*

В последнее время немало интересных исследований по основаниям квантовой теории вращалось вокруг того факта, что многие характеристические особенности квантовой теории тесно переплетены со взаимодействием нескольких систем. Один примечательный результат такого рода – подтверждение ключевой роли комплексных чисел посредством томографии двух систем.

Допустим, что мы определяем новую процессную теорию \mathbb{R} -квантовых отображений, состоящую из квантовых отображений, в которых участвуют только вещественные числа. Точнее, вместо дублирования $\mathbf{matrices}(\mathbb{C})$ мы дублируем $\mathbf{matrices}(\mathbb{R})$. Можно было бы ожидать, что эта теория будет очень похожа на теорию квантовых отображений, но на самом деле отказ от мнимой части комплексных чисел приводит к драматическим последствиям.

Теорема 7.45. Теория \mathbb{R} -квантовых отображений не допускает процессной томографии и, следовательно, не допускает локальной томографии.

Доказательство. Как и в случае квантовых отображений, любое состояние ρ в теории \mathbb{R} -квантовых отображений является \otimes -положительным линейным отображением, поэтому, в частности, оно самосопряженное. Следовательно, любое двумерное состояние в теории \mathbb{R} -квантовых отображений (назовем его «вещбитовым» (rebit) состоянием) можно записать в виде:

$$\begin{array}{c} \downarrow \\ \rho \end{array} = a \begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} + b \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} \right) + c \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array}$$

где $a, b, c \in \mathbb{R}$. Матрицы отображений Белла вещественные, поэтому \widehat{B}_3 является процессом в теории **\mathbb{R} -квантовых отображений**. Применив его к ρ , получим:

$$\begin{array}{c} \widehat{B}_3 \\ \downarrow \\ \rho \end{array} = c \begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} - b \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} \right) + a \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array}$$

Складывая получившееся состояние с самим ρ , получаем:

$$\begin{array}{c} \downarrow \\ \rho \end{array} + \begin{array}{c} \widehat{B}_3 \\ \downarrow \\ \rho \end{array} = (a+c) \left(\begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} \right) = \begin{array}{c} \underline{\underline{\downarrow}} \\ \underline{\underline{\rho}} \end{array}$$

Таким образом, процессы

$$\begin{array}{c} | \\ + \\ \widehat{B}_3 \end{array} \quad \text{и} \quad \begin{array}{c} \underline{\underline{\downarrow}} \\ \underline{\underline{\rho}} \end{array}$$

совпадают на всех состояниях теории **\mathbb{R} -квантовых отображений**, и вместе с тем они, очевидно, не равны. \square

Мы не можем различить процессы на диаграммах (7.40), просто применяя их к состояниям. Ну и что с того? Быть может, мы вообще никогда не увидим между ними различий, а значит, для всех практических целей они одинаковы. Но это не так! И в этом легко убедиться, преобразовав эти процессы в двухкомпонентные состояния. Эквивалентность процессной и локальной томографии вытекает из двойственности процессов и состояний. Применение этой двойственности к процессам на диаграммах (7.40) говорит, что мы не можем различить двухкомпонентные состояния

$$\begin{array}{c} \mu \\ \downarrow \end{array} := \begin{array}{c} \widehat{B}_0 \\ \downarrow \end{array} + \begin{array}{c} \widehat{B}_3 \\ \downarrow \end{array} \quad \text{и} \quad \begin{array}{c} \underline{\underline{\downarrow}} \\ \underline{\underline{\mu}} \end{array}$$

с помощью локальных эффектов. Однако их все же можно различить с помощью глобального эффекта, а именно любого из остальных эффектов, составляющих базис Белла:

$$\begin{array}{c} \widehat{B}_2 \\ \downarrow \\ \mu \end{array} = 0 \neq 1 = \begin{array}{c} \widehat{B}_2 \\ \underline{\underline{\downarrow}} \\ \underline{\underline{\mu}} \end{array}$$

Таким образом, можно заключить, что теория **\mathbb{R} -квантовых отображений** действительно принципиально отличается от теории **квантовых отображений**. В частности, томография процессов и составных систем в ней выглядела бы совершенно по-другому.

Упражнение 7.46. Приведите пример диаграммы, на которой два процесса в (7.40) различимы (т. е. порождают разные вероятности по правилу Борна) в теории **\mathbb{R} -квантовых отображений**.

7.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Описанные выше квантовые измерения и измерения фон Неймана, в частности, очевидно, восходят к работе von Neumann (1932), где среди прочего изложена идея коллапса и тот факт, что коллапс индуцируется проекторами.

Теорема Наймарка для POVM впервые была опубликована в работе Neumark (1943). В работе Ozawa (1984) сформулирован более общий вариант этой теоремы для того, что автор называет «квантовыми приборами», которые включают в том числе и определенные нами квантовые процессы. Перекоммутация запутывания впервые предложена в работе Zukowski et al. (1993), а основанные на телепортации универсальные квантовые вычисления предложены в работе Gottesman and Chuang (1999). Теорема Вигнера, упомянутая в замечании * 7.3, взята из работы Wigner (1931).

Аксиома локальной томографии в той форме, в которой она представлена здесь, взята из работы Chiribella et al. (2010). Похожая формулировка встречалась ранее в работе Barrett (2007), которая, в свою очередь, восходит к реконструкции квантовой теории в работе Hardy (2001). Измерения SIC-POVM восходят к работе Lemmens and Seidel (1973). Упражнение 7.39 предложил нам Крис Фукс (Chris Fuchs), который глубоко убежден, что SIC-POVM играют фундаментальную роль в квантовой теории (Fuchs, 2002). Эта позиция является одной из особенностей интерпретации квантовой теории, которая называется *квантовым байесианизмом*, или *кубизмом* (QBism) (Fuchs et al., 2014).

Проблема измерения выросла из спора Бора и Эйнштейна, который последовал за работами ЭПР (Einstein et al., 1935; Einstein, 1936) и ответом Нильса Бора (Bohr, 1935). Позиции Гейзенберга и Бора были опубликованы гораздо раньше в книгах Heisenberg (1930) и Bohr (1931). Парадокс кота Шрёдингера впервые опубликован в работе Schrödinger (1935), а парадокс друга Вигнера – в работе Wigner (1995a). Проблеме измерения посвящено много учебников, из которых отметим Jammer (1974), Redhead (1987) и Bub (1999). Оригинальные, но все еще популярные работы Everett (1957) и Bohm (1952a,b) посвящены соответственно многомировой интерпретации и примеру теории с контекстным скрытым параметром. Теоремы об ограниченности интерпретации квантового состояния приведены в работах Jauch and Piron (1963), Kochen and Specker (1967) и Pusey et al. (2012). На самом деле результат работы Kochen and Specker (1967) – более-менее очевидное следствие теоремы Глисона (Gleason, 1957), как объяснено в работе Belinfante (1973).

Слова Планка, приведенные в эпиграфе к этой главе, были сказаны в 1936 году в речи по случаю двадцать пятой годовщины Общества кайзера Вильгельма по развитию науки (см. Macrakis, 1993). Впоследствии оно принимало участие в научных исследованиях нацистов и было расформировано, а его функции перешли

к Обществу Макса Планка. Очевидно, поводом к ним послужили именно вышеупомянутые трудности интерпретации, из-за которых многие физики не приняли квантовую теорию.

Модифицированные Пуанкаре воззрения Канта, упомянутые в разделе 7.6.1, взяты из работы Poincaré (1902). Витгенштейновская концепция «значения в контексте» впервые опубликована в работе Wittgenstein (1953). Реляционистские взгляды на пространство и время восходят еще к Лейбницу (см., например, Rickles, 2007).

Уже в своей книге по квантовой теории (von Neumann, 1932) фон Нейман придавал фундаментальное значение роли проекторов как высказываний в квантовом мире. Затем эта идея легла в основу так называемой квантовой логики (Birkhoff and von Neumann, 1936). Фон Нейману квантовая логика представлялась путем к улучшенному формализму квантовой теории. Отчасти это подвигло его на разработку *алгебр фон Неймана* и, в частности, на изучение *факторов типа II*. Все это детально описано в работе Redei (1996). Интересно, что хотя специалисты по квантовой логике приняли ортомодулярный закон, фон Нейман настаивал на более сильном *модулярном законе*:

$$\widehat{P} \leq \widehat{Q} \Rightarrow \widehat{P} \vee (\widehat{R} \wedge \widehat{Q}) = (\widehat{P} \vee \widehat{R}) \wedge \widehat{Q},$$

который имеет место только для конечномерной квантовой теории. В качестве аргумента он выдвигал тот факт, что этот закон справедлив для проективных геометрий и что решетка замкнутых подпространств гильбертова пространства естественно вкладывается в модулярную решетку, которая, в силу фундаментальной теоремы проективной геометрии, дает представление векторного пространства (Piron, 1976; Stubbe and van Steirteghem, 2007).

Многим ученым квантовая логика представлялась не столько логикой, сколько разделом теории вероятностей и алгебры. Разработка ее операционного варианта была начата в работе Maskey (1963), а затем под нее был подведен концептуальный и философский фундамент в работах Piron (1976) и Moore (1999). Константин Пирон (Piron, 1964) также построил то, что можно считать первой реконструкцией квантовой теории на основе операционных принципов.

В предисловии к этой книге уже отмечалось, что один из авторов пришел к осознанию важности процессов через квантовую логику. В частности, если вместо того чтобы рассуждать о статических высказываниях, перейти к вопросу о том, как высказывания эволюционируют, то можно вывести линейность процессов (Faure et al., 1995). Та же аргументация приводит к самой убедительной интерпретации ортомодулярности, соответствующей тому факту, что проекторы – это фактически процессы (Coecke et al., 2001; Coecke and Smets, 2004). В ее основе лежит рассуждение, обобщающее *семантику самого слабого предусловия*, встречающегося в информатике (Dijkstra, 1968; Hoare and He, 1987). Это направление исследований получило дальнейшее развитие в работе Baltag and Smets (2005). Наша любовь к квантовой логике не совсем угасла, о чем свидетельствует недавняя попытка примирить диаграммы с квантовой логикой (Coecke et al., 2013b).

Глава 8

Изображение классически-квантовых процессов

...И, удаляясь, ее окропила Гекатиных зелий
Соком, и в этот же миг, обрызганы снадобьем страшным,
Волосы слезли ее, исчезли ноздри и уши,
Стала мала голова, и сделалось крохотным тело.
Нет уже ног, – по бокам топорщатся тонкие ножки;
Все остальное – живот. Из него тем не менее тянет
Нитку Арахна – паук продолжает плести паутину.

– Овидий. «Метаморфозы», VIII век до н. э.¹

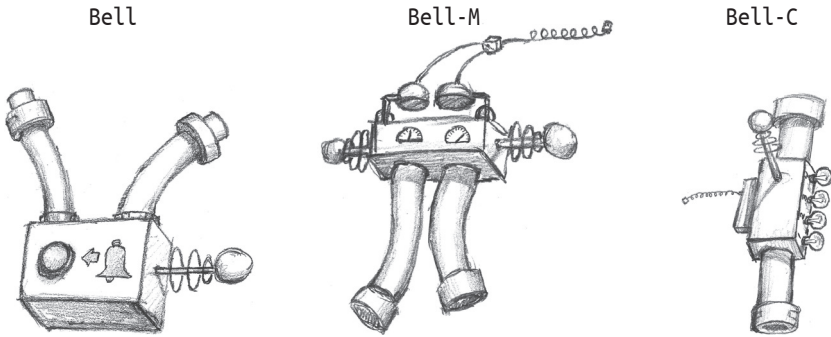
Большинство квантовых протоколов опирается на взаимодействие между квантовыми системами и классическими данными. Например, измерения извлекают классические данные из квантовой системы, а в управляемых операциях классические данные используются, чтобы воздействовать на квантовую систему. Кроме того, учитывая, что истина у каждого своя, мы хотим соотнести квантовую теорию с нашим – классическим – восприятием реальности. Как это ни странно, оказывается, что представить классический мир в свете квантовых процессов гораздо проще, чем наоборот.

Один из способов подойти к этому взаимодействию – выразить как можно больше в чисто диаграммной форме. Раньше мы рисовали диаграммы квантовых процессов, а затем использовали для описания потока классических данных некие «внешние» средства, а именно индексы и скобки, которые невозможно соединить между собой так же естественно, как части диаграммы. Хуже того, в большинстве стандартных учебников классические данные даже не являются частью формализма, а описываются только словами.

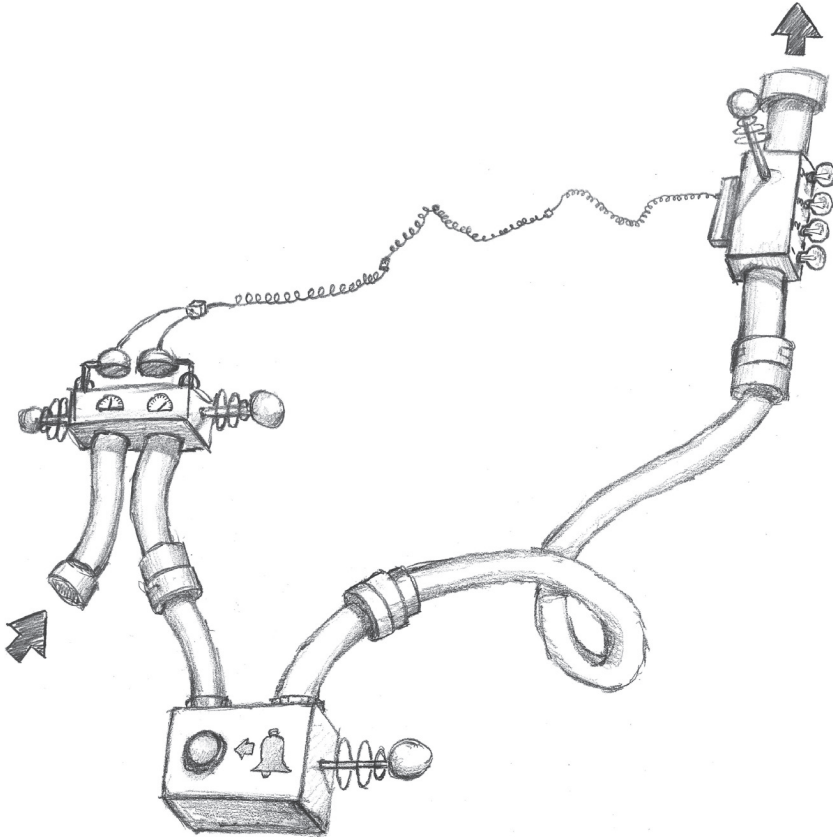
Вместо того чтобы путано и многословно описывать взаимодействие квантовых систем и классических данных или пытаться скрестить диаграммы с символами, нельзя ли просто привести диаграмму всех участвующих устройств и показать, как они соединятся проводами? Например, предположим, что имеется устройство Bell, которое подготавливает состояния Белла, другое устройство Bell-M, ко-

¹ Перевод с лат. С. В. Шервинского.

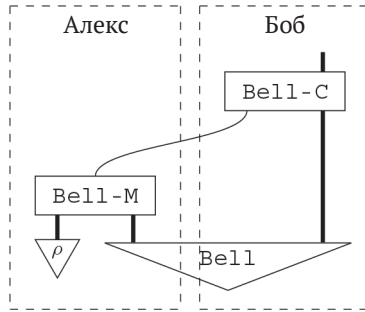
торое выполняет измерения Белла, и третье устройство Bell-C, которое производит корректировки Белла, изображаемые в таком реалистичном стиле:



Далее предположим, что мы хотим рассказать технику, как соединить эти устройства, чтобы осуществить телепортацию:



Это можно было бы сделать на языке спецификаций, т. е. диаграммном языке, в котором блоки соответствуют устройствам, а провода – буквально «соединению» устройств:



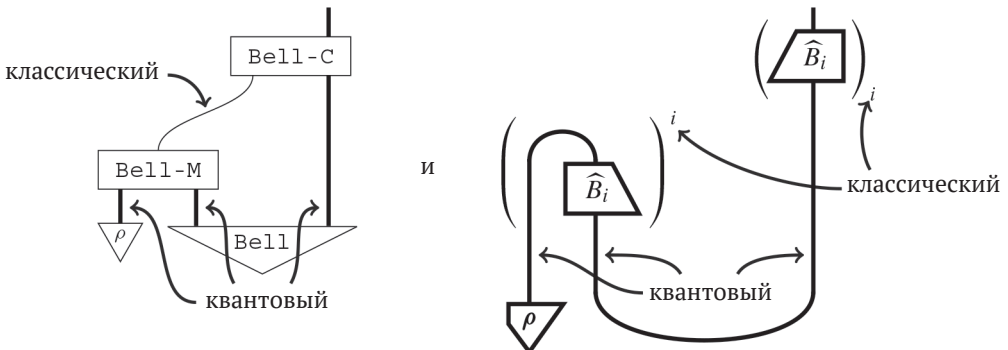
только квантовые и классические провода теперь различаются.

Любой корректно написанной спецификации протокола, т. е. диаграмме на языке спецификаций, должна соответствовать математическая модель, которую теоретик мог бы использовать для прогнозирования действий протокола. Это соответствие между спецификацией и моделью можно изобразить с помощью *интерпретационных скобок* $\llbracket - \rrbracket$. Тогда для телепортации будем иметь:

$$\llbracket \text{Diagram} \rrbracket = \text{Simplified Circuit} \quad (8.1)$$

Таким образом, левая часть описывает порядок настройки оборудования техником, а правая – теоретический прогноз работы этого оборудования. Можно сказать, что истинная предсказательная способность квантовой теории сводится к определению $\llbracket - \rrbracket$.

Как уже было отмечено, здесь имеется небольшая нестыковка, поскольку квантовые системы – это провода, а классические – нечто совершенно иное:



В действительности нам хотелось бы трактовать и классические, и квантовые системы как провода, и тогда рецепт для интерпретации диаграммы спецификации свелся бы просто к интерпретации каждой ее компоненты:

$$\left[\begin{array}{c} \text{Bell-C} \\ \text{Bell-M} \\ \text{Bell} \end{array} \right] := \left[\rho \right] \left[\text{Bell} \right] \left[\text{Bell-M} \right] \left[\text{Bell-C} \right] \quad (8.2)$$

Это означает, что моделирование всего процесса сводится к моделированию четырех меньших процессов



с последующей их композицией.

Мы уже знаем, как это сделать для чисто квантовых блоков и проводов:

$$\left[\rho \right] = \text{wire}(\rho) \quad \left[\text{Bell} \right] = \text{wire}(\text{Bell})$$

поэтому для завершения картины нужно понять, как интерпретировать блоки, к которым подходят также классические провода:

$$\left[\text{Bell-M} \right] = ? \quad \left[\text{Bell-C} \right] = ?$$

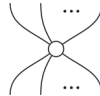
Мы уже с успехом воспользовались тем фактом, что дублирование открывает возможность для некоторых дополнительных процессов, а именно нечистых квантовых отображений. Теперь мы увидим, что оно оставляет место и для некоторых дополнительных классических систем. Дополнив **квантовые отображения** классическими проводами, мы получим новую процессную теорию **классически-квантовых отображений** (classical-quantum map), или, для краткости, **КК-отображений**. Добавив еще принцип причинности, мы получим полную теорию **квантовых процессов**, которым и посвящена эта книга. Тогда оставленные выше пустые места можно заполнить следующим образом:

$$\left[\text{Bell-M} \right] = \text{wire}(\hat{U}) \quad \left[\text{Bell-C} \right] = \text{wire}(\hat{U})$$

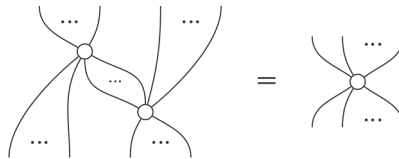
Как и в языке спецификаций, толстые провода представляют квантовые системы, а тонкие – классические системы. Состояние квантовой системы такое же, как и раньше, но, как мы скоро увидим, состоянием классической системы является распределение вероятностей. Следовательно, КК-отображения одновременно обобщают квантовые отображения и естественное понятие соответствия между классическими распределениями вероятностей (т. е. *стохастические отображения*):



Поскольку классические данные можно копировать и удалять, естественно разрешить классическим проводам расходиться и сходиться различными способами. Точки, в которых сходится несколько классических проводов, называются *пауками*:



Пауков можно рассматривать как обобщение чашек и крышек, а их поведение определяется единственным правилом «слияния»:



Если провод – это нечто, соединяющее два конца, то паук – обобщение, допускающее несколько концов. Следовательно, правило слияния пауков, включающее в себя уравнения разгибания чашек и крышек, воплощает идею о том, что «важны только соединения».

Хотя пауки введены, чтобы можно было рассуждать о классических данных, мы будем использовать их и для построения новых квантовых отображений и классически-квантовых гибридов. На самом деле пауки настолько могущественны, что мы сможем с их помощью изложить всю квантовую теорию. Уже знакомые концепции *измерения*, *классического управления* и *смешанности*, а также новые понятия – *классическое копирование*, *запутывание* (нечистых состояний) и *декогеренция* – будут выражены в терминах этих новых разновидностей процессов. Вообще, начиная с этой главы, книга будет просто кишеть пауками!

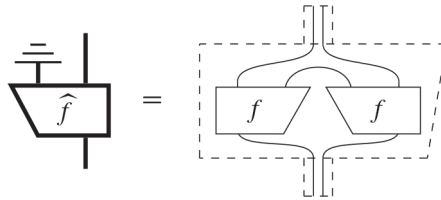
8.1. КЛАССИЧЕСКИЕ СИСТЕМЫ КАК ПРОВОДА

В этом разделе мы покажем, что классические системы, как и квантовые, можно представить в терминах линейных отображений. Таким образом, вместо того чтобы обращаться с классическими входами и выходами квантового процесса

«внешним образом» с помощью индексов, мы можем просто выразить их как провода, которые можно соединять между собой. Это позволит нам выстроить простое изложение теории **квантовых процессов** и восстановить элегантность оригинального (свободного от сумм) варианта принципа причинности.

8.1.1. Двойные и одиночные провода

Теорию **квантовых отображений** можно рассматривать как ограничение теории **линейных отображений**, в котором допускаются только отображения очень специального вида:



Теперь мы хотим построить теорию, включающую отображения, где квантовые и классические системы могут взаимодействовать между собой. Поскольку типы квантовых и классических систем фундаментально различны, нам понадобятся два разных типа проводов. Так как квантовые системы уже представляются проводами двойной толщины, то для введения нового вида систем мы просто вернем одиночные провода:

$$\left(\begin{array}{c} \text{квантовый} := \\ \left| \right. \end{array} \right) \neq \left(\begin{array}{c} \text{классический} := \\ \left| \right. \end{array} \right)$$

И, как мы скоро увидим, это прекрасно согласуется с представлением классических систем. Итак:

$$\frac{\text{классический}}{\text{квантовый}} = \frac{\text{тонкие/одиночные провода}}{\text{толстые/двойные провода}}$$


Классические данные на одиночном проводе кодируются посредством представления классических значений базисными состояниями фиксированного ОНБ. Следовательно, для ОНБ классической системы размерности D это означает, что соответствующие классические данные могут принимать D значений. Например, одному биту соответствует ОНБ двумерной системы:

$$\text{бит} := \left\{ \begin{array}{c} \downarrow \\ \nabla \\ 0 \end{array}, \begin{array}{c} \downarrow \\ \nabla \\ 1 \end{array} \right\}$$

Точнее, мы интерпретируем состояния этого ОНБ следующим образом:

- $\begin{array}{c} \downarrow \\ \nabla \\ i \end{array}$:= «предоставление классического значения i »;

а соответствующие эффекты:

○  := «проверка на совпадение с классическим значением i ».

При такой интерпретации ортонормированность

$$\begin{array}{c} \triangle \\ j \\ \hline i \\ \triangle \end{array} = \delta_i^j \quad (8.3)$$

имеет вполне разумный смысл. Мы получаем вероятность 0 (т. е. «невозможно»), когда проверяем значение $j \neq i$ на совпадение со значением i , и вероятность 1 (т. е. «достоверно»), когда проверяем значение i на совпадение со значением i .

Замечание 8.1. Мы будем использовать для классических данных самосопряженные ОНБ, поскольку у операции сопряжения нет классического аналога; так, выражение «сопряженный бит» лишено смысла.

Когда применяется квантовый процесс, например

$$\left(\begin{array}{c} \text{---} \\ | \\ \square \\ \Phi_i \\ | \\ \text{---} \end{array} \right)_i$$

происходят две вещи. Понятно, что к квантовой системе применяется одна из ветвей Φ_i , но еще и выскакивает классическое значение i , которое говорит, какая ветвь имела место. Чтобы отразить это с помощью классического провода, мы можем представить квантовый процесс в виде:

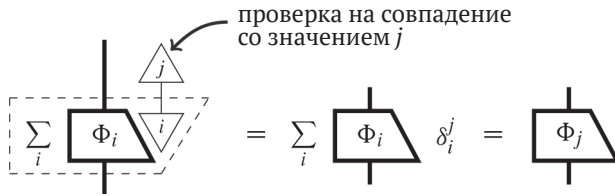
$$\left(\begin{array}{c} \text{---} \\ | \\ \square \\ \Phi_i \\ | \\ \text{---} \end{array} \right)_i \sim \sum_i \begin{array}{c} \text{---} \\ | \\ \square \\ \Phi_i \\ | \\ \text{---} \\ \triangle \\ i \end{array} \quad (8.4)$$

т. е. сделать создание классического выхода явным и представить весь процесс как одно большое линейное отображение.

Аналогично, если выходы квантовых процессов управляются классическим вводом, то мы можем воспользоваться i -эффектами для представления того факта, что проверяется совпадение с входным значением:

$$\left(\begin{array}{c} \text{---} \\ \triangle \\ i \\ | \\ \square \\ \Psi_i \\ | \\ \text{---} \end{array} \right)_i \sim \sum_i \begin{array}{c} \triangle \\ i \\ | \\ \square \\ \Psi_i \\ | \\ \text{---} \end{array} \quad (8.5)$$

Легко видеть, что это дает адекватные представления соответственных квантовых процессов. Но мы по-прежнему можем получить доступ к отдельным ветвям этого процесса, выполнив композицию с подходящим классическим эффектом, т. е. подвергнув его подходящему испытанию:



а для получения доступа к каждой компоненте управляемого процесса нужно предоставить соответствующий вход:



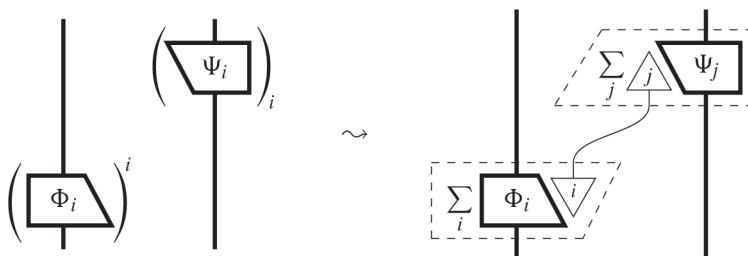
Таким образом, мы можем реконструировать (8.4) посредством

$$\left(\text{box } \Phi_j \right)^j = \left(\sum_i \left(\text{box } \Phi_i \text{ with triangle } j \text{ on top} \right) \right)^j$$

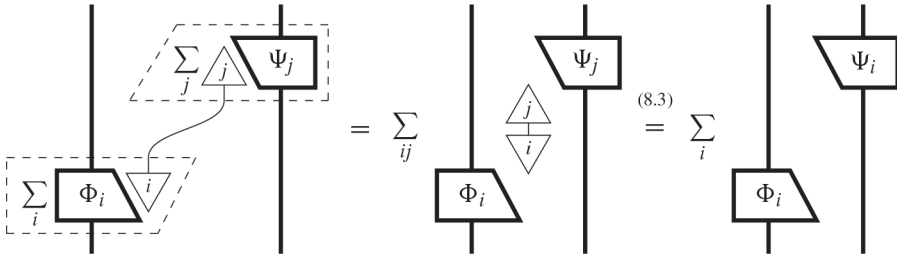
а (8.5) – в виде:

$$\left(\text{box } \Psi_i \right)_i = \left(\sum_j \left(\text{box } \Psi_j \text{ with triangle } i \text{ on left} \right) \right)_i$$

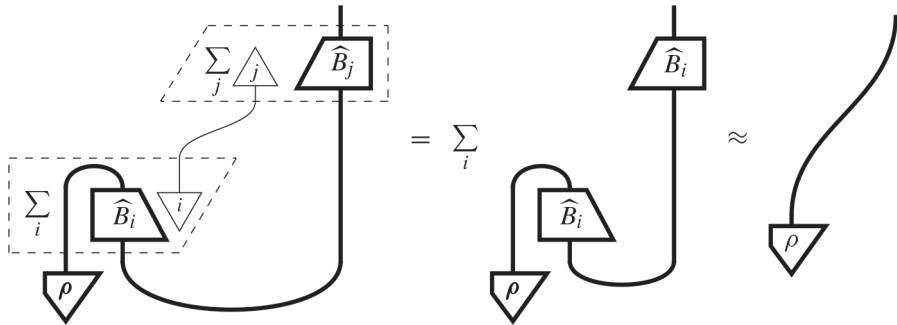
Более того, мы теперь можем соединить проводом i -состояние с i -эффектом, чтобы обозначать классическое взаимодействие:



Обратите внимание, что на правой диаграмме индексы i и j встречаются только локально. Иными словами, линейные отображения в обведенных пунктирной линией блоках – абсолютно независимые процессы. Однако благодаря присутствию соединяющего их классического провода i и j обязаны совпадать вследствие ортонормированности:



Телепортация теперь принимает вид:

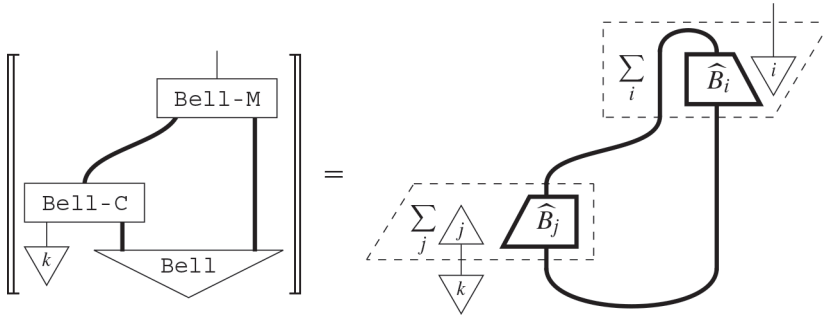


В частности, картина в целом оказывается линейным отображением определенного вида, который мы скоро определим. Очевидно, что такие отображения являются строгим обобщением квантовых отображений, поскольку в них принимают участие и классические системы. Итак, мы смогли устранить синтаксический мусор, который обитал «снаружи» **линейных отображений**, и вернуться к обычным диаграммам процессов, что сулит нам большие преимущества.

8.1.2. Пример: плотное кодирование

Теперь, когда у классических систем появились собственные провода, мы можем рассмотреть протоколы с классическими входами и выходами. Коль скоро телепортация опиралась на классическое взаимодействие (с помощью состояния Белла) для передачи квантового состояния, мы теперь вправе задать встречный вопрос: а нельзя ли использовать квантовое состояние для передачи классического? И если да, то что мы от этого выиграем?

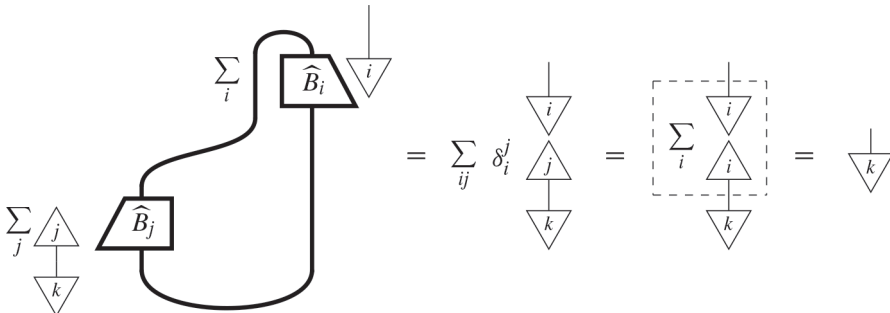
Конечно, магия телепортации была бы невозможной без состояния Белла, поэтому предположим, что оно существует и здесь. Это дает следующую диаграмму спецификации и соответствующую интерпретацию:



Тогда в силу ортонормированности базиса Белла

$$\frac{1}{2} \begin{array}{c} \widehat{B}_j \\ \widehat{B}_i \end{array} = \delta_i^j$$

получаем



Так чего же мы достигли с помощью этого протокола? Рассматриваемая как протокол связи, передача классических данных с помощью квантовых систем представляется несколько тяжеловесным решением. Однако квантовые системы, с которыми мы имеем дело (т. е. толстые провода на картинках), двумерные. С другой стороны, существует четыре состояния Белла, поэтому измерение порождает одно из четырех значений в качестве классического выхода (т. е. тонкие провода на картинках). Таким образом, передав всего один кубит, Алекс передаст два классических бита. Этот результат непосредственно обобщается на D -мерные толстые провода, позволяющие, стало быть, передать D^2 классических значений.

Замечание 8.2. Иногда говорят, что телепортация и плотное кодирование двойственны, мотивируя это перестановкой ролей классических и квантовых каналов (запутанное состояние, конечно, остается квантовым). Однако стоит отметить,

что два свойства матриц Белла – (i) что они порождают унитарные отображения и (ii) что ассоциированные с ними состояния образуют ОНБ – играют разные роли в обоих протоколах. Если телепортация, очевидно, зависит от (i), то ключом к плотному кодированию является (ii). Правда же то, что если кто-то обладает запутанным состоянием заранее, то

- « D -мерный квантовый канал» и
- « D^2 -мерный классический канал»

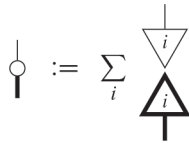
становятся эквивалентны в том смысле, что телепортация позволяет преобразовать классический канал в квантовый, а плотное кодирование – наоборот.

8.1.3. Измеритель и кодировщик

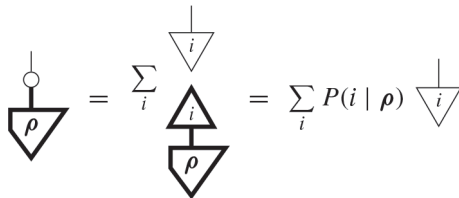
Теперь мы преобразуем квантовый процесс для измерения ОНБ в это новое представление с классическими проводами:



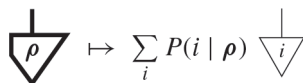
Это линейное отображение настолько важно, что мы будем использовать для него специальное обозначение:



И что же это отображение делает? Давайте применим его к произвольному квантовому состоянию:



Неудивительно, что эти числа в точности совпадают с вероятностями для измерения ОНБ, выведенными по правилу Борна. Таким образом, линейное отображение, представляющее измерение ОНБ, переводит квантовое состояние в распределение вероятностей



всех возможных исходов измерения. В виде матрицы это состояние выглядит так:

$$\begin{array}{c} \circ \\ | \\ \triangleleft \\ \rho \end{array} \Leftrightarrow \begin{pmatrix} P(1 | \rho) \\ P(2 | \rho) \\ \vdots \\ P(D | \rho) \end{pmatrix}$$

Представив измерение ОНБ линейным отображением, которое мы, начиная с этого момента, будем называть *измерителем*, мы можем рассмотреть также его адьюнкт:

$$\begin{array}{c} \circ \\ | \end{array} := \sum_i \begin{array}{c} \downarrow \\ \triangleleft \\ i \\ \triangleleft \\ i \\ | \end{array}$$

Применив это линейное отображение к произвольному распределению вероятностей, получим:

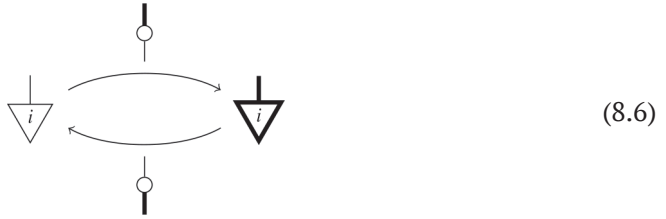
$$\begin{array}{c} \circ \\ | \\ \triangleleft \\ p \end{array} = \sum_i \begin{array}{c} \downarrow \\ \triangleleft \\ i \\ \triangleleft \\ i \\ | \\ \triangleleft \\ p \end{array} = \sum_i p^i \begin{array}{c} \downarrow \\ \triangleleft \\ i \end{array}$$

т. е. кодировку распределения вероятностей в виде квантового состояния, как в предложении 6.74. Поэтому будем называть это линейное отображение *кодировщиком*.

Измерение аннулирует эту операцию. Таким образом, эти два процесса осуществляют взаимное преобразование двух представлений классического распределения вероятностей:

$$\begin{array}{ccc} & \begin{array}{c} \circ \\ | \end{array} & \\ & \leftarrow \quad \rightarrow & \\ \sum_i p^i \begin{array}{c} \downarrow \\ \triangleleft \\ i \end{array} & & \sum_i p^i \begin{array}{c} \downarrow \\ \triangleleft \\ i \end{array} \\ & \leftarrow \quad \rightarrow & \\ & \begin{array}{c} \circ \\ | \end{array} & \end{array}$$

В частности, они преобразуют классические значения в соответствующие квантовые состояния и наоборот:



(8.6)

8.1.4. Классически-квантовые отображения

Хотя процессы измерителя и кодировщика могут показаться весьма специальными, на самом деле это все, что нужно добавить для получения полной теории классически-квантовых отображений. Напомним, что для получения процессной теории **квантовых отображений** мы взяли теорию **чистых квантовых отображений** и добавили в нее один ингредиент (отбрасывание). И точно так же мы можем определить классически-квантовые отображения, добавив два ингредиента в теорию **квантовых отображений**.

Определение 8.3. Классически-квантовым отображением (КК-отображением) называется линейное отображение, полученное композицией двух квантовых отображений: кодировщика и измерителя.



(8.7)

Ассоциированную процессную теорию будем называть теорией **КК-отображений**.

Прежде чем двигаться дальше, докажем следующую теорему.

Теорема 8.4. Теория **КК-отображений** допускает струнные диаграммы.

Доказательство. Поскольку измеритель – адъюнкт кодировщика, теория **КК-отображений** наследует адъюнкцию от теории **линейных отображений**. В главе 6 мы видели, как строятся чашки и крышки для квантовых систем, поэтому нужно только показать, как это делается для классических систем. Они получают-ся таким образом:



В следующем разделе мы увидим очень простой способ доказывать подобные равенства, а пока оставим доказательство (совсем несложное) в качестве упражнения. □

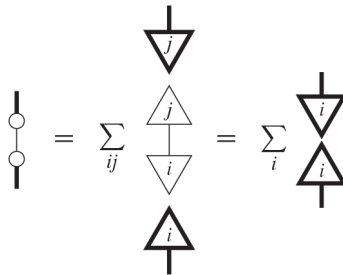
Кроме того, мы всегда можем привести КК-отображения к «нормальной форме» – точно так же, как это было сделано в предложении 6.46 для квантовых отображений.

Предложение 8.5. Любое КК-отображение имеет вид:

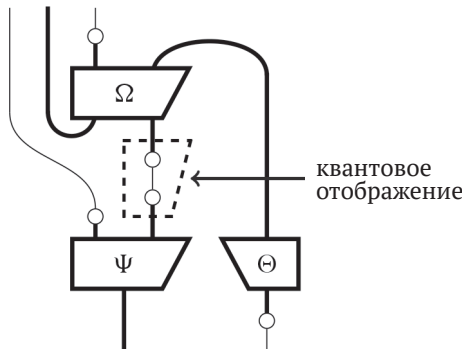


с точностью до изменения порядка некоторых входных или выходных проводов.

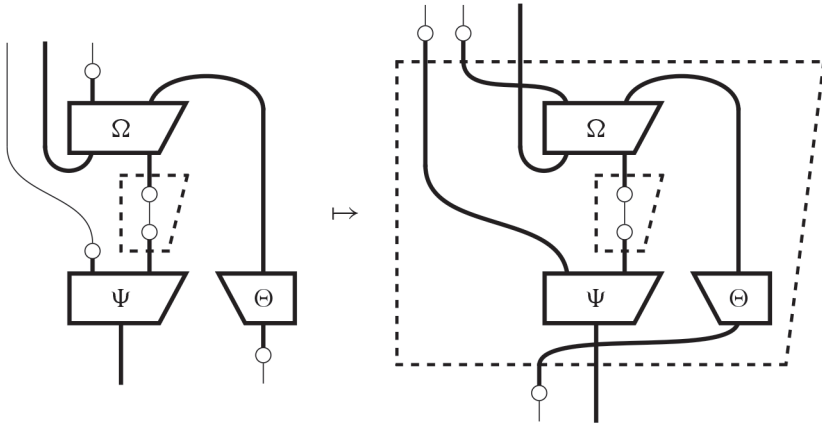
Доказательство. Утверждение доказывается почти так же, как предложение 6.46, устанавливающее стандартную форму для квантовых отображений. Сначала заметим, что при каждом соединении классических проводов от измерителя и кодировщика возникает квантовое отображение:



Поэтому всякое КК-отображение можно записать как квантовое отображение с какими-то измерителями на выходах и кодировщиками на входах:



Затем, переупорядочив некоторые входы и выходы, мы можем собрать все процессы измерения и кодирования вместе:



что дает процесс вида:

(8.9)

Как и в случае отбрасывания, несколько процессов измерения можно объединить в один процесс в большей системе:

$$\begin{array}{c} A \\ | \\ \circ \\ | \\ \hat{A} \end{array} \quad \begin{array}{c} B \\ | \\ \circ \\ | \\ \hat{B} \end{array} = \sum_i \begin{array}{c} \downarrow \\ i \\ \nabla \\ \uparrow \\ i \end{array} \sum_j \begin{array}{c} \downarrow \\ j \\ \nabla \\ \uparrow \\ j \end{array} = \sum_{ij} \begin{array}{c} \downarrow \\ i \\ \nabla \\ \uparrow \\ i \end{array} \begin{array}{c} \downarrow \\ j \\ \nabla \\ \uparrow \\ j \end{array} = \begin{array}{c} A \otimes B \\ | \\ \circ \\ | \\ \hat{A} \otimes \hat{B} \end{array} \quad (8.10)$$

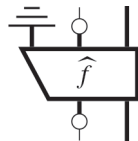
где правая часть – процесс измерения для ОНБ:

$$\left\{ \begin{array}{c} \downarrow \\ i \\ \nabla \\ \uparrow \\ i \end{array} \begin{array}{c} \downarrow \\ j \\ \nabla \\ \uparrow \\ j \end{array} \right\}_{ij}$$

Процессы кодирования можно объединять аналогично. Таким образом, объединение процессов измерения и кодирования в (8.9) дает процесс вида (8.8).

Тогда путем очищения квантового отображения Φ выше получаем:

Следствие 8.6. Любое КК-отображение имеет вид:



Замечание 8.7. В этой главе мы будем предполагать, что каждая классическая система имеет свой собственный «предпочтительный» ОНБ, который будем обозначать белыми треугольниками. Следовательно, ОНБ в системах A и B в равен-

стве (8.10) будут различны, если $A \neq B$. В главе 9, где изучается взаимодействие между разными ОНБ одной и той же системы, мы избавимся от этого предположения, но тогда нужно будет несколько аккуратнее обращаться с классическими проводами. См. раздел 9.2.

Но какое отношение определение 8.3 имеет к усилиям, предпринятым в предыдущих разделах? Ранее мы показали, как однозначно выразить квантовые процессы в виде линейных отображений:

$$\left(\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \right)_i^j \sim \sum_{ij} \left(\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \right)_i^j \quad (8.11)$$

Теперь можно показать, что такие линейные отображения в действительности являются КК-отображениями. Сначала свернем все Φ_{ij} с помощью дублированных состояний и эффектов, принадлежащих ОНБ:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} := \sum_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad (8.12)$$

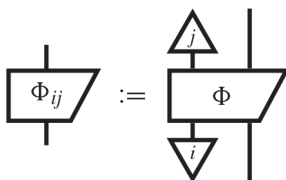
Поскольку это сумма квантовых отображений, то по теореме 6.67 Φ само является квантовым отображением. Поэтому линейное отображение (8.11) – действительно КК-отображение:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \stackrel{(8.12)}{=} \sum_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \stackrel{(8.6)}{=} \sum_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

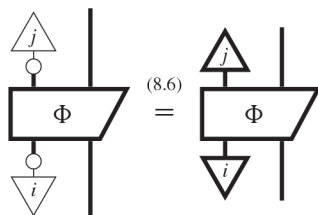
Обратно, любое КК-отображение имеет вид (8.11):

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \stackrel{(5.17)}{=} \sum_j \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \stackrel{(8.6)}{=} \sum_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \stackrel{(8.6)}{=} \sum_{ij} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \Phi \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

где



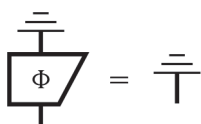
Поэтому для общего КК-отображения квантовые отображения Φ_{ij} являются в точности теми ветвями этого отображения, которые были выбраны посредством классических входов и выходов:



Однако в определении 6.100 квантовых процессов был важный дополнительный нюанс, которого у КК-отображений пока еще нет. А именно ничто не гарантирует, что в совокупности эти ветви отвечают принципу причинности (6.77). Чтобы разобраться с этим элегантно, без привлечения сумм, нам понадобится еще один диаграммный компонент.

8.1.5. Удаление и причинность

Когда-то давно, еще до включения недетерминированности в общую картину, у нас было простое и красивое равенство, отражающее причинность:



Если отбросить все исходящее из процесса наружу, то можно было бы вообще обойтись без процесса и отбросить все входящее в него. Чтобы обобщить это на КК-отображение, нужно просто определить, что значит «отбрасывание» классической системы. Для этого введем новый процесс, называемый *удалением*:



Из самого названия ясно, что такой процесс должен делать с любым классическим значением j :



но тогда, поскольку все классические значения вместе образуют ОНБ, удаление оказывается определено полностью и однозначно:

$$\text{⊖} := \sum_i \text{⊖}_i \quad (8.14)$$

Может возникнуть мысль, что его необходимо включить в теорию **КК-отображений** вручную, но фактически оно там уже есть:

$$\text{⊖} \stackrel{(5.37)}{=} \sum_i \text{⊖}_i \stackrel{(8.6)}{=} \sum_i \text{⊖}_i \stackrel{(8.14)}{=} \text{⊖} \quad (8.15)$$

что, конечно, совершенно разумно. Если мы закодируем какие-то классические данные как квантовую систему, а затем отбросим эту систему, то получится то же самое, как если бы мы просто удалили данные. Тогда напрашивается следующее определение.

Определение 8.8. КК-отображение называется *каузальным*, если:

$$\text{⊖} \stackrel{\text{causal}}{=} \text{⊖} \quad (8.16)$$

А это на самом деле эквивалентно нашему прежнему определению каузальности.

Предложение 8.9. Для КК-отображения

$$\text{⊖} \quad (8.17)$$

определения каузальности 6.100 и 8.8 совпадают.

Доказательство. КК-отображение (8.17) кодирует квантовый процесс

$$\left(\text{⊖}_{ij} \right)_i, \quad \text{где} \quad \text{⊖}_{ij} := \text{⊖}_{ij}$$

Предполагая, что каузальность определена как в определении 8.8, получаем следующие равенства для всех i :

Определение 8.10. Теорией **квантовых процессов** называется подтеория КК-отображений, состоящая из всех каузальных КК-отображений.

Поскольку удаление – это просто классический аналог отбрасывания:



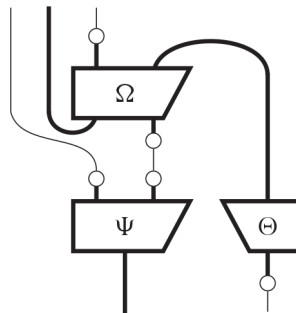
то определение 8.8 – лишь небольшое дополнение к нашему исходному девизу:

если все квантовые/классические выходы квантового процесса отбрасываются/удаляются, то это все равно, что этого процесса никогда и не существовало.

Итак, нам удалось (как и было обещано) расширить интерпретацию каузальности квантовых отображений из раздела 6.2.4 на квантовые процессы, которые могут содержать также классические входы и выходы. Таким образом, классические и квантовые входы с точки зрения каузальности теперь уравниены в правах. Следовательно, любое утверждение о каузальности квантовых отображений непосредственно переносится на квантовые процессы. Например, результаты, касающиеся несигнальности, установленные в разделе 6.3.2, теперь применимы и к общим квантовым процессам.

8.2. ОТ ПАУКОВ К КЛАССИЧЕСКИМ ОТОБРАЖЕНИЯМ

Теперь у нас имеется полноправная теория **квантовых процессов**, охватывающая как классические, так и квантовые системы в виде проводов. Это позволяет рассуждать о таких процессах с помощью диаграмм:



К сожалению, эти диаграммы содержат весьма специфичные линейные отображения, а именно измеритель и кодировщик, и для установления равенств между диаграммами нам неизбежно придется использовать их явные формы:



в которых участвуют ОНБ-состояния и суммы. Это неудобно.

В этом и в следующем разделах мы разработаем лучшее решение. Мы представим измеритель и кодировщик как чисто диаграммные сущности, что позволит нам выводить равенства между диаграммами **квантовых процессов**, вообще не прибегая к явным матричным формам измерителя и кодировщика.

Для этого нам нужно будет лучше понять, что такое классические процессы. Мы собрали довольно разнообразный арсенал квантовых отображений, но почти ничего не сказали об их классических аналогах. Одно классическое отображение (удаление) мы уже видели и познакомимся еще с несколькими, прежде чем установим, что все они являются частными случаями очередной диаграммной революции, которая грядет в этой книге: правления пауков!

8.2.1. Классические отображения

Ограничив определение 8.3, мы придем к следующему определению.

Определение 8.11. *Классическим отображением* называется КК-отображение, имеющее только классические входы и выходы, т. е. линейное отображение f вида:

$$\begin{array}{c} | \\ \hline f \\ \hline | \end{array} := \begin{array}{c} \circ \\ | \\ \hline \Phi \\ \hline | \\ \circ \end{array} \tag{8.18}$$

а *классическим процессом* – классическое отображение, являющееся каузальным:

$$\begin{array}{c} | \\ \hline f \\ \hline | \end{array} = \begin{array}{c} \circ \\ | \\ \circ \end{array}$$

Записывая классическое отображение в виде суммы по ветвям, как в (8.11), получаем:

$$\begin{array}{c} \circ \\ | \\ \hline \Phi \\ \hline | \\ \circ \end{array} = \sum_{ij} \begin{array}{c} \triangleleft j \\ \triangleleft i \end{array} \diamond \Phi_{ij}$$

Конечно, квантовые отображения без входов и выходов – это просто положительные числа, поэтому классическое отображение – не что иное, как матрица положительных чисел:

$$\sum_{ij} p_i^j \begin{array}{c} \triangleleft j \\ \triangleleft i \end{array} \leftrightarrow \begin{pmatrix} p_1^1 & p_2^1 & \cdots & p_m^1 \\ p_1^2 & p_2^2 & \cdots & p_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ p_1^n & p_2^n & \cdots & p_m^n \end{pmatrix}$$

В частности, классические состояния – это просто векторы, состоящие из положительных вещественных чисел:

$$\sum_j p^j \downarrow_j \leftrightarrow \begin{pmatrix} p^1 \\ p^2 \\ \vdots \\ p^n \end{pmatrix}$$

Для классических процессов каузальность сводится к

$$\forall i : \sum_j p_i^j = 1.$$

То есть в матрицах классических процессов все элементы положительные, а сумма элементов в каждом столбце равна 1. Для классических состояний каузальность принимает вид:

$$\sum_j p^j = 1,$$

т. е. каузальные классические состояния – это в точности распределения вероятностей!

Матрицы классических процессов часто называются *стохастическими матрицами*, а сами линейные отображения – *стохастическими отображениями*. Слово «стохастический» – по существу, синоним слова «случайный», и стохастические отображения соответствуют процессам, воздействующим на распределения вероятностей, так что некоторый элемент случайности присутствует. Если квантовые процессы – это наиболее общие отображения, переводящие одно каузальное квантовое состояние в другое, то стохастические отображения – это самые общие отображения, переводящие одно распределение вероятностей в другое.

Пример 8.12. Представьте себе процесс, который принимает классический бит и с вероятностью 1/3 изменяет его на противоположный (т. е. с вероятностью 2/3 оставляет бит неизменным). Его можно было бы описать таким стохастическим отображением:

$$\begin{array}{|c} \hline \diagdown \\ \hline f \\ \hline \diagup \\ \hline \end{array} \leftrightarrow \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix} \tag{8.19}$$

Если мы введем бит 0

$$\begin{array}{|c} \hline \diagdown \\ \hline f \\ \hline \diagup \\ \hline 0 \\ \hline \end{array} = \frac{2}{3} \begin{array}{|c} \hline \diagdown \\ \hline \\ \hline \diagup \\ \hline 0 \\ \hline \end{array} + \frac{1}{3} \begin{array}{|c} \hline \diagdown \\ \hline \\ \hline \diagup \\ \hline 1 \\ \hline \end{array}$$

то получим бит 0 с вероятностью 2/3 и бит 1 с вероятностью 1/3. Если же мы введем бит 1, то результат будет противоположным:

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \triangle 1 \end{array} = \frac{1}{3} \begin{array}{c} \downarrow \\ \triangle 0 \end{array} + \frac{2}{3} \begin{array}{c} \downarrow \\ \triangle 1 \end{array}$$

Детерминированный классический процесс переводит любое ОНБ-состояние в одно (и только одно) ОНБ-состояние, т. е. действует как функция от классического значения. Отсюда вытекает следующее

Определение 8.13. Классический процесс f называется *детерминированным*, если существует функция

$$f : \{1, \dots, m\} \mapsto \{1, \dots, n\}$$

такая, что

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \triangle i \end{array} = \begin{array}{c} \downarrow \\ \triangle f(i) \end{array} \tag{8.20}$$

Для краткости мы будем называть детерминированные классические процессы *функциональными отображениями*. Чтобы убедиться в том, что любое линейное отображение, описываемое равенством (8.20), автоматически является классическим процессом, достаточно изучить его матрицу. Ее элементы равны 0 или 1, т. е. являются положительными числами¹. Кроме того, в каждом столбце присутствует ровно одна единица, откуда сразу следует каузальность.

Ограничив определение 8.13 на состояния, мы заключаем, что детерминированные классические состояния – это просто ОНБ-состояния, иначе говоря, точечные распределения (см. раздел 5.1.4). Детерминированные состояния – это классический аналог чистых квантовых состояний, т. к. они не получаются (нетривиальным) смешением распределений вероятностей.

Упражнение 8.14. Покажите, что если

$$\begin{array}{c} \downarrow \\ \triangle p \end{array} = \sum_i \begin{array}{c} \downarrow \\ \triangle q_i \end{array}$$

то p является детерминированным классическим состоянием тогда и только тогда, когда для любого i имеет место

$$\begin{array}{c} \downarrow \\ \triangle p \end{array} \approx \begin{array}{c} \downarrow \\ \triangle q_i \end{array}$$

Упражнение 8.15. Напомним (см. замечание 8.7), что все понятия, введенные в этом разделе, зависят от конкретного выбора ОНБ для каждого классического

¹ Авторы допускают вольность речи, называя 0 положительным числом, хотя в русскоязычной литературе принято относить его к неотрицательным числам. – *Прим. перев.*

типа. Действительно, если выразить матрицу классического отображения или состояния в другом ОНБ, то обычно элементы уже не будут положительными. Найдите ОНБ, в котором матрица стохастического отображения (8.19) имеет неположительные элементы.

Теперь давайте рассмотрим некоторые очень специальные классические процессы.

8.2.2. Копирование и удаление

Классические данные можно не только удалять, но и копировать. Но вот что удивительно, так это то, что у некоторых особенностей квантовых процессов, связанных с отбрасыванием, нет классических аналогов, связанных с удалением. И прежде всего это относится к очищению. Иными словами, возможность очищения – характеристическая особенность квантовых процессов. С другой стороны, у копирования нет аналога в квантовых системах (см. раздел 4.4.2), так что это типично классический процесс. Поэтому вместо того чтобы считать невозможность клонирования недостатком квантовых систем, мы будем рассматривать *возможность копирования* (или *возможность клонирования*) характеристической особенностью классических.

8.2.2.1. Удаление

Выше мы видели, что удаление – это классический аналог отбрасывания и потому является единственным каузальным эффектом в классической системе.

Точно так же адьюнкт удаления

$$\frac{1}{D} \circlearrowleft = \frac{1}{D} \sum_i \triangleleft_i$$

является классическим аналогом максимального смешанного состояния:

$$\frac{1}{D} \underline{\underline{\circlearrowleft}} = \frac{1}{D} \sum_i \underline{\underline{\triangleleft_i}}$$

У этого классического состояния есть стандартное название.

Определение 8.16. Классическое состояние

$$\frac{1}{D} \circlearrowleft$$

называется *равномерным распределением вероятностей*.

В квантовом случае у нас было понятие редуцированных квантовых состояний (см. предложение 6.33):

$$\underline{\underline{\triangleleft_i}} \hat{\psi}$$

Так и в случае состояния двух классических систем, если мы удалим одну из систем:

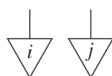
$$\begin{array}{c} \circ \\ | \\ \triangleleft \\ x \end{array} \stackrel{(8.14)}{=} \sum_i \begin{array}{c} \triangleleft \\ i \\ | \\ \triangleleft \\ x \end{array}$$

то получим знакомую теоретико-вероятностную операцию, называемую *маргинализацией*. Классическое состояние (читай: распределение вероятностей) x после удаления одной из систем называется *маргинальным* распределением.

Хотя у редуцированных состояний есть естественные классические аналоги, имеющие много практических применений, для классического мира характерен один примечательный недостаток:

у очищения квантовых состояний нет классического аналога.

Другими словами, не всякое классическое состояние может быть реализовано как маргинал детерминированного классического состояния. Все детерминированные классические состояния двух систем имеют вид:



Далее, очевидно, что удаление одной системы снова дает детерминированное состояние. Отсюда следует, что единственные состояния, которые можно «очистить» до детерминированного состояния, изначально являлись детерминированными!

Сравнивая эту ситуацию с квантовым случаем, мы можем представить распределения вероятностей как квантовые состояния (см. предложение 6.74):

$$\sum_i p^i \begin{array}{c} \downarrow \\ i \end{array}$$

Это действительно квантовое состояние и потому может быть очищено:

$$\sum_i p^i \begin{array}{c} \downarrow \\ i \end{array} = \begin{array}{c} \overline{\overline{}} \\ | \\ \triangleleft \\ \widehat{\psi} \end{array}$$

В явном виде для

$$\begin{array}{c} \downarrow \\ \psi \end{array} := \boxed{\sum_i \sqrt{p^i} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array}}$$

мы действительно имеем

$$\boxed{\sum_i \sqrt{p^i} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array}} \boxed{\sum_j \sqrt{p^j} \begin{array}{c} \downarrow \\ j \end{array} \begin{array}{c} \downarrow \\ j \end{array}} = \sum_i p^i \begin{array}{c} \downarrow \\ i \end{array}$$

Таким образом, магия очищения проистекает из того факта, что у квантовых состояний есть два способа комбинирования процессов посредством суммирования, смешивания и суперпозиции:

$$\sum_i p^i \text{ (triangle with } \psi_i \text{)} \quad \text{и} \quad \text{double} \left(\sum_i \sqrt{p^i} \text{ (triangle with } \psi_i \text{)} \right), -$$

и именно последнее обладает дополнительной гибкостью для очищения любого квантового состояния.

8.2.2.2. Копирование

Определение 8.17. Копированием называется следующее классическое отображение:

$$\text{(circle with two lines)} := \sum_i \begin{matrix} \downarrow i & \downarrow i \\ \uparrow i \end{matrix}$$

Это отображение также ведет себя, как ожидается, на базисных состояниях:

$$\begin{matrix} \downarrow j \\ \text{(circle with two lines)} \\ \downarrow j \end{matrix} = \sum_i \begin{matrix} \downarrow i & \downarrow i \\ \uparrow i \\ \downarrow j \end{matrix} = \begin{matrix} \downarrow j & \downarrow j \end{matrix} \tag{8.21}$$

В действительности состояние копируется отображением $\text{(circle with two lines)}$ тогда и только тогда, когда оно является базисным.

Теорема 8.18. Копирование однозначно определяет ОНБ. Точнее, для любого ненулевого состояния ψ :

$$\begin{matrix} \downarrow \psi \\ \text{(circle with two lines)} \\ \downarrow \psi \end{matrix} \in \left\{ \begin{matrix} \downarrow i \\ \text{(circle with two lines)} \\ \downarrow i \end{matrix} \right\}_i \text{ тогда и только тогда, когда } \begin{matrix} \downarrow \psi \\ \text{(circle with two lines)} \\ \downarrow \psi \end{matrix} \stackrel{(*)}{=} \begin{matrix} \downarrow \psi & \downarrow \psi \end{matrix}$$

Доказательство. Сначала заметим, что копирование является изометрией:

$$\begin{matrix} \text{(circle with two lines)} \\ \text{(circle with two lines)} \end{matrix} = \sum_j \begin{matrix} \downarrow j & \downarrow j \\ \uparrow j & \uparrow j \\ \downarrow i & \downarrow i \end{matrix} = \sum_i \begin{matrix} \downarrow i & \downarrow i \\ \uparrow i \end{matrix} = \left| \right. \tag{8.22}$$

В предположении (*) отсюда следует, что

$$\begin{array}{c} \psi \\ \downarrow \\ \psi \end{array} \stackrel{(8.22)}{=} \begin{array}{c} \psi \\ \circ \\ \circ \\ \psi \end{array} = \begin{array}{c} \psi \\ \downarrow \\ \psi \end{array} \begin{array}{c} \psi \\ \downarrow \\ \psi \end{array}$$

Уравнение $p = p^2$ имеет всего два решения: 0 и 1, поэтому ψ обязано быть нормированным. Из теоремы 4.85 мы знаем, что нормированные состояния, допускающие совместное клонирование изометрией, должны быть ортогональны. Поскольку, в силу (8.21), ОНБ-состояния также скопированы, отсюда следует, что ψ должно быть либо ОНБ-состоянием, либо ортогонально любому ОНБ-состоянию. Но единственное состояние, ортогональное любому ОНБ-состоянию, – это 0, поэтому ψ должно совпадать ровно с одним из ОНБ-состояний. \square

Таким образом, не только каждый ОНБ, состоящий из классических состояний, определяет отображение копирования, но и обратно – отображение копирования однозначно определяет ОНБ. Более того, возможность копирования дает диаграммную характеристику детерминированных классических процессов.

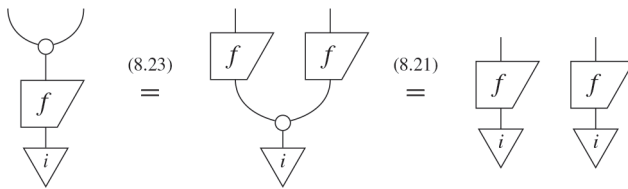
Предложение 8.19. Линейное отображение f является функциональным отображением (т. е. детерминированным классическим процессом) тогда и только тогда, когда оно удовлетворяет следующим двум условиям:

$$\begin{array}{c} \circ \\ \downarrow \\ \downarrow \\ f \end{array} = \begin{array}{c} \downarrow \quad \downarrow \\ f \quad f \\ \downarrow \\ \circ \end{array} \quad \begin{array}{c} \circ \\ f \end{array} = \begin{array}{c} \circ \end{array} \quad (8.23)$$

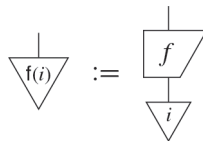
Доказательство. Сначала предположим, что f – функциональное отображение. По определению 5.2, линейные отображения равны, если они совпадают на некотором ОНБ, поэтому для доказательства обоих равенств достаточно выполнить композицию с ОНБ-состояниями:

$$\begin{array}{c} \circ \\ \downarrow \\ f \\ \downarrow \\ i \end{array} \stackrel{(8.20)}{=} \begin{array}{c} \circ \\ \downarrow \\ f(i) \end{array} \stackrel{(8.21)}{=} \begin{array}{c} \downarrow \quad \downarrow \\ f(i) \quad f(i) \end{array} \stackrel{(8.20)}{=} \begin{array}{c} \downarrow \quad \downarrow \\ f \quad f \\ \downarrow \quad \downarrow \\ i \quad i \end{array} \stackrel{(8.21)}{=} \begin{array}{c} \downarrow \quad \downarrow \\ f \quad f \\ \downarrow \\ \circ \\ \downarrow \\ i \end{array}$$

Второе равенство доказывается аналогично. Обратно, имеем:



Таким образом, $f \circ i$ копируется отображением копирования и, в силу второго равенства (8.23), отлично от нуля. Тогда, по теореме 8.18, состояние $f \circ i$ должно быть ОНБ-состоянием. Следовательно, функцию f можно определить следующим образом:



□

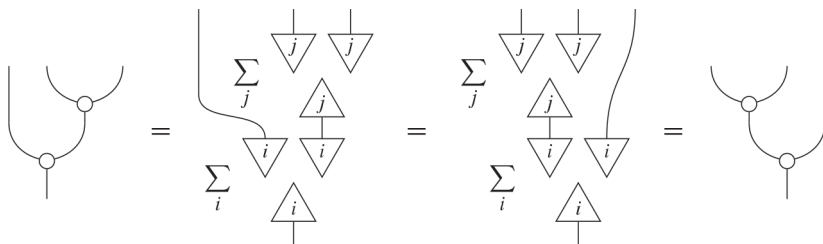
Системы на входе и выходе f (и, значит, операции копирования в левой и правой частях равенства выше) могут быть различны. В частности, копирование ОНБ-состояний – просто частный случай, когда система на входе f тривиальна.

Естественно ожидать, что если копируются классические данные, то две одинаковые копии можно беспрепятственно переставить местами. Кроме того, если одну из получившихся копий скопировать еще раз, то оба способа получения трех копий будут одинаковы. Так оно и есть в действительности.

Предложение 8.20. Имеют место равенства:



Доказательство. Раскрывая определения, имеем:



и

$$\text{Loop with dot} = \sum_i \text{Crossed triangles} = \sum_i \text{Parallel triangles} = \text{Loop with dot}$$

8.2.2.3. Копирование и удаление

Можно также ожидать, что если скопировать классические данные, а затем одну копию удалить, то результат получится такой, как будто мы вообще ничего не делали. И это тоже правда.

Предложение 8.21. Имеют место равенства:

$$\text{Loop with dot} = | = \text{Loop with dot} \tag{8.26}$$

Доказательство. Раскрывая определения, имеем:

$$\text{Loop with dot} = \sum_j \text{Down triangle with line} = \sum_i \text{Up triangle with line} = |$$

Отметим, что отсюда немедленно следует каузальность копирования, т. к. удаление выходов – то же самое, что удаление входа:

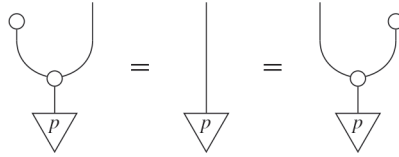
$$\text{Loop with dot} = \text{Dot on line}$$

Замечание* 8.22. Ранее в замечании 3.17 мы сказали, что копирование – пример коумножения. Равенства (8.24) и (8.25) означают, что копирование коассоциативно и кокоммутативно – это коалгебраические аналоги ассоциативности и коммутативности соответственно. Равенство (8.26) означает, что операция удаления – это коединица, т. е. коалгебраический аналог единицы в алгебре. Наконец, равенства в предложении 8.19 означают, что функциональные отображения являются гомоморфизмами комоноидов.

В (6.48) мы видели, что клонирование невозможно для распределения вероятностей общего вида, и действительно:

$$\text{Loop with dot} = \sum_i p^i \text{Parallel triangles} \neq \left(\sum_i p^i \text{Triangle} \right) \left(\sum_j p^j \text{Triangle} \right)$$

Однако распределения вероятностей можно распространять. В самом деле, мы можем интерпретировать *распространение* как существование отображения, которое можно применить к любому классическому состоянию p и такого, что и Алекс, и Боб смогут восстановить p , просто удалив вторую систему:

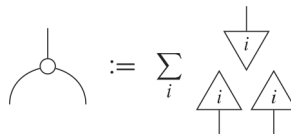


Итак, мы имеем два эквивалентных способа выразить распределения вероятностей, а также ассоциированные с ними операции копирования и удаления:

| | | |
|-----------------------------|--|---|
| Состояние | $\downarrow_p := \sum_i p^i \downarrow_i$ | $\Downarrow_p := \sum_i p^i \Downarrow_i$ |
| Копирование/распространение | $\curvearrowright := \sum_i \begin{matrix} \downarrow_i & \downarrow_i \\ \uparrow_i \end{matrix}$ | $? := \sum_i \begin{matrix} \Downarrow_i & \Downarrow_i \\ \Uparrow_i \end{matrix}$ |
| Удаление/отбрасывание | $\circ := \sum_i \Uparrow_i$ | $\bar{\Uparrow} := \sum_i \Uparrow_i$ |

8.2.2.4. Сравнение

Сравнение – операция, адъюнктивная копированию:



Это классическое отображение принимает два ОНБ-состояния. Если оба состояния одинаковы, то оно возвращает это состояние, в противном случае возвращается нулевое состояние:

$$\begin{matrix} \circ \\ \swarrow \quad \searrow \\ \triangle_i \quad \triangle_j \end{matrix} = \delta_i^j \downarrow_i \tag{8.27}$$

Замечание 8.23. Операция сравнения, в отличие от своего адъюнкта, не является каузальной. В частности, образом распределения вероятностей не является распределение вероятностей. Тем не менее операция имеет понятную семантику и оказывается полезной.

Мы можем просто применить адъюнкцию к равенствам (8.24), (8.25) и (8.26) и получить соответствующие им равенства для операции сравнения.

Предложение 8.24. Имеют место равенства:

$$\begin{array}{c} \circ \\ | \\ \text{---} \circ \\ | \quad | \\ \text{---} \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \circ \\ | \quad | \\ \text{---} \end{array} \quad (8.28)$$

$$\begin{array}{c} \circ \\ | \\ \text{---} \circ \\ | \quad | \\ \text{---} \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \end{array} \quad (8.29)$$

$$\begin{array}{c} \circ \\ | \\ \text{---} \circ \\ | \quad | \\ \text{---} \end{array} = | = \begin{array}{c} \circ \\ | \\ \text{---} \circ \\ | \quad | \\ \text{---} \end{array} \quad (8.30)$$

где адьюнктом удаления является операция

$$\begin{array}{c} \circ \\ | \\ \text{---} \end{array} := \sum_i \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \quad (8.31)$$

Замечание* 8.25. Равенства (8.28), (8.29) и (8.30) – не столь экзотические, алгебраические варианты коалгебраических равенств из замечания 8.22, они выражают ассоциативность, коммутативность и унитарность.

Для произвольных состояний

$$\begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \psi := \sum_i \psi^i \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \phi := \sum_j \phi^j \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array}$$

операция сравнения означает поэлементное умножение матриц:

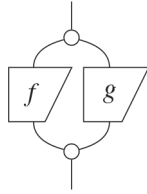
$$\begin{array}{c} \circ \\ | \\ \text{---} \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \psi \quad \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \phi \end{array} = \sum_i \psi^i \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \phi = \sum_{ij} \psi^i \phi^j \delta_{ij} \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \psi = \sum_i \psi^i \phi^i \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \psi$$

В виде операции над матрицами она записывается так:

$$\begin{array}{c} \circ \\ | \\ \text{---} \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \psi \quad \begin{array}{c} \downarrow \\ | \\ \text{---} \end{array} \phi \end{array} \leftrightarrow \begin{pmatrix} \psi^1 \\ \vdots \\ \psi^D \end{pmatrix} \star \begin{pmatrix} \phi^1 \\ \vdots \\ \phi^D \end{pmatrix} := \begin{pmatrix} \psi^1 \phi^1 \\ \vdots \\ \psi^D \phi^D \end{pmatrix} \quad (8.32)$$

Иногда операцию \star называют *произведением Адамара*, или *произведением Шура*, она обобщается на произвольные матрицы.

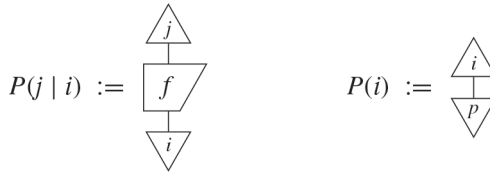
Упражнение 8.26. Покажите, что для любых двух линейных отображений f и g одного типа диаграмма



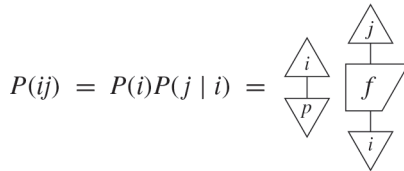
дает произведение Адамара матриц

$$\begin{pmatrix} f_1^1 & \cdots & f_D^1 \\ \vdots & \ddots & \vdots \\ f_1^D & \cdots & f_D^D \end{pmatrix} \star \begin{pmatrix} g_1^1 & \cdots & g_D^1 \\ \vdots & \ddots & \vdots \\ g_1^D & \cdots & g_D^D \end{pmatrix} = \begin{pmatrix} f_1^1 g_1^1 & \cdots & f_D^1 g_D^1 \\ \vdots & \ddots & \vdots \\ f_1^D g_1^D & \cdots & f_D^D g_D^D \end{pmatrix}$$

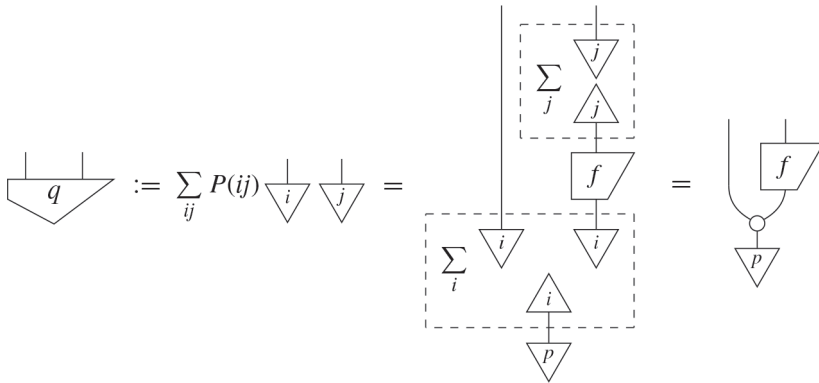
Пример 8.27. Еще одно применение отображения копирования – преобразование каузальных классических отображений в каузальные двухкомпонентные классические состояния. В теории вероятностей первые называются *условными распределениями вероятностей*, а вторые – *совместными распределениями вероятностей*. Пусть некоторые вероятности записаны в терминах классического отображения и конкретного входного состояния:



В терминологии теории вероятностей $P(i)$ называются *априорными вероятностями*. Вместе с условными вероятностями они используются для вычисления совместных вероятностей $P(ij)$, т. е. вероятностей того, что «события i и j произошли одновременно»:



Поскольку это дает распределение вероятностей, мы можем образовать новое классическое состояние двух систем:



что дает нам выражение совместного распределения. Получившееся состояние каузальное, потому что таковыми являются f, p и копирование.

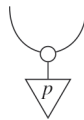
Мы можем также пойти в другом направлении и преобразовать совместное распределение в условное. Для этого нам понадобится *обратное состояние*:

$$\downarrow p^{-1} := \sum_i \frac{1}{p^i} \downarrow i$$

или, эквивалентно, единственное классическое состояние, удовлетворяющее условию

(8.33)

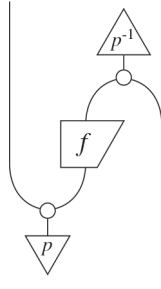
(Если вас беспокоит деление на ноль, см. соглашение 8.29 ниже.) Тогда, считая



«чашкой», мы можем построить ассоциированную «крышку» с помощью p^{-1} :

(8.34)

Это равенство следует непосредственно из (8.33) и правила «слияния пауков», которое мы скоро явим миру. А пока для доказательства (8.34) можно воспользоваться определениями копирования/объединения. Комбинирование крышки и чашки дает нам способ преобразовать $P(j | i)$ в $P(i | j)$, называемый *байесовской инверсией*:



Упражнение* 8.28. Для классического отображения

$$\begin{array}{|c} \hline f \\ \hline \end{array} \leftrightarrow \begin{pmatrix} 1/3 & 1/2 \\ 2/3 & 1/2 \end{pmatrix}$$

вычислите ассоциированные совместные распределения для следующих априорных распределений:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

Затем вычислите байесовскую инверсию f для этих состояний.

Соглашение 8.29. В определении обратного состояния выше мы неявно предполагали, что у нашего распределения вероятностей имеется *полный носитель*, т. е.

$$\begin{array}{|c} \hline p \\ \hline \end{array} := \sum_i p^i \begin{array}{|c} \hline i \\ \hline \end{array}, \quad \text{где} \quad \forall i : p^i \neq 0. \quad (8.35)$$

Если мы свободны в выборе размерности классической системы, то это предположение не ограничивает общность: мы всегда можем перейти от любого распределения вероятностей к распределению с полным носителем в системе меньшей размерности, избавившись от классических значений, встречающихся с нулевой вероятностью.

8.2.3. Пауки

Нам встречались следующие классические отображения, допускающие естественную интерпретацию как операции с классическими данными:

- *копирование и удаление:*

$$\begin{array}{c} \cup \\ \circ \\ | \end{array} := \sum_i \begin{array}{c} \downarrow i \\ \downarrow i \\ \uparrow i \end{array} \qquad \begin{array}{c} \circ \\ | \end{array} := \sum_i \begin{array}{c} \uparrow i \\ | \end{array}$$

- *сопоставление и (ненормированное) равномерное состояние:*

$$\begin{array}{c} \cup \\ \circ \\ \cup \end{array} := \sum_i \begin{array}{c} \downarrow i \\ \uparrow i \\ \uparrow i \end{array} \qquad \begin{array}{c} \circ \\ | \end{array} := \sum_i \begin{array}{c} \downarrow i \\ | \end{array}$$

Но зачем останавливаться на этом? Мы можем добавить, например:

- состояния и эффекты, представляющие *прямолинейную корреляцию* двух классических систем:

$$\begin{array}{c} \cup \\ \circ \\ \cup \end{array} := \sum_i \begin{array}{c} \downarrow i \\ \downarrow i \end{array} \qquad \begin{array}{c} \circ \\ \cup \end{array} := \sum_i \begin{array}{c} \uparrow i \\ \uparrow i \end{array}$$

Можно вывести различные равенства (и их адъюнкты), имеющие естественные интерпретации, аналогичные (8.24), (8.25) и (8.26), например:

- *копирование*, за которым следует *сопоставление*, эквивалентно «ничегонеделанью»:

$$\begin{array}{c} \circ \\ \cup \\ \cup \\ \circ \\ | \end{array} = |$$

- «*копирование*» равномерного состояния дает линейно коррелированное состояние:

$$\begin{array}{c} \cup \\ \circ \\ \cup \\ \circ \\ | \end{array} = \begin{array}{c} \cup \\ \circ \\ | \end{array}$$

Некоторые из этих равенств даже кажутся знакомыми.

- Классические данные допускают разгибание:

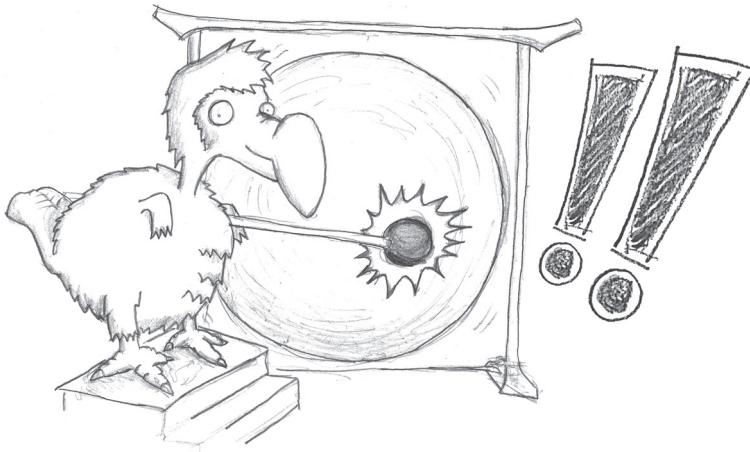
$$\begin{array}{c} \circ \\ \cup \\ \cup \\ \cup \\ \circ \\ | \end{array} = | \tag{8.36}$$

Упражнение 8.30. Докажите приведенные выше равенства для классических отображений.

Представьте себе медленно нарастающее крещендо где-то за сценой:



Естественно, хочется выписать все равенства, справедливые для классических отображений. Сколько их? Сотни? Или, быть может, бесконечное число? А теперь заключительный удар в гонг:



Существует всего одно такое равенство! А все равенства, которые мы до сих пор видели, на самом деле являются разными воплощениями одного и того же равенства. Чтобы убедиться в этом, необходимо осознать, что все приведенные выше классические отображения – частные случаи одного семейства отображений, которые мы назвали пауками.

Определение 8.31. Пауками называются линейные отображения вида:

$$\begin{array}{c} \overbrace{\quad\quad\quad}^n \\ \diagdown \quad \diagup \\ \circ \\ \diagup \quad \diagdown \\ \underbrace{\quad\quad\quad}_m \end{array} := \sum_i \begin{array}{c} \overbrace{\quad\quad\quad}^n \\ \downarrow \quad \downarrow \quad \dots \quad \downarrow \\ \triangle \quad \triangle \quad \dots \quad \triangle \\ \uparrow \quad \uparrow \quad \dots \quad \uparrow \\ \underbrace{\quad\quad\quad}_m \end{array} \quad (8.37)$$

На интуитивном уровне пауки вынуждают все входы и выходы быть одним и тем же базисным элементом. А раз так, то иногда полезно интерпретировать их как «большой символ Кронекера», ведь это именно то, что мы получаем при вычислении матрицы паука:

$$\delta_{i_1 \dots i_m}^{j_1 \dots j_n} = \begin{cases} 1 & \text{если } i_1 = \dots = i_m = j_1 = \dots = j_n \\ 0 & \text{в противном случае} \end{cases} .$$

Обычный символ Кронекера

$$\delta_i^j = \begin{cases} 1 & \text{если } i = j \\ 0 & \text{в противном случае} \end{cases}$$

является частным случаем – как матрица тождественного отображения.

Упражнение 8.32. Докажите обобщенное правило копирования для пауков:

$$\text{Spider with } n \text{ legs } j_1, \dots, j_n \text{ and } m \text{ legs } i_1, \dots, i_m = \delta_{i_1 \dots i_m}^{j_1 \dots j_n} \quad (8.38)$$

которое обобщает, например, равенства (8.21) и (8.27).

Прямо из определения мы можем вывести два свойства пауков. Во-первых, паук с двумя ногами – это просто провод:

$$\text{Spider with 2 legs} = \text{vertical line} \quad \text{Spider with 2 legs and loop} = \text{U-shaped wire} \quad \text{Spider with 2 legs and loop} = \text{curved wire} \quad (8.39)$$

а во-вторых, пауки демонстрируют изрядную симметрию.

Предложение 8.33. Все пауки инвариантны относительно «перекоммутации ног»:

$$\text{Spider with legs crossing} = \text{Spider with legs straight} \quad (8.40)$$

и сопряжения (т. е. горизонтального отражения):

$$\text{Spider with legs crossing} = \text{Horizontal reflection of spider} \quad (8.41)$$

Доказательство. Оба равенства следуют непосредственно из (8.37). □

И наконец, торжественный финал...



Все встречавшиеся до сих пор равенства для классических отображений можно заменить одним простым правилом:

если два паука соприкасаются, то они сливаются.

Точнее, справедлива следующая теорема.

Теорема 8.34. Композиция пауков производится следующим образом:

$$\begin{array}{c}
 \overbrace{\quad\quad\quad}^{n_1} \\
 \dots \\
 \text{---} \\
 \dots \\
 \underbrace{\quad\quad\quad}_{m_1}
 \end{array}
 \quad
 \begin{array}{c}
 \overbrace{\quad\quad\quad}^{n_2} \\
 \dots \\
 \text{---} \\
 \dots \\
 \underbrace{\quad\quad\quad}_{m_2}
 \end{array}
 \quad
 \begin{array}{c}
 \overbrace{\quad\quad\quad}^{n_1 + n_2} \\
 \dots \\
 \text{---} \\
 \dots \\
 \underbrace{\quad\quad\quad}_{m_1 + m_2}
 \end{array}
 \quad (8.42)$$

для $k \geq 1$.

Доказательство. Раскрыв обоих пауков, получаем:

$$\sum_i \left(\begin{array}{c} \overbrace{\downarrow i \dots \downarrow i}^{n_1} \\ \underbrace{\uparrow i \dots \uparrow i}_{m_1} \downarrow j \dots \downarrow j \underbrace{\uparrow j \dots \uparrow j}_{m_2} \end{array} \right) = \sum_{ij} \delta_i^j \left(\begin{array}{c} \overbrace{\downarrow i \dots \downarrow i}^{n_1} \quad \overbrace{\downarrow j \dots \downarrow j}^{n_2} \\ \underbrace{\uparrow i \dots \uparrow i}_{m_1} \quad \underbrace{\uparrow j \dots \uparrow j}_{m_2} \end{array} \right) = \sum_i \left(\begin{array}{c} \overbrace{\downarrow i \dots \downarrow i}^{n_1+n_2} \\ \underbrace{\uparrow i \dots \uparrow i}_{m_1+m_2} \end{array} \right)$$

□

Теперь мы можем доказать любое равенство, встречающееся в предыдущих разделах, просто сплющив левую и правую части в одного паука. Вот, например, равенство с участием копирования:

$$\left(\begin{array}{c} \text{Cup} \\ \text{Cup} \end{array} \right) \stackrel{(8.42)}{=} \left(\begin{array}{c} \text{Cup} \\ \text{Cup} \end{array} \right) \stackrel{(8.42)}{=} \left(\begin{array}{c} \text{Cup} \\ \text{Cup} \end{array} \right)$$

Вообще, в силу (8.39) чашки и крышки тоже являются пауками, поэтому мы можем сплющивать диаграммы пауков в одного большого паука.

Следствие 8.35. Любая связная струнная диаграмма, состоящая только из пауков, равна одному пауку:

$$\left(\begin{array}{c} \text{Complex diagram} \end{array} \right) = \left(\begin{array}{c} \text{Single spider} \end{array} \right) \tag{8.43}$$

Следовательно, такая диаграмма однозначно определяется числом входов и выходов, и мы можем установить равенство, просто пересчитав их.

Будем называть это правило *слиянием пауков*.

Следствие 8.36. Пауки обладают свойством «перебрасывания ног», т. е. если загнуть одну ногу паука вверх или вниз, то снова получится паук:

$$(8.44)$$

а значит, результатом транспонирования паука тоже будет паук.

Разумеется, этот факт в сочетании с самосопряженностью пауков означает, что применение адъюнкции к пауку тоже дает паука:

Упражнение 8.37. Пользуясь только свойствами пауков, докажите, что паук без ног равен «окружности» (т. е. размерности):

Упражнение 8.38. Как уже было сказано в замечании 8.23, некоторые пауки не каузальны. Чтобы операция корреляции стала каузальной, достаточно ввести нормировочный коэффициент:

Однако для операций сравнения и сопоставления никакое число не подойдет, поскольку для $i \neq j$ имеем:

Вообще, какие пауки являются каузальными, какие можно сделать каузальными посредством нормировки, а какие нельзя?

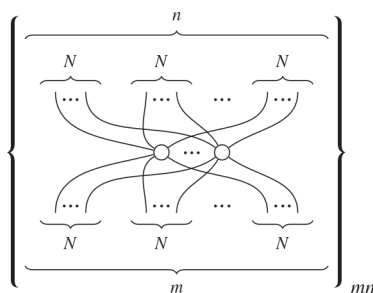
В разделе 5.2.2 мы видели, как кодировать битовые строки базисными состояниями. Можно также ассоциировать с ними пауков.

Упражнение 8.39. Пауки

для двумерного базиса

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array}, \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \right\}$$

ассоциируются с *битами*. Покажите, что следующее семейство классических отображений:



является также семейством пауков. Далее покажите, что оно ассоциировано с ОНБ, состоящим из N -битовых строк:

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \dots \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array}, \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \dots \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array}, \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \dots \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array}, \dots, \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \dots \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} \right\}$$

Замечание 8.40. Равенства

$$\begin{array}{c} \cup \\ \circ \end{array} = \cup \qquad \begin{array}{c} \circ \\ \cup \end{array} = \cup \qquad (8.45)$$

необходимые, например, для «перебрасывания ног», проистекают из того факта, что мы выбрали самосопряженный ОНБ (см. раздел 5.2.3). В некоторых (редких) случаях полезно определять пауков для несамосопряженных базисов, и тогда мы должны либо отказаться от этих равенств, либо каким-то образом исправить их (см. раздел* 8.6.3).

8.2.4. Если нечто ведет себя как паук, то это и есть паук

Коль скоро пауки так важны, нужно научиться распознавать их. Как можно отличить настоящего паука от, скажем, додо, который нарядился пауком в отчаянной попытке избежать вымирания?



В теореме 8.18 мы показали, что «копирующий паук» определяет ОНБ в терминах состояний, которые он «копирует»:

$$\left\{ \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \middle| \begin{array}{c} \circ \\ \downarrow \\ \triangle \\ i \end{array} \right\} = \left\{ \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \quad \begin{array}{c} \downarrow \\ \triangle \\ i \end{array} \right\} \quad (8.46)$$

Следовательно, семейство пауков из определения 8.31 всегда определяет ОНБ однозначно. Удивительно, но верно и обратное, и это нетривиальный результат: любой набор линейных отображений, для которого композиция ведет себя как для семейства пауков, на самом деле семейством пауков и является.

Теорема 8.41. Любой набор линейных отображений

$$\left\{ \begin{array}{c} \overbrace{\quad\quad\quad}^n \\ \dots \\ f_m^n \\ \dots \\ \underbrace{\quad\quad\quad}_m \end{array} \right\}_{mn}$$

удовлетворяющий условиям:

$$\begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_m^n \\ \dots \end{array} = \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_n^m \\ \dots \end{array} \quad \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_m^n \\ \dots \\ \circ \\ \dots \end{array} = \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_m^n \\ \dots \end{array} \quad \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_1^1 \\ \dots \end{array} = \left| \right.$$

для которого композиция обладает свойством:

$$\begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_{m'+k}^{n'} \\ \dots \end{array} \quad \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_m^{n+k} \\ \dots \end{array} = \begin{array}{c} \dots \\ \downarrow \\ \triangle \\ f_{m+m'}^{n+n'} \\ \dots \end{array}$$

является семейством пауков, т. е. существует ОНБ

$$\left\{ \begin{array}{c} | \\ \downarrow \\ \text{\scriptsize } i \\ \nabla \end{array} \right\}_i$$

такой, что

$$\begin{array}{c} \overbrace{\quad\quad\quad}^n \\ \text{\scriptsize } \dots \\ \text{\scriptsize } f_m^n \\ \text{\scriptsize } \dots \\ \underbrace{\quad\quad\quad}_m \end{array} = \sum_i \begin{array}{c} \overbrace{\quad\quad\quad}^n \\ \begin{array}{ccc} \nabla & \nabla & \dots & \nabla \\ \text{\scriptsize } i & \text{\scriptsize } i & & \text{\scriptsize } i \end{array} \\ \underbrace{\quad\quad\quad}_m \\ \begin{array}{ccc} \nabla & \nabla & \dots & \nabla \\ \text{\scriptsize } i & \text{\scriptsize } i & & \text{\scriptsize } i \end{array} \\ \downarrow \end{array}$$

Поскольку нас в основном интересуют пауки для самосопряженных ОНБ (см. замечание 8.1), мы специализируем этот результат для такого случая. В предложении 5.60 мы видели, что ОНБ является самосопряженным тогда и только тогда, когда

$$\cup = \sum_i \begin{array}{c} | \\ \downarrow \\ \text{\scriptsize } i \\ \nabla \end{array} \begin{array}{c} | \\ \downarrow \\ \text{\scriptsize } i \\ \nabla \end{array}$$

Теперь мы знаем, что правая часть – просто паук с двумя выходами, поэтому имеет место

Следствие 8.42. Набор линейных отображений из теоремы 8.41 представляет самосопряженный ОНБ тогда и только тогда, когда он дополнительно удовлетворяет условию

$$\begin{array}{c} | \quad | \\ \downarrow \quad \downarrow \\ \text{\scriptsize } f_0^2 \\ \nabla \end{array} = \cup$$

В доказательстве теоремы 8.41 используются методы *теории представлений*, поэтому оно выходит за рамки книги. Впрочем, в разделе* 8.6.1 мы напомним, как его можно провести. Однако кульминационный момент заключается в том, что равенства, которые, как мы выяснили, справедливы для пауков, на самом деле являются «аксиомами» пауков, т. е. всем им одновременно удовлетворяют пауки и только пауки. Поэтому мы называем их *уравнениями пауков*. Важное следствие – то, что теперь мы можем определять ОНБ, которые, на первый взгляд, ничего общего с диаграммами не имеют, используя чисто диаграммную концепцию пауков.

Следствие 8.43. ОНБ можно определить в терминах одних лишь диаграммных равенств, а именно уравнений пауков.

Более того, поскольку пауки имеют смысл в любой процессной теории, то же самое справедливо в отношении допускающих копирование состояний и эффектов. Как ни странно, ортонормированность получается почти автоматически.

Упражнение 8.44. В предположении, что числа в процессной теории удовлетворяют условию

$$\lambda^2 = \lambda \implies \lambda \in \{0, 1\}$$

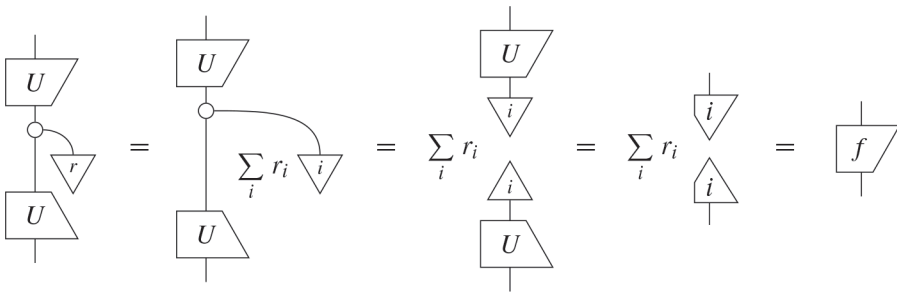
для некоторого ОНБ и вещественных чисел r_i . Пусть U – унитарное отображение, которое переводит ОНБ, ассоциированный с пауком, в ОНБ, показанный выше:

$$\begin{array}{|c} \hline U \\ \hline \end{array} \quad :: \quad \begin{array}{|c} \hline i \\ \hline \end{array} \mapsto \begin{array}{|c} \hline i \\ \hline \end{array}$$

и пусть

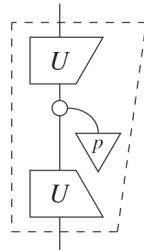
$$\begin{array}{|c} \hline r \\ \hline \end{array} := \sum_i r_i \begin{array}{|c} \hline i \\ \hline \end{array}$$

Тогда



Кроме того, по теореме 5.71, если f положительно, числа r_i положительны. Поэтому r оказывается классическим состоянием. \square

Разложение (8.48)



говорит нам, что «внутри» всякого положительного линейного отображения нет ничего, кроме пауков, унитарных отображений и классических состояний.

Небольшая вариация этого разложения позволяет выразить положительное линейное отображение в терминах классического состояния с полным носителем (см. соглашение 8.29). Чтобы убедиться в этом, нужно сделать систему в середине поменьше и заменить унитарные отображения изометриями:

(8.49)

Упражнение 8.47. Докажите, что любое положительное линейное отображение допускает разложение (8.49).

Далее, ослабив требование о совпадении изометрий вверху и внизу, мы можем получить разложение, имеющее место для всех линейных отображений.

Теорема 8.48. Любое линейное отображение f допускает *сингулярное разложение*:

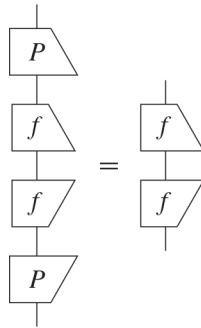
для некоторых изометрий U и V и классического состояния p с полным носителем.

Доказательство. Поскольку $f^\dagger \circ f$ положительно, мы можем воспользоваться спектральной теоремой для его представления в виде (8.49):

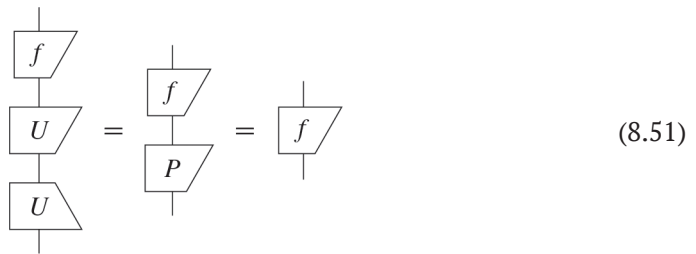
(8.50)

Теперь заметим, что поскольку U – изометрия, следующее отображение является проектором (т. е. положительно и идемпотентно, см. определение 4.69):

Тогда из формы равенства (8.50) немедленно следует, что



Поэтому из упражнения 5.77 (которое также вытекает непосредственно из спектральной теоремы) имеем:



Теперь для

$$\downarrow q := \sum_i q^i \downarrow i$$

где все $q^i \neq 0$, определим два дополнительных состояния:

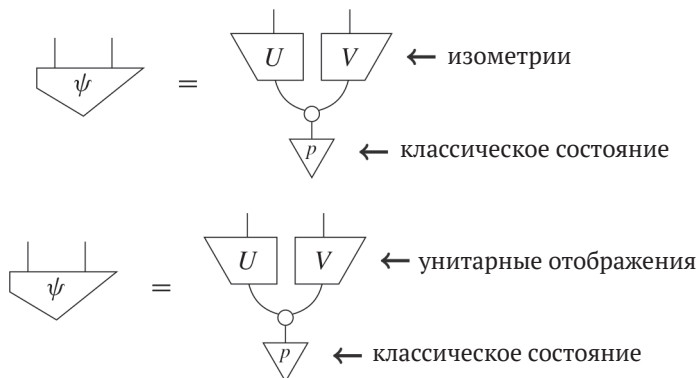
$$\downarrow q^{\frac{1}{2}} := \sum_i \sqrt{q^i} \downarrow i \qquad \downarrow q^{-\frac{1}{2}} := \sum_i \frac{1}{\sqrt{q^i}} \downarrow i$$

которые в силу (8.32) удовлетворяют условиям:



Перегнув провод, мы также выясним, что находится «внутри» любого двухкомпонентного состояния.

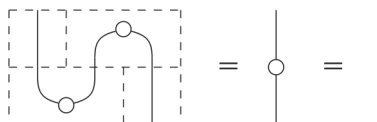
Следствие 8.49. Для любого двухкомпонентного состояния ψ имеет место разложение



Замечание 8.51. Вариант сингулярного разложения для двухкомпонентного состояния часто называют *разложением Шмидта*.

8.2.6. Паучьи диаграммы и полнота

В определении пауков мы уже выделили чашки и крышки как частные случаи пауков, которые назвали корреляцией и сравнением. Но, конечно, определяющим свойством чашек и крышек является связь между ними, т. е. тот факт, что их композиция дает тождественное отображение. По существу, это прямое проявление правила слияния пауков (8.34):



Довольно забавно рассматривать «разгибание проводов» как частный случай «слияния пауков», но именно это мы и установили:

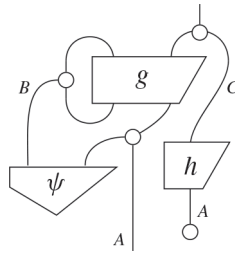
рассуждения в терминах струнных диаграмм – частный случай рассуждения в терминах пауков!

Если провод соединяет два конца, то паук соединяет много концов. Таким образом, говоря о слиянии пауков, мы говорим о соединении многих объектов с помощью нескольких пауков.

И как струнные диаграммы можно рассматривать либо как «схемные диаграммы + чашки и крышки», либо как новый вид диаграмм (см. теорему 4.19), так и диаграммы, содержащие пауков, можно трактовать двояко.

Определение 8.52. Паучья диаграмма состоит из блоков и проводов, которым разрешено соединять любое количество входов и выходов.

На диаграмме мы представляем эти «мультипровода» в виде пауков, например:



В ассоциированной диаграммной формуле (см. определения 3.8 и 4.21) их можно представить, просто повторив имена проводов сколько угодно раз:

$$\psi^{B_1 \tilde{A}_1} g_{B_1 \tilde{A}_1}^{B_1 \hat{C}_1} h_{A_2}^{\hat{C}_1} \quad (8.55)$$

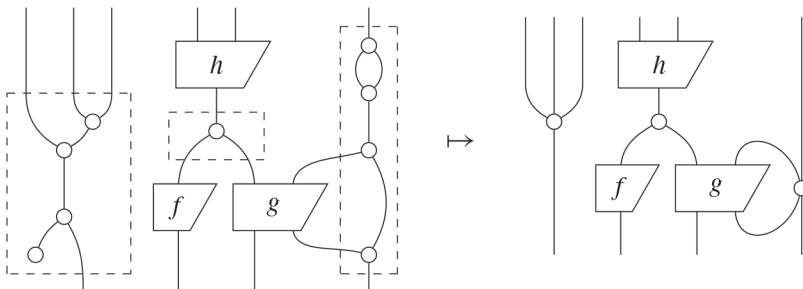
Для «мультипроводов» уже не понятно, какие имена проводов соответствуют входам, а какие – выходам, поэтому мы помечаем входы галочкой ($\tilde{-}$), а выходы – крышечкой ($\hat{-}$). Это позволяет различить, например, такие диаграммы:

$$\begin{array}{c} \circ \\ | \\ \text{f} \\ | \\ \circ \end{array} \longleftrightarrow f_{A_1}^{A_2} \quad \text{и} \quad \begin{array}{c} | \\ \text{f} \\ | \\ \circ \end{array} \longleftrightarrow \hat{f}_{A_1}^{A_2}$$

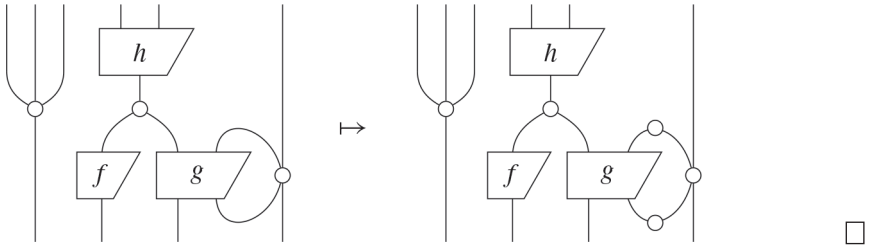
Теорема 8.53. Следующие два понятия эквивалентны:

- (i) паузы диаграммы и
- (ii) схемные диаграммы, к которым присоединены паузы для каждого типа, в том смысле что (ii) можно однозначно выразить через (i) и наоборот.

Доказательство. Мы можем преобразовать схемную диаграмму с паузами в паузную диаграмму, просто слив всех связанных пауков в один:



Обратно, если заменить чаше- и крышкообразные провода в паучьей диаграмме соответствующими пауками, то получится схемная диаграмма с пауками:



Напомним (см. раздел 5.4.1), что струнные диаграммы полны относительно **линейных отображений**. То есть равенство между струнными диаграммами имеет место для всех гильбертовых пространств и линейных отображений тогда и только тогда, когда струнные диаграммы одинаковы.

Всегда имеется возможность, что обогащение диаграммного языка приведет к нарушению полноты. Поскольку язык паучьих диаграмм богаче, мы можем записать на нем больше равенств (добавив равенства, содержащие пауков), но сможем ли мы по-прежнему доказать их? К счастью, да.

Теорема 8.54. Пауچьи диаграммы полны относительно **линейных отображений**, т. е. для любых двух паучьих диаграмм D и E следующие утверждения эквивалентны:

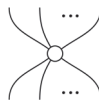
- $D = E$;
- для любых интерпретаций D, E в виде **линейных отображений** $\llbracket D \rrbracket = \llbracket E \rrbracket$.

Таким образом, мы можем сформулировать такое же утверждение, как для струнных диаграмм:

равенство между паучьими диаграммами имеет место для всех гильбертовых пространств и линейных отображений тогда и только тогда, когда пауچьи диаграммы одинаковы.

8.3. ОТ ПАУКОВ К КВАНТОВЫМ ОТОБРАЖЕНИЯМ

Прочитавшие два предыдущих раздела, возможно, заметили подозрительное сходство между нотацией пауков



и нотацией измерителя и кодировщика:



Конечно, никакой случайности тут нет. В этом разделе мы увидим, что это тоже некоторые виды пауков. А затем с помощью данного факта сделаем кое-какие

интересные штуки. В частности, это даст возможность пользоваться чисто диаграммными правилами, например слиянием пауков, для выполнения большей части трудной работы.

8.3.1. Измеритель и кодировщик как пауки

Идея КК-отображений заключается в том, чтобы классические и квантовые системы могли взаимодействовать. Используя нашу пропорцию

$$\frac{\text{классический}}{\text{квантовый}} = \frac{\text{тонкие/одиночные провода}}{\text{толстые/двойные провода}}$$

мы можем выразить блоки, входы и выходы которых включают как классические, так и квантовые провода. В разделе 8.1.3 мы видели, что квантовые состояния можно преобразовать в классические данные и наоборот, применяя измеритель и кодировщик. Можно ли придать этим процессам форму столь же элегантную, как форма паука для классических процессов? Да!

Мы уже видели отображения с двумя входящими проводами и одним исходящим и наоборот: пауки копирования и сопоставления. Однако вместо того чтобы рассматривать их как операции над классическими данными, мы можем трактовать пару проводов как один квантовый провод, перекинув тем самым мост от классического к квантовому:

$$\text{classical spider} := \text{quantum spider} \quad \text{quantum spider} := \text{classical spider} \tag{8.56}$$

Раскрывая определение пауков, мы видим, что это действительно дает нам измеритель:

$$\text{quantum spider} = \sum_i \text{classical spider with two spiders} = \sum_i \text{classical spider with one spider}$$

а применив адьюнкцию, получим кодировщик.

Отсюда можно понять, что эти процессы делают в терминах пауков. Например, на ОНБ-состояниях кодировщик раскрывается как копирование, т. е. мы получаем:

$$\text{classical spider} = \sum_i p^i \text{quantum spider} = \sum_i p^i \text{quantum spider}$$

Аналогично измеритель можно понять в терминах сопоставления, поэтому для того чтобы увидеть, что измеритель делает с произвольным квантовым состоянием ρ

$$\begin{array}{c} \downarrow \\ \rho \end{array} = \sum_{ij} \rho^{ij} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ j \end{array}$$

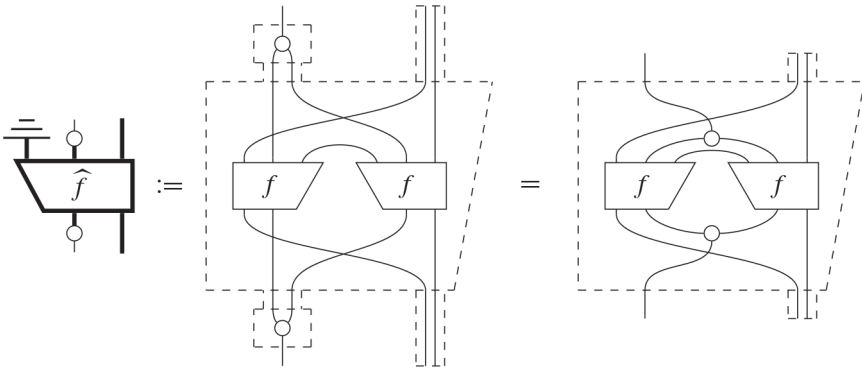
мы можем воспользоваться тем фактом, что измерение раскрывается как сопоставление:

$$\begin{array}{c} \circ \\ \downarrow \\ \rho \end{array} = \sum_{ij} \rho^{ij} \begin{array}{c} \circ \\ \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ j \end{array} = \sum_i \rho^{ii} \begin{array}{c} \downarrow \\ i \end{array}$$

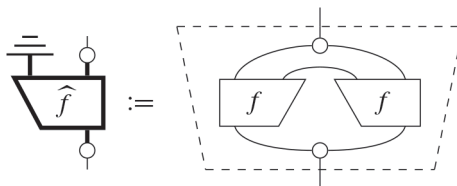
Это значит, что все внедиагональные элементы матрицы ρ в базисе произведения обнуляются, а диагональные (которые, по следствию 5.41, положительны) остаются без изменения. В разделе 8.1.3 мы уже видели, что эти диагональные элементы являются вероятностями для измерения ОНБ согласно правилу Борна:

$$\rho^{ii} := \begin{array}{c} \downarrow \\ i \\ \rho \end{array} = P(i | \rho)$$

В силу следствия 8.6 мы всегда можем выразить КК-отображение в терминах чистого квантового отображения посредством измерения, кодирования и отбрасывания. Теперь можно придать этому утверждению общую форму в терминах пауков:

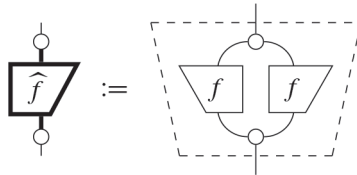


В частном случае классических отображений имеем:

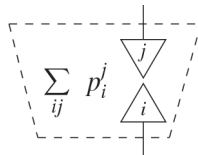


Но на самом деле упрощение на этом не заканчивается.

Упражнение 8.55. Покажите, что все классические отображения имеют вид:



Так как это упрощение опирается на свойства линейных отображений, для классических отображений придется использовать такую форму:



Очевидно, упражнение 8.55 не распространяется на более общие КК-отображения, т. к. это означало бы, в частности, что все квантовые отображения чистые. Но мы теперь знаем – это частный случай упражнения 8.55, – что классическое состояние p всегда можно записать в виде измерения ОНБ некоторого чистого квантового состояния:



Более того, зная, что кодировщик получается из копирующего паука, мы теперь можем показать, что любое квантовое состояние получается путем кодирования классического состояния – в силу диаграммной формы спектральной теоремы.

Предложение 8.56. Любое квантовое состояние ρ кодирует классическое состояние следующим образом:



Доказательство. Раскрывая приведенное выше равенство, получаем:

The equation shows two equivalent circuit diagrams. The left diagram consists of two trapezoidal blocks labeled f connected in parallel. The right diagram consists of two trapezoidal blocks labeled U connected in parallel, with a measurement symbol (circle with a vertical line through it) labeled p below them. The equation is labeled (8.57) on the right.

для некоторого f . Это просто согнутая версия разложения (8.48), которая возможна благодаря спектральной теореме. \square

Замечание 8.57. Унитарное отображение U необходимо, потому что мы решили использовать в этой книге только самосопряженные ОНБ. В противном случае, как мы покажем в разделе* 8.6.3, разложение можно упростить:

$$\begin{array}{c} \downarrow \\ \rho \end{array} = \begin{array}{c} \circ \\ | \\ \downarrow \\ p \end{array} \left. \begin{array}{l} \text{кодировщик} \\ \text{классическое} \\ \text{состояние} \end{array} \right\}$$

Мы можем также воспользоваться тем фактом, что измеритель и кодировщик – «загримировавшиеся» пауки, и выписать еще несколько равенств.

Предложение 8.58. Имеют место следующие утверждения.

1. Кодировщик с последующим измерителем эквивалентен «ничегонеделанью»:

$$\begin{array}{c} \circ \\ | \\ \circ \end{array} = | \tag{8.58}$$

2. Результат транспонирования кодировщика – измеритель:

$$\begin{array}{c} \text{U} \\ \circ \end{array} = \begin{array}{c} \circ \\ | \end{array} \tag{8.59}$$

3. Измеритель с последующим удалением – это отбрасывание:

$$\begin{array}{c} \circ \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \circ \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \tag{8.60}$$

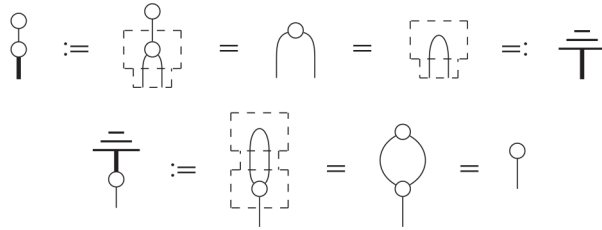
4. Кодировщик с последующим отбрасыванием – это удаление:

$$\begin{array}{c} \text{---} \\ | \\ \circ \end{array} = \begin{array}{c} \circ \\ | \end{array} \quad \begin{array}{c} \circ \\ | \\ \text{---} \end{array} = \begin{array}{c} \circ \\ | \end{array} \tag{8.61}$$

Доказательство. Все эти равенства получаются раскрытием дублированных частей и применением правила слияния пауков:

$$\begin{array}{c} \circ \\ | \\ \circ \end{array} := \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = |$$

$$\begin{array}{c} \text{U} \\ \circ \end{array} := \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \circ \\ | \end{array}$$



Тот факт, что отбрасывание разлагается, как в первом равенстве (8.60), позволяет сформулировать новый вариант предложения 6.79, в котором утверждалось, что квантовое отображение разделяется, когда редуцированное отображение чистое. Помимо отбрасывания квантовых выходов, это применимо также к удалению классических выходов.

Предложение 8.59. Если редуцированное отображение КК-отображения чистое:

$$\begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \text{---} \\ \Phi \end{array} = \begin{array}{c} | \\ \text{---} \\ \hat{f} \end{array} \tag{8.62}$$

то процесс Φ разделяется следующим образом:

$$\begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \text{---} \\ \Phi \end{array} = \begin{array}{c} | \\ \text{---} \\ p \end{array} \begin{array}{c} | \\ \text{---} \\ \hat{f} \end{array}$$

для некоторого (каузального) классического состояния p (т. е. распределения вероятностей).

Доказательство. В силу равенства (8.60) равенство (8.62) эквивалентно следующему:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \\ | \\ \text{---} \\ \Phi \end{array} = \begin{array}{c} | \\ \text{---} \\ \hat{f} \end{array}$$

поэтому по предложению 6.79 имеем:

$$\begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \text{---} \\ \Phi \end{array} \stackrel{(6.52)}{=} \begin{array}{c} \circ \\ | \\ \text{---} \\ \rho \end{array} \begin{array}{c} | \\ \text{---} \\ \hat{f} \end{array} = \begin{array}{c} | \\ \text{---} \\ p \end{array} \begin{array}{c} | \\ \text{---} \\ \hat{f} \end{array}$$

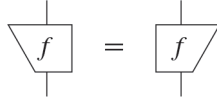
где мы положили

$$\begin{array}{c} | \\ \text{---} \\ p \end{array} := \begin{array}{c} \circ \\ | \\ \text{---} \\ \rho \end{array}$$

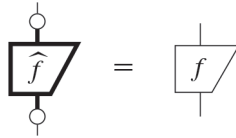
а это состояние каузальное в силу каузальности измерителя и ρ . □

Кроме того, несколько фактов, которые раньше были выведены с помощью сумм, теперь можно вывести, применяя только диаграммы, например следующий.

Упражнение 8.60. Докажите с помощью диаграмм, что классические отображения являются самосопряженными:



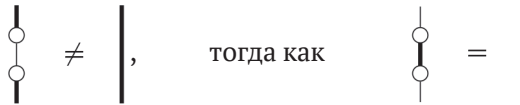
Воспользуйтесь этим результатом для доказательства того, что для функциональных отображений имеет место равенство



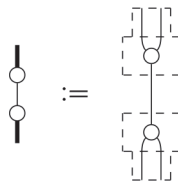
8.3.2. Декогеренция

Этот раздел посвящен очень важному (и имеющему дурную славу!) квантовому процессу. Дурная слава связана с тем, что у него есть неприятная привычка перемешивать прекрасные чистые состояния, которые физики пытаются подготовить в своих лабораториях, в результате чего сильно осложняется построение таких объектов, как квантовые компьютеры.

Равенство (8.58) показывает, что если перейти от классических данных к классическим данным с помощью квантовой системы, то классическая система остается неизменной. Но измерение – лишь одностороннее обращение кодирования. То есть если составить композицию отображений в противоположном порядке, то квантовая система наверняка претерпит изменения в силу возмущающей природы измерения. Таким образом:



Определение 8.61. Декогеренцией относительно ОНБ называется квантовый процесс:



На самом деле мы уже встречались с этим процессом при доказательстве предложения 8.5, когда устанавливали нормальную форму КК-отображений. Там мы существенно опирались на то, что этот процесс – квантовое отображение. Теперь,

когда мы знаем, что измеритель и кодировщик – пауки, это следует прямо из правила слияния пауков:

(8.63)

Нам еще необходимо показать, что декогеренция не равна тождественному процессу, но мы можем высказать гораздо более сильное утверждение. Она не только не равна тождественному процессу, но даже не является чистым отображением.

Предложение 8.62. Декогеренция не является чистым квантовым отображением.

Доказательство. Предположим, что декогеренция является чистым квантовым отображением. Тогда для некоторого линейного отображения f мы имели бы:

Но раз так, то в силу правила слияния пауков:

т. е. тождественный процесс несвязен. Поэтому декогеренция не может быть чистой. □

Если взглянуть на диаграммную форму декогеренции, то становится понятным, почему она не совпадает с тождественным процессом. Хотя вход и выход дублированы, квантовая система посередине кажется «сдавленной» в одиночный (классический) провод. Поэтому все, что «жило» в двух проводах, втискивается в один провод (что в общем случае не обходится без потери данных), а затем снова «расправляется» на два провода. В физических терминах это означает, что квантовое состояние вынужденно становится классическим, а затем снова квантовым.

С другой стороны, коль скоро декогеренция применена к квантовой системе, то вред уже причинен. Повторное применение оставляет систему неизменной.

Лемма 8.63. Декогеренция является проектором.

Доказательство. Очевидно, что декогеренция – самоадьюнктное, а также идемпотентное отображение:

$$\begin{array}{c} \circ \\ | \\ \circ \\ | \\ \circ \\ | \\ \circ \\ | \\ \circ \end{array} \stackrel{(8.58)}{=} \begin{array}{c} \circ \\ | \\ \text{---} \\ | \\ \circ \end{array} = \begin{array}{c} \circ \\ | \\ \circ \end{array}$$

□

В частности, мы теперь можем выделить подмножество *декогерентных* состояний ρ , т. е. таких, на которые дальнейшая декогеренция не оказывает влияния:

$$\begin{array}{c} \circ \\ | \\ \circ \\ \downarrow \\ \rho \end{array} = \begin{array}{c} \downarrow \\ \rho \end{array}$$

Что это за состояния? Поскольку декогеренция – результат композиции измерителя и кодировщика, то из предыдущего раздела мы знаем, что она делает с матрицей квантового состояния:

$$\begin{array}{c} \circ \\ | \\ \circ \\ \downarrow \\ \rho \end{array} = \sum_{ij} \rho^{ij} \begin{array}{c} \circ \\ | \\ \circ \\ | \\ \circ \\ | \\ \circ \end{array} = \sum_i \rho^{ii} \begin{array}{c} \downarrow \\ i \end{array} \begin{array}{c} \downarrow \\ i \end{array} = \sum_i \rho^{ii} \begin{array}{c} \downarrow \\ i \end{array}$$

Следовательно, она сохраняет в точности те состояния, для которых все внедиагональные элементы равны нулю. Этот факт можно сформулировать в эквивалентном виде.

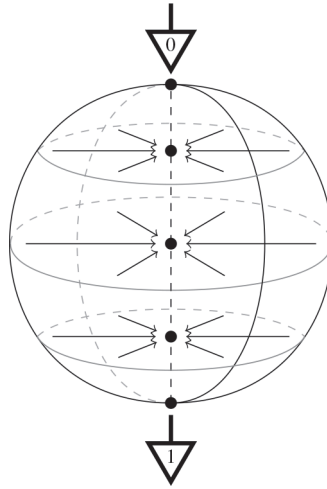
Теорема 8.64. Декогеренция сохраняет квантовое состояние ρ тогда и только тогда, когда она кодирует распределение вероятностей, т. е. имеет вид:

$$\begin{array}{c} \downarrow \\ \rho \end{array} = \sum_i p^i \begin{array}{c} \downarrow \\ i \end{array} \tag{8.64}$$

Упражнение 8.65. Если определить декогеренцию как вполне положительное отображение (см. замечание 6.50), то что она делает с матрицами плотности?

Для кубитов шар Блоха (см. раздел 6.2.7) дает изящную геометрическую картину того, что декогеренция делает с состояниями и какие состояния остаются

неизменными в результате (повторной) декогеренции. Декогеренция проецирует каждое состояние на ось, проходящую через два ОНБ-состояния:



(8.65)

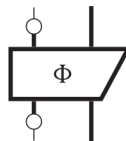
Вспомним соответствие

$$\sum_i p^i \downarrow_i \leftrightarrow \sum_i p^i \downarrow_i$$

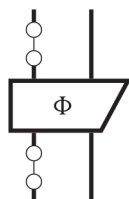
которое можно переписать без сумм в виде:



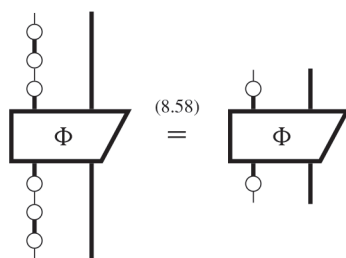
Это соответствие говорит, что квантовый выход, к которому применена декогеренция, ведет себя в точности как классический выход. На самом деле это соответствие обобщается на произвольные квантовые процессы. Присоединяя отображения измерения и кодирования к его классическим входам и выходам, мы можем преобразовать любое КК-отображение



в квантовое отображение



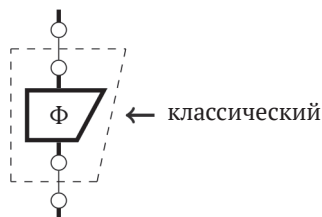
где присутствие классического входа и выхода КК-отображения, с которого мы начали, теперь засвидетельствовано присутствием декогеренции. Мы также легко восстановим это КК-отображение, подключив отображения кодирования и измерения:



Мораль сей басни такова:

декогеренция вынуждает квантовые системы вести себя как классические.

Для квантового отображения это легко видеть непосредственно, нарисовав картинку. Когда мы компонуем декогеренцию с входами и выходами любого квантового процесса, он по существу становится классическим:



Поскольку декогеренция вынуждает квантовую систему вести себя как классическая, не должно вызывать удивления, что декогеренция – не друг тому, кто хочет задействовать квантовые особенности, например для построения квантового компьютера. На практике квантовые системы часто испытывают *частичную декогеренцию*:

$$(1 - p) \left| \right. + p \begin{array}{c} \circ \\ | \\ \circ \end{array}$$

причем чем дольше мы пытаемся хранить систему, тем больше становится значение p . Время, за которое p достигает значения 1, называется *временем декогеренции*, и в типичном случае оно очень мало. Одна из самых сложных проблем при построении квантового компьютера – продлить это время как можно дольше, сохранив возможность взаимодействовать с квантовой системой различными интересными способами.

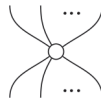
Упражнение* 8.66. Охарактеризуйте частичную декогеренцию без использования сумм.

8.3.3. Классические, квантовые и гибридные пауки

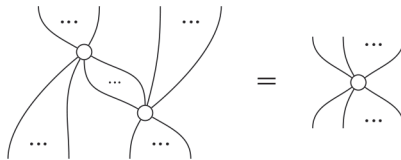
В этом разделе мы увидим, как измеритель и кодировщик возникают в виде представителей нового вида пауков. На самом деле все вычисления в оставшейся части книги – это примеры встречи и взаимодействия различных пауков. Сейчас мы построим таксономию, выделив пауков трех типов: классических, квантовых и (самых интересных) гибридных.

Что такое классические пауки, мы уже знаем.

Определение 8.67. *Классическим* называется паук, имеющий только тонкие ноги:

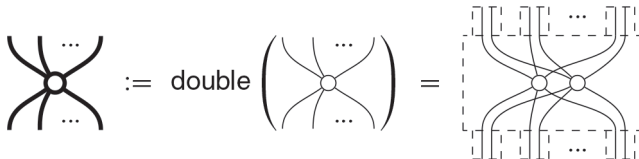


И мы знаем, как они компонуются:



Ну а поскольку классические пауки – это линейные отображения, мы можем преобразовать их в чисто квантовые отображения путем дублирования.

Определение 8.68. *Квантовым пауком* называется квантовое отображение вида:



А поскольку равенства между линейными отображениями переносятся в дублированный мир (см. следствие 6.16), мы также знаем, как они компонуются.

Следствие 8.69. Квантовые пауки компонуются следующим образом:

$$\text{Diagram} = \text{Diagram} \quad (8.66)$$

Пример 8.70 (состояние Гринбергера–Хорна–Цайлингера). Важными примерами квантовых пауков являются состояния квантовых пауков. Мы уже встречались с одним таким: состоянием двухсистемного квантового паука, представляющим собой не что иное, как *состояние Белла*:

$$\text{Diagram} = \text{Diagram}$$

Состояние трехсистемного квантового паука:

$$\text{Diagram}$$

называется *состоянием Гринбергера–Хорна–Цайлингера (ГХЦ)* и имеет много важных приложений. Например, в разделе 11.1 мы приведем основанное на нем доказательство квантовой нелокальности. Будучи записано в терминах ОНБ, ГХЦ-состояние кубита имеет вид:

$$\text{Diagram} = \text{double} \left(\begin{matrix} \downarrow \\ 0 \end{matrix} \begin{matrix} \downarrow \\ 0 \end{matrix} \begin{matrix} \downarrow \\ 0 \end{matrix} + \begin{matrix} \downarrow \\ 1 \end{matrix} \begin{matrix} \downarrow \\ 1 \end{matrix} \begin{matrix} \downarrow \\ 1 \end{matrix} \right)$$

Поскольку оно следующим образом связано с (дублированным) копирующим пауком:

$$\text{Diagram} = \text{Diagram}$$

то, по теореме 8.18, оно характеризует (дублированный) ОНБ.

Пользуясь лишь копированием, мы можем вывести отсюда, что если любая из трех систем находится в одном из базисных состояний этого ОНБ, то это справедливо и для двух остальных:

$$\text{Diagram} = \begin{matrix} \downarrow \\ i \end{matrix} \begin{matrix} \downarrow \\ i \end{matrix} \quad (8.67)$$

Состояния прочих n -системных квантовых пауков

$$\text{Diagram}$$

обычно называются *обобщенными ГХЦ-состояниями*.

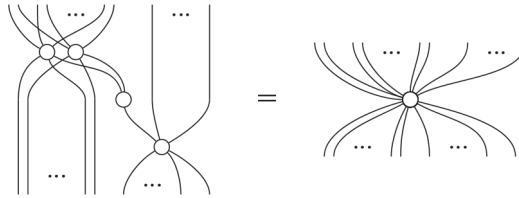
Третий тип пауков содержит как классические, так и квантовые провода. Мы уже встречали два исключительно важных примера такого рода:



Вообще, мы можем использовать измеритель и кодировщик для соединения любого классического паука с любым квантовым:

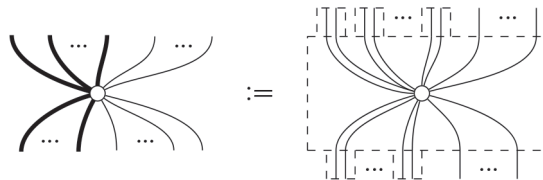


и тем самым получить целое семейство классически-квантовых гибридов. Раскрывая определение дублированного паука, мы видим, что все кружочки можно слить в один:



Таким образом, самыми полезными пауками, которых можно получить с помощью диаграммы (8.68), являются пауки всего с одним (нежирным) кружочком.

Определение 8.71. *Гибридным пауком* называется КК-отображение вида



То есть это пауки, получаемые, если интерпретировать некоторые пары ног классического паука как дублированные системы (т. е. *свернуть*), а остальные оставить одиночными.

Гибридный паук состоит только из одного (нежирного) кружочка, поэтому если у него нет квантовых ног, то он является просто классическим пауком, однако гибридный паук без классических ног квантовым не является.



Например, декогеренция – это гибридный паук с одним квантовым входом и одним квантовым выходом:

$$\begin{array}{c} \circ \\ | \\ \circ \\ | \end{array} = \begin{array}{c} \boxed{\circ} \\ | \\ \boxed{\circ} \\ | \end{array} = \begin{array}{c} \boxed{\circ} \\ | \\ \boxed{\circ} \\ | \end{array} = \begin{array}{c} \circ \\ | \\ \circ \\ | \end{array} \quad (8.69)$$

тогда как соответствующий квантовый паук – тождественный процесс:

$$\begin{array}{c} \circ \\ | \end{array} = \begin{array}{c} \boxed{\circ} \\ | \\ \boxed{\circ} \\ | \end{array} = \begin{array}{c} | \\ | \\ | \\ | \end{array} = \begin{array}{c} | \end{array}$$

Отбрасывание тоже является гибридным пауком:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \boxed{\text{---}} \\ | \\ \boxed{\text{---}} \end{array} = \begin{array}{c} \boxed{\circ} \\ | \\ \boxed{\circ} \\ | \end{array} = \begin{array}{c} \circ \\ | \end{array} \quad (8.70)$$

тогда как квантовый паук с одним квантовым входом – это чистый (некаузальный) квантовый эффект:

$$\begin{array}{c} \circ \\ | \end{array} = \begin{array}{c} \boxed{\circ} \\ | \\ \boxed{\circ} \\ | \end{array}$$

Разумеется, гибридные пауки могут сливаться:

$$\begin{array}{c} \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \end{array} = \begin{array}{c} \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \\ \dots \end{array}$$

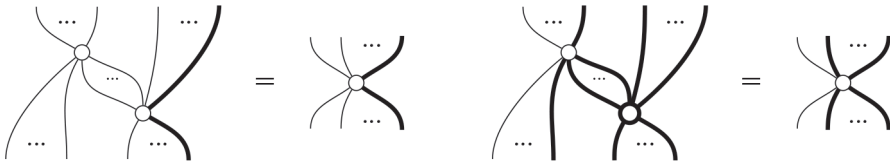
Однако результат не всегда является гибридным пауком, например:

$$\begin{array}{c} \circ \\ | \\ \circ \\ | \end{array} = \begin{array}{c} | \end{array}$$

Чтобы разобраться в механизме слияния гибридных пауков, включая слияние с классическими и квантовыми, следует рассуждать в терминах двух, а не трех видов пауков, а именно:

- пауки «с одним кружочком» := классические пауки + гибридные пауки;
- пауки «с двумя кружочками» := квантовые пауки.

Теорема 8.72. Любая композиция пауков с участием, по крайней мере, одного паука с одним кружочком дает паука с одним кружочком, например:



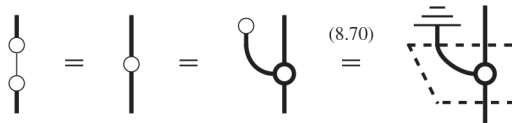
Это можно сформулировать несколько иначе.

Следствие 8.73. Любая связная диаграмма классического, квантового или гибридного паука должна быть равна одной из следующих:

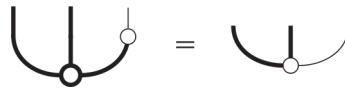
1. Квантовый паук, если содержит только дублированные кружочки.
2. Классический паук, если содержит только классические входы и выходы.
3. Гибридный паук в противном случае.

Хрестоматийным примером паука с одним кружочком, не являющегося классическим, является декогеренция, которая вынуждает квантовые системы вести себя как классические. Теорема 8.72 обобщает этот факт на мир пауков, в котором наличие одного кружочка можно интерпретировать как «зараженность классичностью».

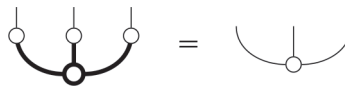
Пример 8.74. В равенстве (8.63) мы показали, что декогеренция – квантовое отображение. Теперь видно, что это доказательство – пример слияния гибридных пауков:



Пример 8.75. При измерении одной из трех систем в ГХЦ-состоянии мы получаем гибридного паука:



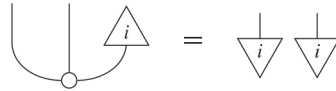
Если измерить все три системы, то получится классический паук:



Этот классический паук описывает классические выходы измерения. Разложив его по ОНБ в случае кубита

$$\begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline 1 \\ \hline \end{array}$$

мы видим, что во всех трех измерениях получается один и тот же исход, хотя этот исход может быть равен как 0, так и 1. Это снова следует из обобщенного правила копирования:



которое обобщается на квантовых и гибридных пауков:

$$= \delta_{i_1 \dots i_m}^{j_1 \dots j_n} \quad (8.71)$$

$$= \delta_{i_1 \dots i_m}^{j_1 \dots j_n} \quad (8.72)$$

Как и в случае классических пауков, квантовых и гибридных пауков можно объединить, получив таким образом квантово-гибридные пауки-произведения в составных системах:

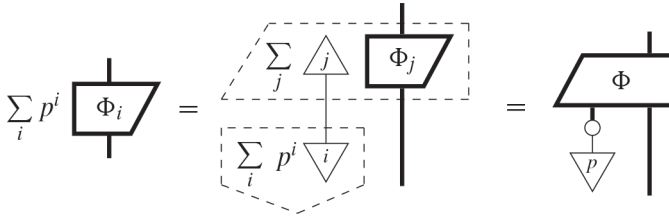


В случае гибридных пауков мы разрешаем соединять классические ноги только с классическими, а квантовые только с квантовыми. В частности, отображения измерения и кодирования для составных систем очевидны:

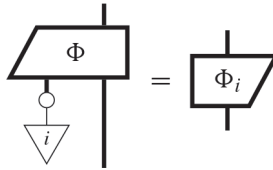


8.3.4. Смешивание с пауками

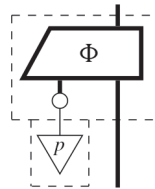
Пауки позволяют чисто диаграммно определить смешивание, тогда как раньше для этого приходилось использовать суммы. Сначала вспомним, что означает «смешивание» для квантовых процессов. Смесь (см. определение 6.70) дает возможность представить ситуацию, когда имеется один из возможных квантовых процессов, но мы не знаем, какой именно. Иными словами, с получением этого процесса связана классическая случайность, которую можно выразить как некоторое распределение вероятности, включаемое в управляемый квантовый процесс. На самом деле легко показать, что любая смесь получается следующим образом:



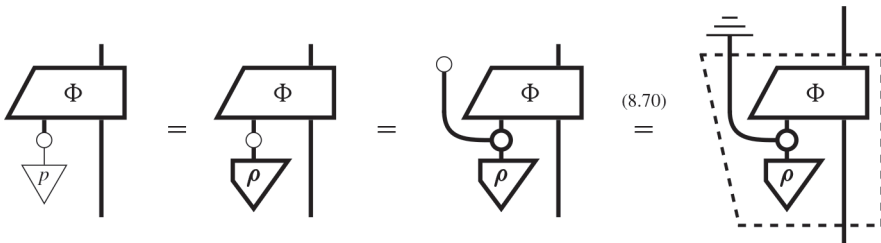
Квантовый процесс с классическим входом представляет смешиваемые объекты, а распределение вероятностей p – само смешивание. Мы можем получить компоненты смеси посредством ОНБ-состояний:



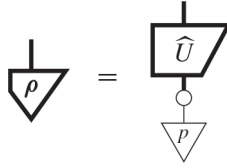
Теперь вернемся к результатам о смешивании из главы 6. Прежде всего тот факт, что любая смесь каузальных квантовых отображений является каузальным квантовым отображением (см. теорему 6.71), следует из того, что композиция каузальных КК-отображений



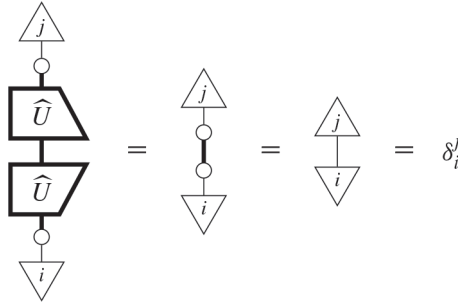
снова является каузальным КК-отображением. В этом случае нет классических входов и выходов, поэтому мы действительно имеем каузальное квантовое отображение. Ну а то, что любую смесь можно интерпретировать в терминах отбрасывания части системы, теперь следует из правила слияния гибридных пауков:



То, что любое каузальное квантовое состояние можно рассматривать как смесь чистых каузальных квантовых состояний (теорема 6.72), – просто утверждение о том, что квантовое состояние кодирует классическое (предложение 8.56):

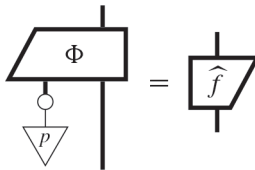


а тот факт, что эти состояния всегда можно выбрать ортонормированными, уже встроено:



Теперь воспользуемся этой диаграммной формой смешивания для доказательства ранее недоказанного утверждения, а именно что если результат смешивания квантовых процессов чистый, то все смешиваемые процессы должны быть чистыми и на самом деле равны результату смешивания. Для этого предположим, что у распределения вероятностей p , использованного для смешивания, имеется полный носитель (см. соглашение 8.29), что имеет смысл, поскольку компонент с вероятностью 0 все равно ничего не привносит в смесь.

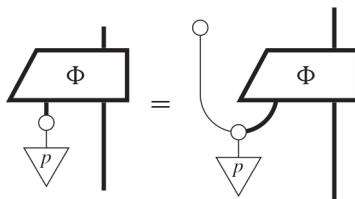
Предложение 8.76. Если смесь чистая



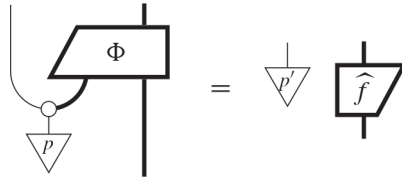
то



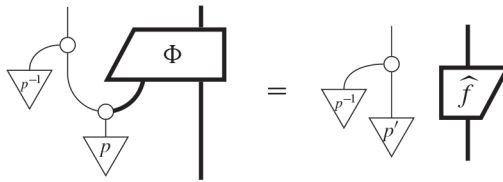
Доказательство. Сначала представим любую смесь как редуцированное КК-отображение:



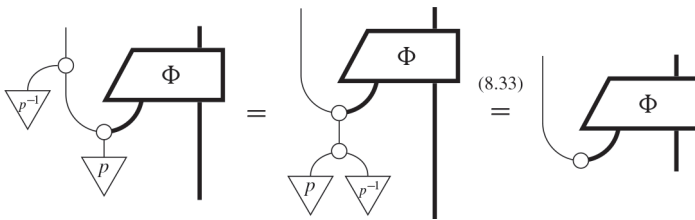
В силу предложения 8.59 КК-отображение должно разделяться следующим образом:



Мы предположили, что p имеет полный носитель, поэтому применим p^{-1} к обеим частям:



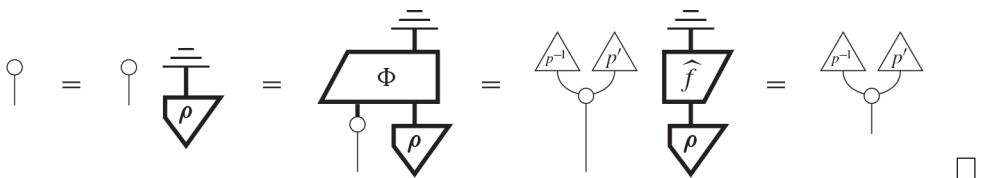
После слияния пауков левая часть принимает вид:



поэтому перегибание классического провода вниз дает

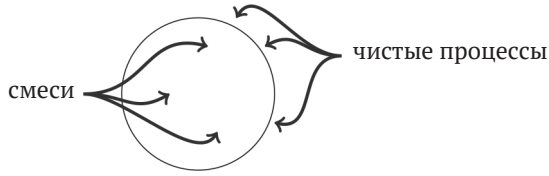
$$\text{Diagram} = \text{Diagram} \quad (8.74)$$

Наконец, тот факт, что классический эффект в (8.74) обязан быть удалением, следует из каузальности Φ (которая также влечет за собой каузальность \hat{f}). В этом легко убедиться, подключив произвольное каузальное состояние ρ к квантовому входу и отбросив выход:



Хотя это доказательство целиком диаграммное, оно устанавливает геометрическое свойство пространства квантовых состояний, а именно что каждое чистое

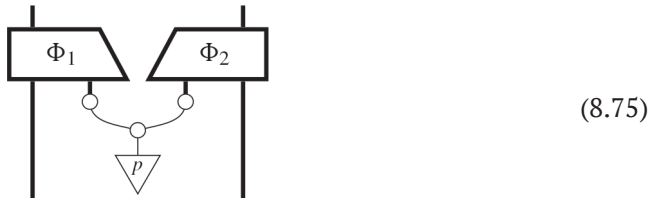
состояние «крайнее», т. е. никакое чистое состояние нельзя разложить в нетривиальную смесь (т. е. выпуклую комбинацию). Например, в шаре Блоха имеем:



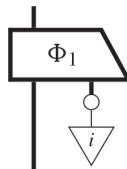
8.3.5. Запутывание для нечистых состояний

Смешивание с пауками, в свою очередь, дает полную характеристику квантового запутывания, которая применима не только к чистым, но и к любым квантовым состояниям. Далее мы приведем диаграммное доказательство того, что эта характеристика сводится к \otimes -разделимости для чистых состояний.

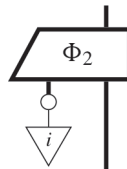
Нетривиальная часть запутывания для нечистых состояний заключается в том, что посредством смешивания мы можем получить \otimes -неразделимые процессы даже в случаях, когда ничего подобного квантовому запутыванию нет и в помине. Предположим, например, что имеется такая смесь:



У нас есть смесь двух процессов, но управляются они не двумя независимыми классическими состояниями, а одним и тем же классическим состоянием, на что указывает наличие отображения копирования. И хотя мы не знаем, какой процесс имеет место в действительности, нам, по крайней мере, известно, что всякий раз как слева имеет место



справа должно иметь место



То есть две части смеси *классически коррелированы*. Диаграмма как целое связанная, но часть, связывающая обе компоненты, целиком классическая. Такое со-

единение по своей природе сильно отличается, например, от квантовых чашек, которыми мы пользовались для вывода разнообразных квантовых особенностей.

Таким образом, чтобы правильно определить запутывание, мы должны не только указать, что квантовое состояние не разделяется, но и что оно не просто связано классическими корреляциями.

Определение 8.77. Двухкомпонентное квантовое состояние ρ называется *запутанным*, если его нельзя представить в следующей форме для некоторых квантовых отображений Φ_1 и Φ_2 :

(8.76)

Если состояние не является запутанным, то будем называть его *распутанным*.

Хотя мы определяем распутанные состояния с помощью классической чашки («прямолинейные корреляции»), можно было бы с равным успехом воспользоваться произвольными классическими корреляциями, как мы сделали в (8.75) выше.

Предложение 8.78. Двухкомпонентное квантовое состояние ρ является запутанным, если его нельзя записать в следующей форме для некоторых квантовых состояний Φ_1 и Φ_2 и распределения вероятностей p :

(8.77)

Доказательство. Если состояние распутанное в смысле определения 8.77, то

т. е. оно имеет форму (8.77). Обратно, имеем:

т. е. состояние действительно имеет форму (8.76). □

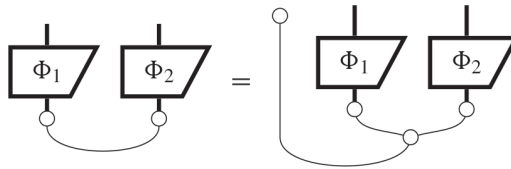
Пример 8.79. Благодаря двойственности процессов и состояний декогеренция является источником классически коррелированного состояния вида (8.76):



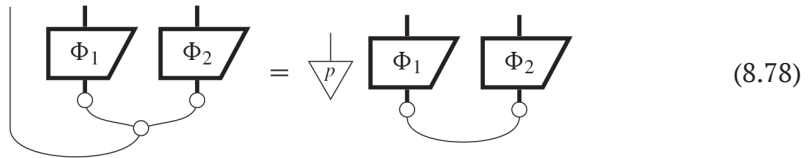
В главе 6, определяя запутывание для чистых состояний как \otimes -неразделимость, мы ничего не знали о классических проводах. Однако оно все равно возникает как частный случай.

Предложение 8.80. Если чистое квантовое состояние является распутанным в смысле определения 8.77, то оно \otimes -разделимо.

Доказательство. Сначала, как в доказательстве предложения 8.76, представим процесс, предполагаемый чистым, в виде редуцированного процесса с помощью слияния пауков. В этом случае мы можем представить любое чистое распутанное состояние как следующее редуцированное состояние:



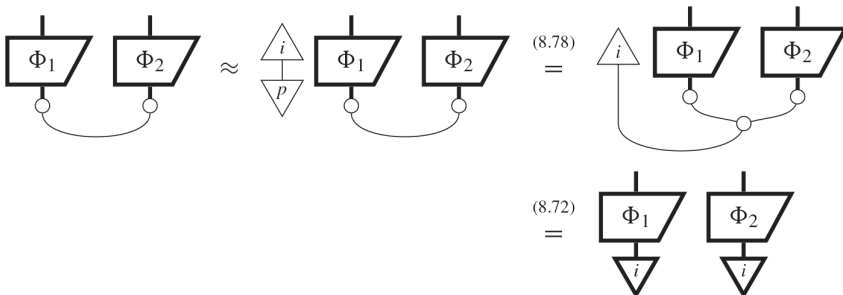
Поскольку двухкомпонентное состояние, полученное путем удаления классической системы, чистое, то, по предложению 8.59, состояние в целом должно разделяться следующим образом:



для некоторого классического состояния p . Поэтому существует, по крайней мере, одно базисное состояние i такое, что:

$$\begin{array}{c} \triangle i \\ \hline \triangle p \end{array} \neq 0$$

Отсюда имеем:

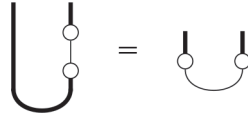


□

В качестве следствия получаем такой факт.

Следствие 8.81. Квантовая чашка – запутанное состояние.

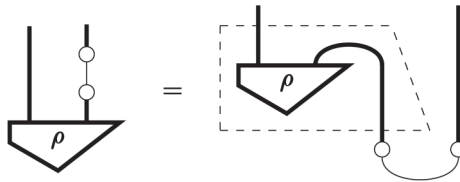
Располагая диаграммными формами для многих квантовых особенностей, мы легко можем исследовать связи между ними. Например, что случится, если применить декогеренцию к одной из систем в состоянии Белла? Оно распутывается:



Это проявление более общего факта.

Теорема 8.82. Декогеренция разрушает запутывание, т. е. если применить декогеренцию к одной из двух систем в запутанном состоянии, то оно распутается.

Доказательство. Имеем:

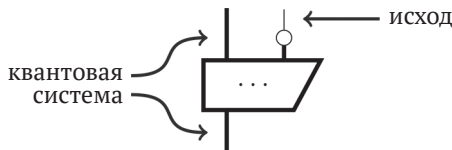


□

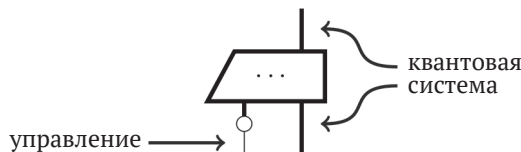
8.4. ИЗМЕРЕНИЯ И ПРОТОКОЛЫ С УЧАСТИЕМ ПАУКОВ

Теперь мы воспользуемся пауками для получения диаграммного представления всех встречавшихся ранее семейств квантовых измерений и квантовых протоколов без использования ветвей и сумм.

Невозможные измерения являются КК-отображениями такого вида:



тогда как управляемые унитарные отображения имеют двойственную форму:

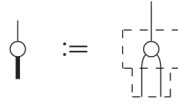


Соединив проводами подобные отображения, мы получим графические представления телепортации, плотного кодирования и перекоммутации запутывания.

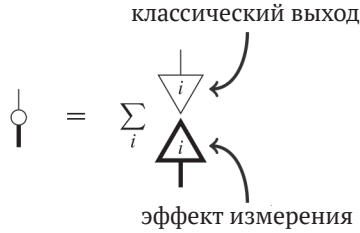
И в конце этого раздела мы вернемся к теореме Наймарка о дилатации. После перевода на язык КК-отображений и пауков она окажется просто тавтологией.

8.4.1. Измерения ОНБ

В измерении



мы использовали тот же базис для эффектов измерения, что и для классических выходов:



Конечно, нет никаких причин считать, что эти базисы одинаковы, поэтому произвольные (возмущающие) измерения ОНБ являются квантовыми процессами вида



Но из предложения 7.4 мы знаем, что можно получить измерения в любом ОНБ, применив унитарное отображение к некоторому фиксированному ОНБ, так что справедливо

Следствие 8.83. Любое возмущающее измерение ОНБ имеет вид:

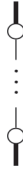


где \hat{U} – унитарный квантовый процесс.

Простой процесс измерения



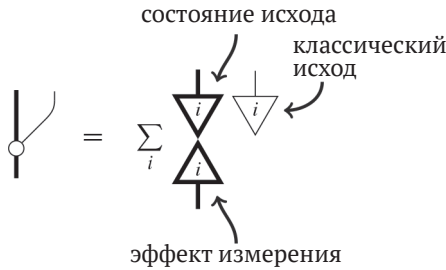
конечно, является частным случаем, когда \hat{U} – тождественный процесс. У процесса измерения имеется также невозмущающий аналог, который оставляет квантовую систему неизменной, но переводит каждое состояние в собственное состояние измерения, зависящее от исхода измерения. Мы можем изобразить его как измеритель, за которым следует кодировщик:



Однако в конце мы должны также получить классическое значение, поэтому, перед тем как подавать его на вход кодировщика, сделаем копию:

$$(8.80)$$

Если раскрыть это как сумму, то мы увидим выражение невозмущающего измерения ОНБ в виде КК-отображения:



В частности, это гибридный паук, и мы можем установить каузальность с помощью слияния гибридных пауков:

$$(8.70)$$

Если отбросить квантовый выход, то получится то же возмущающее измерение, что и прежде:

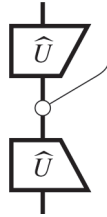
$$(8.70)$$

С другой стороны, если отбросить классический выход, то получится декогеренция:

$$(8.81)$$

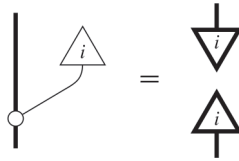
Как и в возмущающем случае, выразим общее невозмущающее измерение ОНБ в терминах гибридных пауков и унитарного процесса.

Предложение 8.84. Любое невозмущающее измерение ОНБ имеет вид:



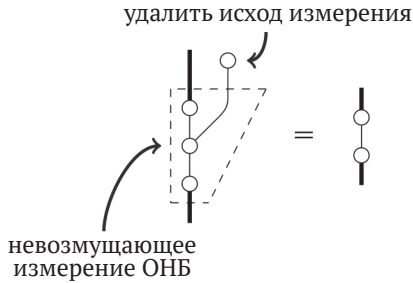
где \hat{U} – унитарный квантовый процесс.

Упражнение 8.85. Сначала покажите, что упражнение 8.32 обобщается на квантовых и гибридных пауков. Затем воспользуйтесь частным случаем этого результата:



для доказательства предложения 8.84.

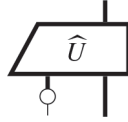
Замечание 8.86. Равенство (8.81) позволяет по-другому осмыслить декогеренцию:



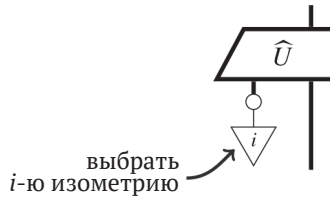
В предыдущей главе мы пришли к важному выводу о том, что квантовое измерение – это просто разновидность квантового процесса. Оно представляет взаимодействие между квантовой системой и нами. У этого взаимодействия счастливый результат – мы получаем некоторую информацию о квантовом состоянии: исход измерения. Декогеренция – это то, что происходит с квантовым состоянием, когда какое-то взаимодействие с окружающей средой становится причиной коллапса состояния, как если бы оно подверглось измерению. К сожалению, такое измерение особенно неприятно, потому что происходит спонтанно, и мы даже не знаем его исхода!

8.4.2. Управляемые унитарные процессы

Чтобы на диаграммах представить протоколы (чему посвящено несколько последующих разделов), нам нужно будет представить управляемую изометрию в виде однозначно определенного КК-отображения:



Поскольку мы можем восстановить индивидуальные изометрии следующим образом:



то управляемая изометрия является КК-отображением таким, что для всех i :

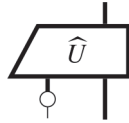
(8.82)

Тогда управляемый унитарный процесс дополнительно удовлетворяет условию

(8.83)

При помощи пауков мы можем свернуть эти индексированные наборы равенства в одно равенство.

Предложение 8.87. КК-отображение



является управляемой изометрией тогда и только тогда, когда оно удовлетворяет условию

(8.84)

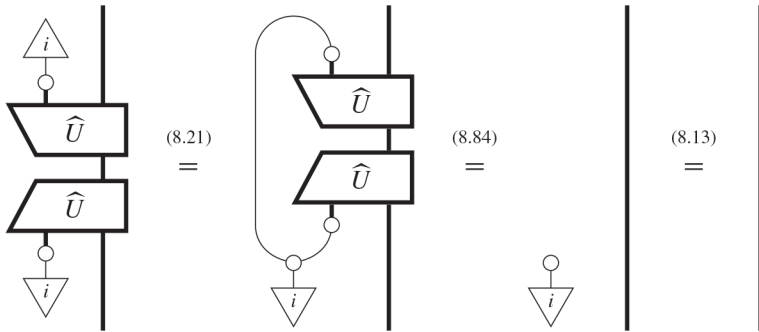
и является управляемым унитарным процессом тогда и только тогда, когда дополнительно удовлетворяет условию

(8.85)

Доказательство. Мы докажем эквивалентность (8.82) и (8.84). Сначала предположим, что (8.82) выполняется для всех i . Тогда

(8.21) (8.82) (8.13)

Поскольку левая и правая части совпадают на всех состояниях ОНБ, то имеет место (8.84). Обратно, предполагая, что (8.84) выполняется для всех i , получаем:



Эквивалентность (8.83) и (8.85) доказывается аналогично. □

Упражнение 8.88. Закончите доказательство предложения 8.87, т. е. распространите его на случай управляемых изометрий.

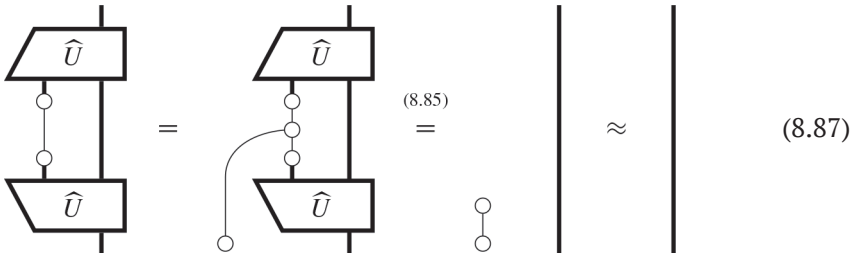
Мы можем задать вопрос, верно ли, что управляемая изометрия в целом сама является изометрией. Оказывается, что да.

Предложение 8.89. Квантовый процесс



удовлетворяющий условию (8.85), является изометрией с точностью до числа.

Доказательство. Имеем:

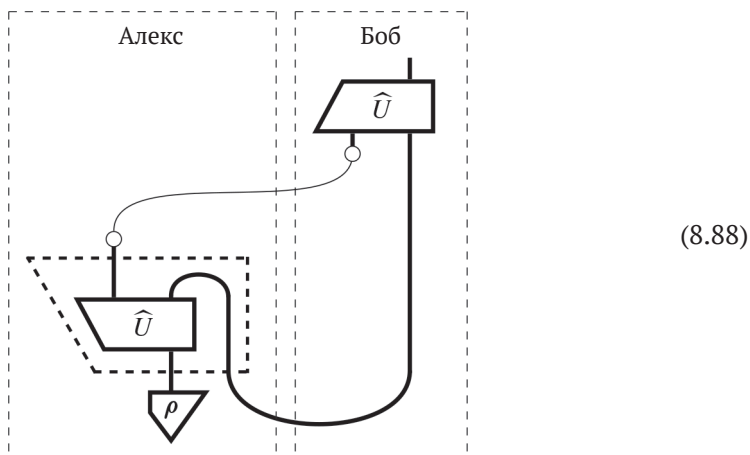


□

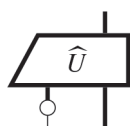
Упражнение 8.90. Является ли процесс (8.86) унитарным, если выполняется также условие (8.84)?

8.4.3. Телепортация

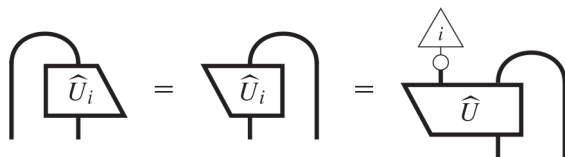
Телепортацию общего вида теперь можно представить следующим образом:



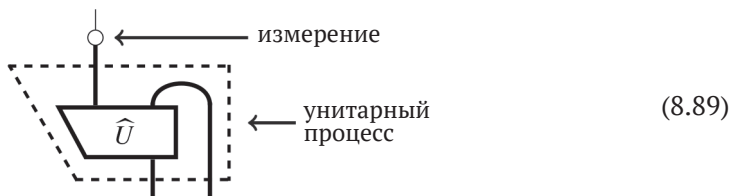
Ключевая идея заключается в том, что в диаграмму входят как процесс



так и его адьюнкт, что позволяет воспользоваться предложением 8.89 для их взаимного сокращения. Однако в этих двух вхожденииах КК-отображение играет совершенно разные роли. С одной стороны, это управляемый унитарный процесс, удовлетворяющий условиям (8.84) и (8.85). С другой стороны, оно используется для построения измерения ОНБ:



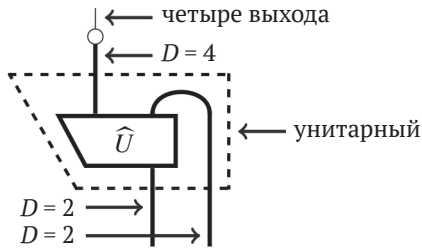
Из следствия 8.83 мы теперь знаем, что измерение ОНБ получается в точности тогда, когда имеется унитарный процесс, за которым следует процесс измерения:



Унитарность обведенного рамкой отображения означает, что выполняются следующие два равенства:

$$\begin{array}{c} \text{Diagram 1: } \hat{U} \text{ on two lines with a crossing} \\ \text{Diagram 2: } \hat{U} \text{ on two lines with a loop} \end{array} = \begin{array}{c} \text{Diagram 3: } \text{Two parallel lines} \\ \text{Diagram 4: } \text{One line} \end{array} \quad (8.90)$$

В частности, если каждая входная система D -мерна, то для того чтобы приведенное выше отображение было унитарным, размерность выходной системы должна быть равна D^2 . Поэтому если все входные системы – кубиты, то выходная система должна быть четырехмерной:



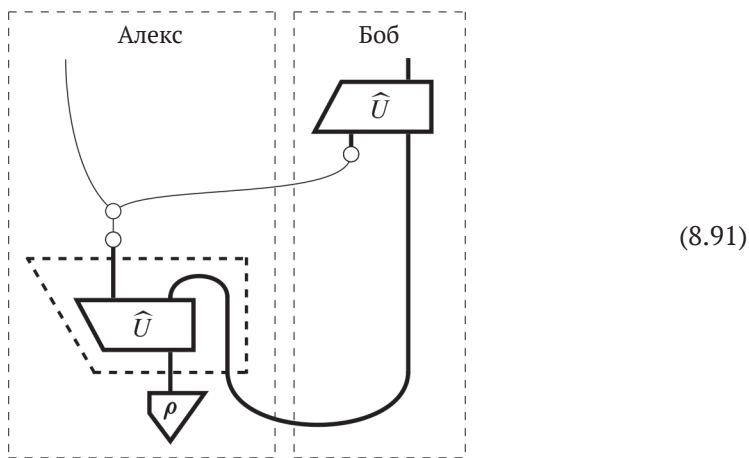
Замечание 8.91. Отметим, что унитарность заняла место равенств (6.79) и (6.80), которые мы использовали в разделе 6.4.6 при описании обобщенного протокола телепортации. В обоих случаях гарантируется ОНБ эффектов измерения. Чтобы телепортация «работала», это необязательно. Для этого нужно только, чтобы процесс (8.89) был каузальным, и, стало быть, должно выполняться первое из равенств (8.90). Это соответствует большему числу исходов измерения, чем строго необходимо; например, Алекс мог бы выполнить измерение POVM, подбросив монету и решив, какое из двух измерений ОНБ произвести.

Теперь мы можем показать, что равенство (8.88) корректно реализует телепортацию:

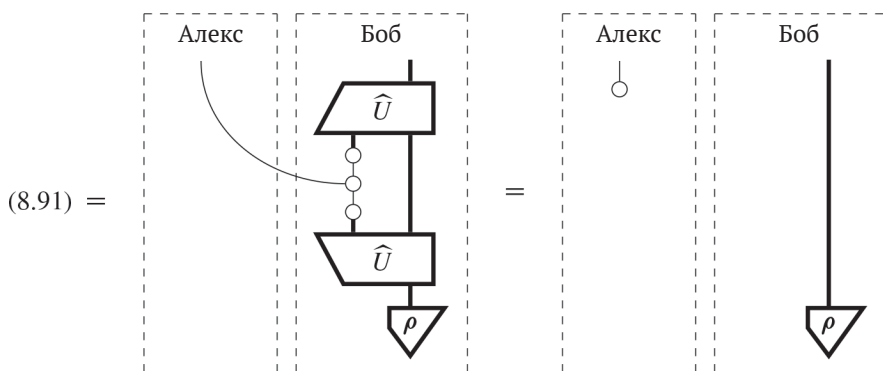
$$(8.88) = \begin{array}{|c|} \hline \text{Алекс} \\ \hline \end{array} \begin{array}{|c|} \hline \text{Боб} \\ \hline \end{array} \approx \begin{array}{|c|} \hline \text{Алекс} \\ \hline \end{array} \begin{array}{|c|} \hline \text{Боб} \\ \hline \end{array}$$

где на последнем шаге используется предложение 8.89.

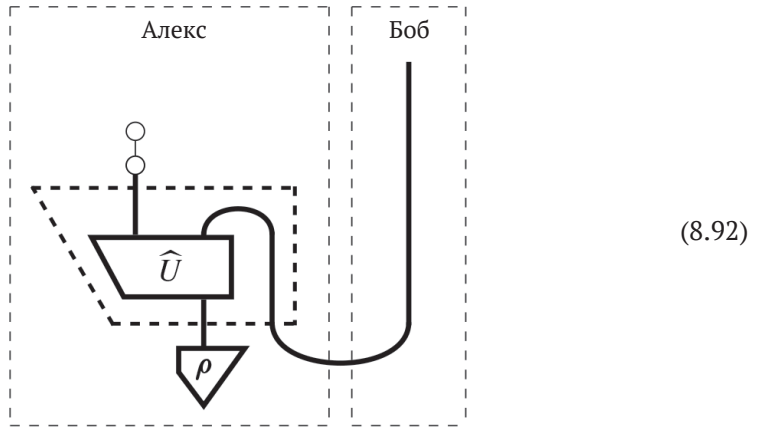
Если вы вдруг не заметили, обратите внимание на небольшую странность в том, как мы описывали телепортацию до сих пор. Исход измерения Алекса используется Бобом для внесения корректировки, но затем все выглядит так, будто этот исход измерения удален из всех блокнотов и воспоминаний. В действительности мы ожидаем получить в конце какие-то классические данные, соответствующие полученным Алексом исходам измерений. Это можно поправить, сделав копию классических данных, перед тем как они «потребляются» управляемым унитарным процессом:



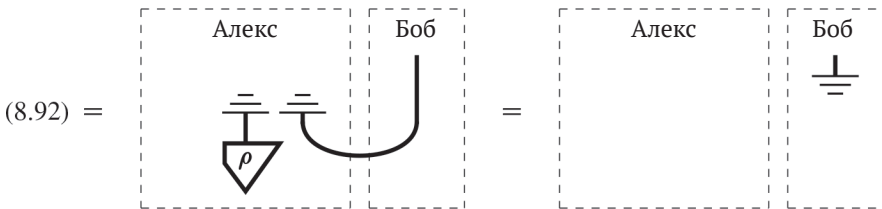
Интересно, что теперь для доказательства корректности нам необходимо равенство (8.85) в полном объеме, а не его редуцированный вариант (8.87):



Сейчас мы можем дать более ясную (свободную от сумм) картину того, что произойдет, если удалить классические данные сразу после измерения и не вносить вообще никаких корректировок, как мы делали в разделе 6.4.4. Теперь это выглядело бы так:

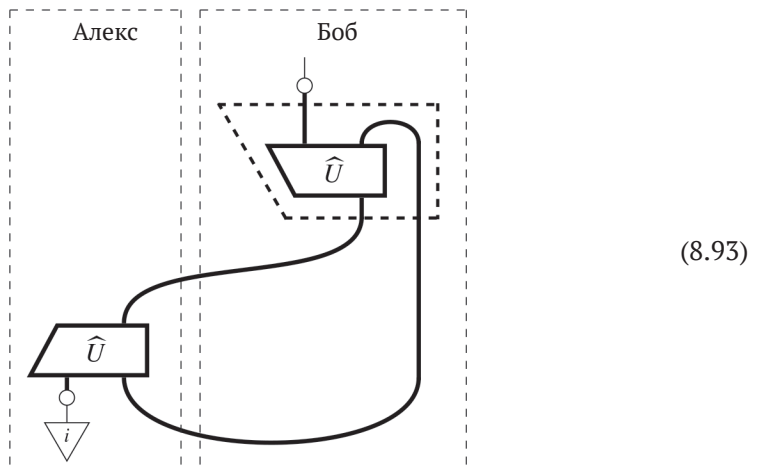


Из каузальности КК-отображений следует, что

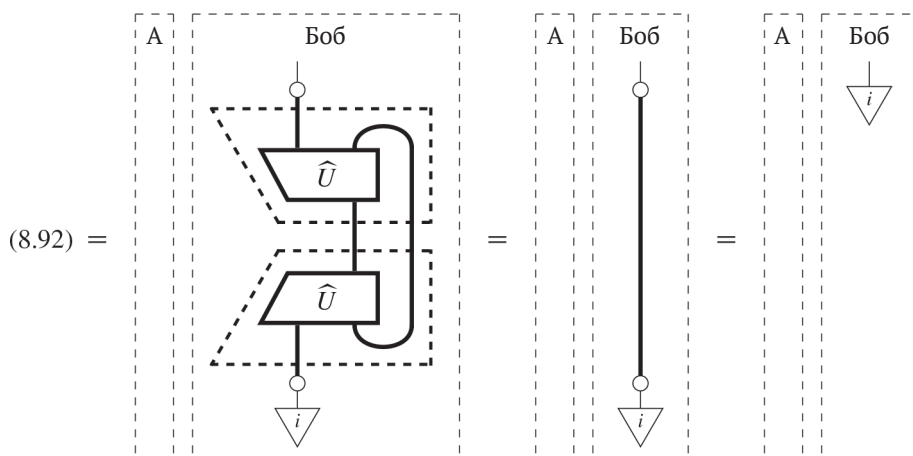


8.4.4. Плотное кодирование

Напомним (см. раздел 8.1.2), что плотное кодирование – это протокол, в котором Алекс применяет квантовые системы для передачи классических данных. Для этого он использует свои классические данные, чтобы выполнить управляемый унитарный процесс для половины состояния Белла, а затем отправляет свою половину Бобу, который может впоследствии восстановить данные Алекса, измерив обе квантовые системы вместе. На диаграмме плотное кодирование выглядит так:



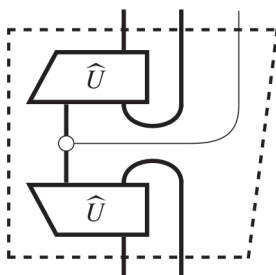
но это можно упростить до



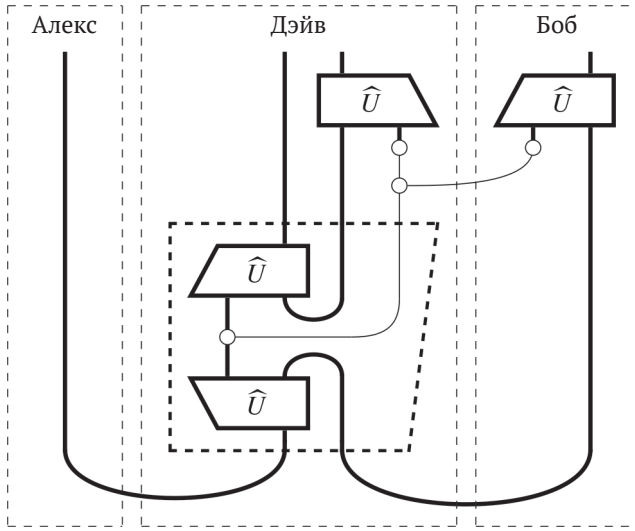
где на первом шаге использовано равенство (8.90), т. е. унитарность обведенных рамочкой блоков. Итак, для доказательства корректности мы опираемся на равенство, отличное от того, что использовалось для телепортации, – на этот факт мы уже указывали в замечании 8.2.

8.4.5. Перекоммутация запутывания

Напомним (см. раздел 7.2.4), что перекоммутация запутывания – это протокол, который переставляет местами запутывание в четырех квантовых системах посредством невозмущающего измерения двух из этих систем. Для реализации протокола Алекс и Боб в начальный момент разделяют общее состояние Белла с третьей стороной (в данном случае додо Дэйвом). Затем Дэйв выполняет невозмущающий вариант измерения, которое мы использовали раньше:

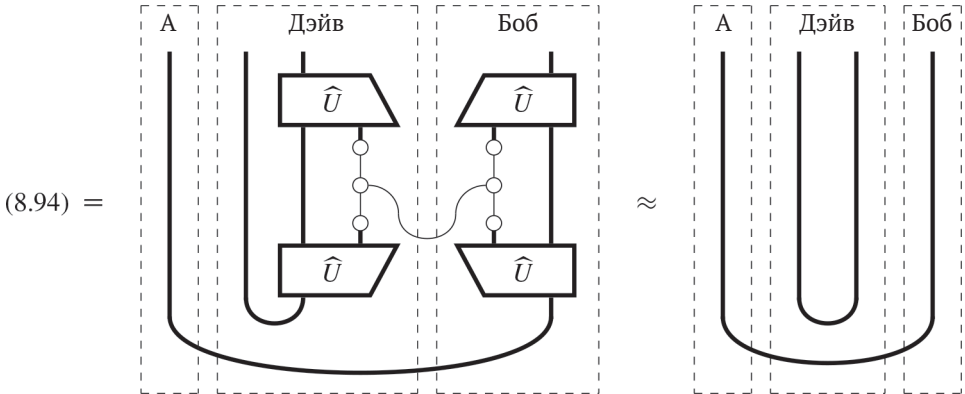


В силу предложения 8.84 это действительно невозмущающее измерение ОНБ. Затем исход этого измерения нужно скопировать в два управляемых унитарных процесса, которые производят корректировки. И вот как выглядит протокол в целом:



(8.94)

Мы можем упростить эту диаграмму, воспользовавшись слиянием гибридных пауков и уравнениями управляемой изометрии, чтобы исключить все отображения \hat{U} :



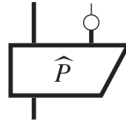
где мы дважды использовали предложение 8.89.

8.4.6. Измерения фон Неймана

В разделе 7.3.1 мы показали, что измерение фон Неймана можно определить как квантовый процесс, подчиняющийся постулату о редукции, т. е. такой, что для любых i, j :

$$\begin{array}{c} \hat{P}_j \\ \hat{P}_i \end{array} = \delta_i^j \begin{array}{c} \hat{P}_i \end{array} \quad (8.95)$$

Теперь мы можем записать измерение фон Неймана как одно КК-отображение:



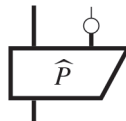
для которого ассоциированные проекторы можно восстановить следующим образом:



Стало быть, (8.95) для всех i и j теперь принимает вид:

(8.96)

Предложение 8.92. Квантовый процесс



является измерением фон Неймана тогда и только тогда, когда он удовлетворяет условию

(8.97)

Доказательство. Сначала предположим, что (8.97) выполняется. Тогда, используя

$$\begin{array}{c} \triangle i \\ \triangle j \\ \circ \\ | \end{array} \stackrel{(8.38)}{=} \delta_i^j \begin{array}{c} \triangle i \\ | \end{array} \quad (8.98)$$

получаем:

$$\begin{array}{c} \triangle i \\ \circ \\ \hat{P} \\ | \\ \triangle j \\ \circ \\ \hat{P} \\ | \end{array} = \begin{array}{c} \triangle i \\ \triangle j \\ \circ \\ \hat{P} \\ | \\ \circ \\ \hat{P} \\ | \end{array} \stackrel{(8.96)}{=} \begin{array}{c} \triangle i \\ \triangle j \\ \circ \\ \hat{P} \\ | \end{array} \stackrel{(8.98)}{=} \delta_i^j \begin{array}{c} \triangle i \\ \circ \\ \hat{P} \\ | \end{array}$$

Обратно, предполагая справедливость (8.96), мы можем аналогично показать, что левая и правая части (8.97) совпадают на всех классических эффектах, образующих ОНБ. Поэтому они равны (см. доказательство предложения 8.87). \square

У равенства (8.97) имеется прямое операционное прочтение. Измерения фон Неймана обладают тем свойством, что если измерить один раз, а затем повторить, то во второй раз получится такой же результат, как в первый. Равенство (8.97) отражает этот факт: если произвести измерение два раза, то мы получим точно такой же выход, как если бы измерили один раз, а затем скопировать исход этого измерения.

Пример 8.93. Невозмущающее измерение ОНБ, описываемое равенством (8.80), является измерением фон Неймана, если положить

$$\begin{array}{c} | \\ \hat{P} \\ | \end{array} := \begin{array}{c} \cup \\ \circ \\ | \end{array}$$

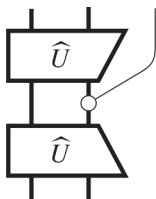
Затем, воспользовавшись слиянием гибридных пауков, получаем:

$$\begin{array}{c} \circ \\ \hat{P} \\ | \end{array} = \begin{array}{c} \cup \\ \circ \\ | \end{array} = \begin{array}{c} | \\ \circ \\ | \end{array}$$

и снова воспользуемся слиянием гибридных пауков:

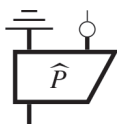
$$\begin{array}{c} \triangle i \\ \circ \\ \hat{P} \\ | \\ \triangle j \\ \circ \\ \hat{P} \\ | \end{array} = \begin{array}{c} | \\ \circ \\ | \\ \circ \\ | \end{array} = \begin{array}{c} \cup \\ \circ \\ | \\ \circ \\ | \end{array} = \begin{array}{c} \triangle i \\ \triangle j \\ \circ \\ \hat{P} \\ | \end{array}$$

Упражнение 8.94. Покажите, что более общая форма невозмущающего измерения ОНБ, представленная в предложении 8.84, является измерением фон Неймана и что вообще для любого унитарного процесса \hat{U} процесс



является измерением фон Неймана.

Как и раньше, мы получаем возмущающие измерения фон Неймана путем отбрасывания квантового выхода ассоциированного невозмущающего измерения:

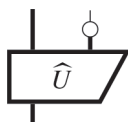


8.4.7. Измерения POVM и теорема Наймарка о дилатации

В предыдущей главе мы определили возмущающее измерение POVM как любой квантовый процесс, состоящий из эффектов. Таким образом, «возмущающее измерение POVM» – это в действительности общий процесс, переводящий квантовую систему в классическую:



В разделе 7.3.3 мы видели, что «невозмущающие измерения POVM» – это просто квантовые процессы с чистыми ветвями. В виде КК-отображения это принимает вид:



(8.99)

В разделе 7.3.3 было показано, что эти процессы уже достаточно общие, чтобы восстановить все возмущающие измерения POVM путем отбрасывания квантовой системы.

Легко видеть, что каузальность КК-отображения (8.99) транслируется в каузальность лежащего в его основе чистого квантового отображения \hat{U} :

$$\text{Diagram 1} = \text{Diagram 2} = \text{Diagram 3} \quad (8.100)$$

Поскольку \hat{U} чистое и каузальное, по теореме 6.56 оно является изометрией.

Упражнение 8.95. Обобщите (8.100) на случай произвольных КК-отображений. То есть покажите, что для любого квантового процесса

$$\text{Diagram} \quad (8.101)$$

всегда можно выбрать квантовое отображение Φ , так что оно будет каузальным. Обратно, покажите, что для любого каузального квантового отображения Φ ассоциированное КК-отображение (8.101) каузальное.

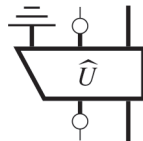
Теперь еще раз вернемся к теореме Наймарка о дилатации (теорема 7.31), которая утверждает, что любое невозмущающее измерение POVM можно выразить в терминах изометрии и измерения ОНБ. Невозмущающее измерение POVM (8.99) является каузальным КК-отображением, поэтому \hat{U} – изометрия. А благодаря нашему представлению квантовых процессов как КК-отображений:

$$\text{Diagram 1} = \text{Diagram 2} \quad \left\{ \begin{array}{l} \leftarrow \text{измерение ОНБ} \\ \leftarrow \text{изометрия} \end{array} \right.$$

тут доказывать-то и нечего!

Объединяя этот результат с дилатацией Стайнспринга для каузальных квантовых отображений, мы получаем простую альтернативную интерпретацию квантовой теории.

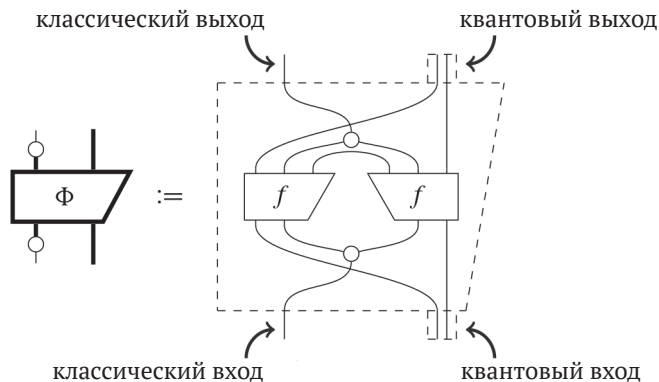
Теорема 8.96. Квантовые процессы – это линейные отображения вида



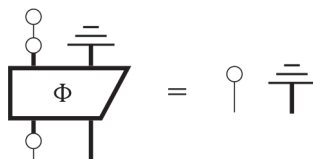
где \hat{U} – изометрия.

8.5. Итоги: что следует запомнить

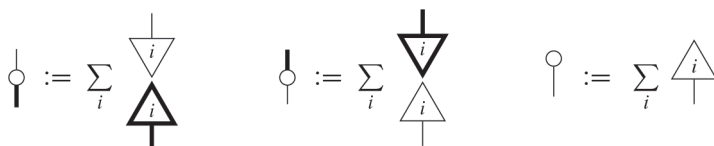
1. Теория **квантовых процессов** (или квантовая теория) – это процессная теория *классически-квантовых отображений*:



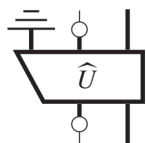
которые дополнительно являются *каузальными*:



где

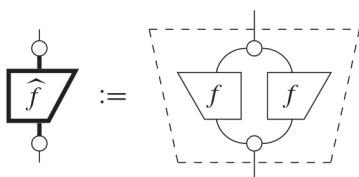


Эквивалентно, в силу теоремы Стайнстринга о дилатации, квантовые процессы – это линейные отображения вида:



где \hat{U} – изометрия.

- Теория всех **классически-квантовых отображений** допускает струнные диаграммы. Она включает подтеории **квантовых отображений** и **классических отображений**, причем последняя состоит из процессов вида:



3. Особенно хорошо ведут себя классические отображения, называемые *классическими пауками*:

$$\text{Spider} := \sum_i \left(\begin{array}{c} \triangle_i \\ \triangle_i \end{array} \right)$$

Они компонуются следующим образом:

$$\text{Spider} \circ \text{Spider} = \text{Spider}$$

4. Примером классического паука является *копирование*:

$$\text{Copying Spider} = \sum_i \left(\begin{array}{c} \triangle_i \\ \triangle_i \end{array} \right)$$

В частности, копирование определяет ОНБ:

$$\begin{array}{c} \psi \\ \triangle \end{array} \in \left\{ \begin{array}{c} i \\ \triangle \end{array} \right\} \text{ тогда и только тогда, когда } \begin{array}{c} \text{Copying Spider} \\ \psi \\ \triangle \end{array} \stackrel{(*)}{=} \begin{array}{c} \psi \\ \triangle \end{array} \begin{array}{c} \psi \\ \triangle \end{array}$$

Другой пример – *удаление*:

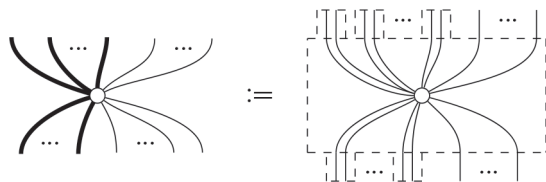
$$\text{Deletion Spider} = \sum_i \begin{array}{c} \triangle_i \end{array}$$

которое, как мы видели в п. 1 выше, играет ключевую роль в формулировке понятия каузальности. Конкретно, это классический аналог отбрасывания:

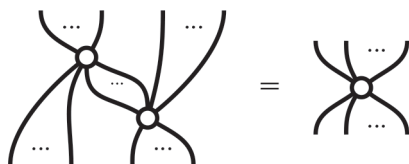
$$\begin{array}{c} \triangle \\ \text{---} \\ \text{---} \end{array} \leftrightarrow \begin{array}{c} \circ \\ | \end{array}$$

5. Путем дублирования классических пауков или объединения в пары некоторых ног

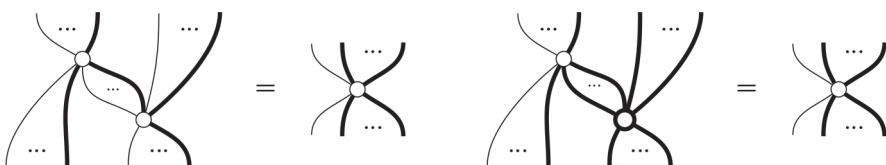
$$\text{Spider} := \text{double} \left(\text{Spider} \right)$$



мы получаем соответственно *квантовых* и *гибридных пауков*. Квантовые пауки компонуются, как классические:



тогда как любая композиция пауков, включающая, по крайней мере, одного паука с одним кружочком снова дает паука с одним кружочком:



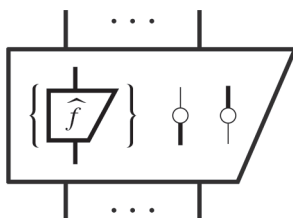
6. Примером квантового паука является *ГХЦ-состояние*:

$$\text{cup with dot} = \text{double} \left(\sum_i \text{triangle } i \right)$$

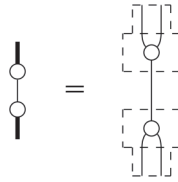
Примерами гибридных пауков являются *измеритель* и *кодировщик*:



с которыми мы уже встречались в п. 1 выше. В частности, любое КК-отображение можно получить композицией чистых квантовых отображений, измерителя и кодировщика:

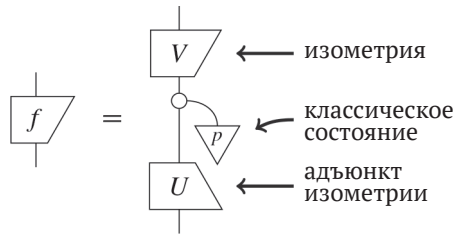


Другой пример гибридного паука – *декогеренция*:

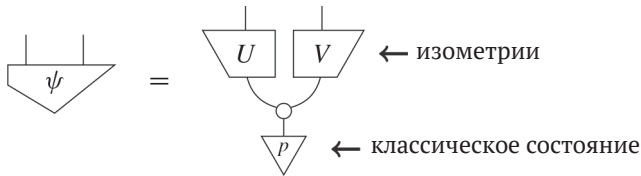


которая моделирует деградацию квантового состояния в классическое.

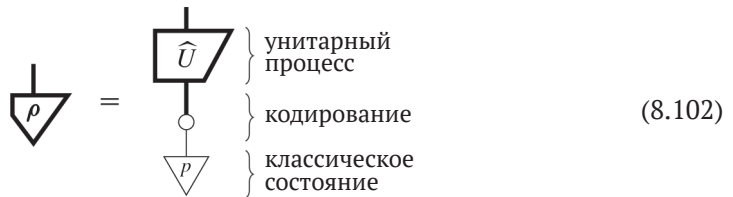
7. Любое линейное отображение f можно разложить следующим образом:



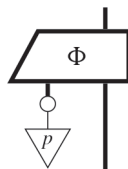
для подходящим образом выбранных пауков, а двухкомпонентные состояния допускают разложение вида:



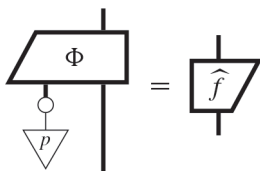
Все квантовые состояния ρ кодируют классические состояния:



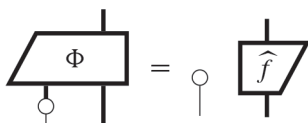
8. Смешивание нескольких процессов **одного** типа с помощью распределения вероятностей p можно представить в виде КК-отображения:



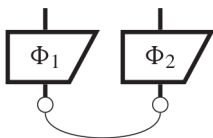
В силу (8.102) любое каузальное квантовое состояние можно рассматривать как смесь чистых каузальных квантовых состояний. Если смесь чистая:



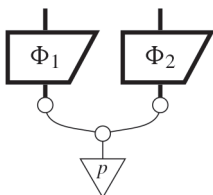
то



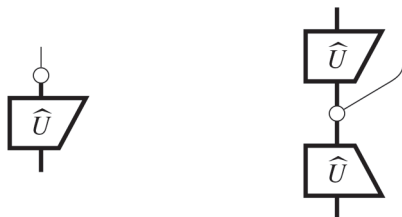
9. Двухкомпонентное квантовое состояние является *запутанным*, если его нельзя представить в виде



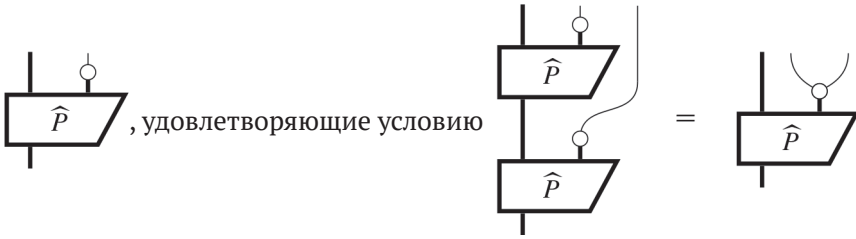
или, эквивалентно, если нельзя записать в виде смеси:



10. Возмущающие и невозмущающие измерения ОНБ имеют соответственно следующий вид для некоторого унитарного процесса \hat{U} :



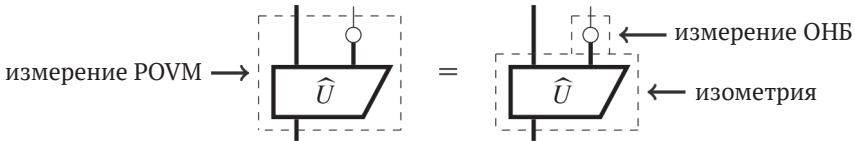
Невозмущающие измерения фон Неймана – это квантовые процессы:



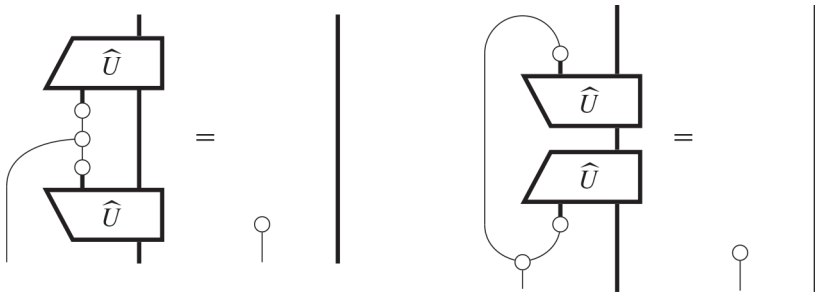
Возмущающие измерения фон Неймана – то же самое, но с отброшенным квантовым выходом. Возмущающие и невозмущающие измерения POVM – это квантовые процессы вида:



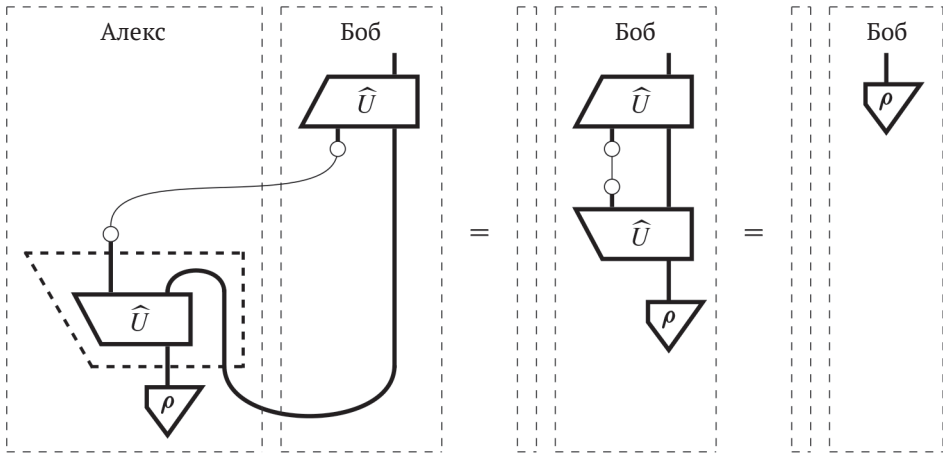
В частности, процесс \hat{U} должен быть изометрией в силу каузальности, поэтому теорема Наймарка о дилатации теперь сводится к двум разным прочтениям одной и той же диаграммы:



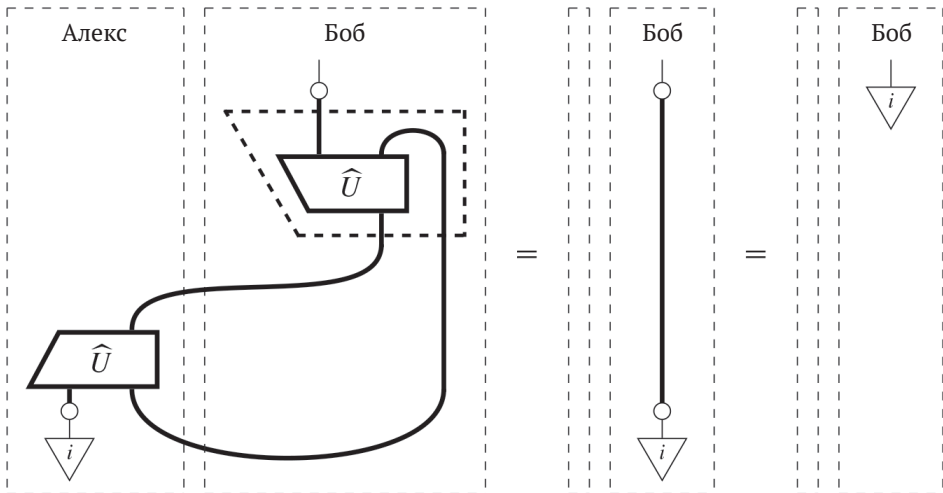
11. Управляемые унитарные процессы можно определить следующим образом:



Это позволяет дать полностью диаграммные представления квантовых протоколов, например *квантовой телепортации*:



и плотного кодирования:

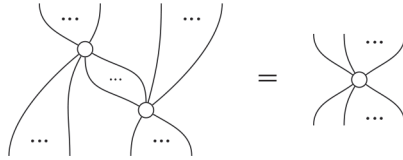


8.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

В этом разделе мы подробнее остановимся на том, что такое пауки с алгебраической и коалгебраической точками зрения. На самом деле если опустить требование коммутативности, то обнаружится, что они являются графическим инструментом для изучения C^* -алгебр – структур, популярных среди специалистов по алгебре и математической физике. Затем мы вкратце обсудим, как выглядят пауки для несамосопряженных ОНБ. Оказывается, что у них на ногах растут волосы! И если вы еще недостаточно напугались, то в последнем разделе мы еще и увидим, как пауки вылезают у нас изо рта!

8.6.1. Пауки как алгебры Фробениуса*

Мы вводили пауков как созданий с произвольным количеством ног, которые сливаются, когда «дрыгают ногами»:

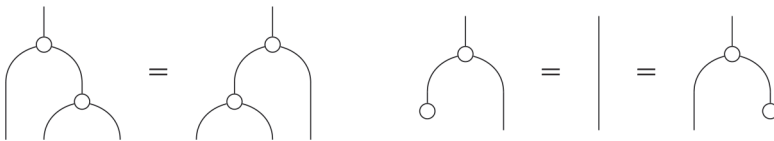


Однако это сильно отличается от обычного способа определения этих процессов и даже от того, в каком виде они предстали при нашей первой встрече. Обычно они определяются в терминах чего-то, более знакомого математикам.

Определение 8.97. Ассоциативная алгебра над векторным пространством V состоит из пары линейных отображений:

$$\text{multiplication spider} : V \otimes V \rightarrow V \qquad \text{unit spider} : \mathbb{C} \rightarrow V$$

таких, что отображение $\text{multiplication spider}$ ассоциативно и обладает единицей unit spider :



Это то же самое, что наличие операции умножения элементов V , которая была бы унитарной и линейной относительно обоих аргументов. Однако у такого способа записи есть преимущество: его очень легко перевернуть вверх ногами! Это стандартное соглашение в теории категорий: нечто называется «кообъектом», если это «объект», в котором все отображения перевернуты.

Определение 8.98. Коассоциативная алгебра над векторным пространством V состоит из пары линейных отображений:

$$\text{comultiplication spider} : V \rightarrow V \otimes V \qquad \text{counit spider} : V \rightarrow \mathbb{C}$$

таких, что отображение $\text{comultiplication spider}$ коассоциативно и обладает коединицей counit spider :



Самый очевидный способ получить такой объект – считать, что V гильбертово, а не просто векторное пространство, и взять адьюнкт ассоциативной алгебры:

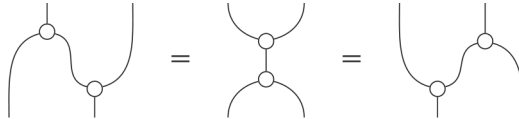
$$\circlearrowleft := (\circlearrowright)^\dagger \qquad \circlearrowright := (\circlearrowleft)^\dagger$$

Наверное, алгебраические структуры вам хорошо знакомы, а вот коалгебраические – нет. Быть может, одна из причин этого состоит в том, что они не очень интересны в тех процессных теориях, где \otimes ведет себя как декартово произведение. Например, если в определении 8.98 заменить теорию **линейных отображений** теорией **функций**, то единственными коассоциативными алгебрами будут «универсальные» функции копирования:

$$\circlearrowleft : X \rightarrow X \times X :: x \mapsto (x, x).$$

Однако если \otimes не является декартовым произведением, как, например, в теории **линейных отображений**, то появляется множество интересных коалгебр, и, что более важно, мы можем определять интересные структуры, обладающие как алгебраической, так и коалгебраической частью. Главным нашим примером будет такой.

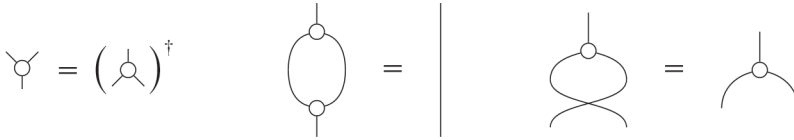
Определение 8.99. Алгебра Фробениуса состоит из ассоциативной алгебры $(\circlearrowright, \circlearrowleft)$ и коассоциативной алгебры $(\circlearrowleft, \circlearrowright)$, которые дополнительно удовлетворяют уравнениям Фробениуса:



С помощью алгебр Фробениуса можно также определить «паукоподобные» отображения:

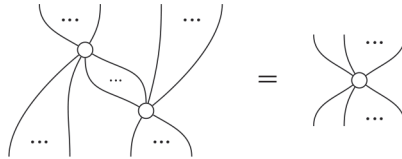
Однако если мы хотим, чтобы эти пауки сливались, как в теореме 8.34, и чтобы их множество было замкнуто относительно адьюнкции, то понадобится специальный вид алгебр Фробениуса.

Определение 8.100. Инволютивной специальной коммутативной алгеброй Фробениуса (dagger special commutative Frobenius algebra – \dagger -SCFA) называется алгебра Фробениуса, удовлетворяющая дополнительным условиям:

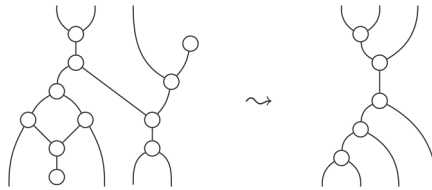


Очевидно, что символ \dagger (инволютивная) в названии \dagger -SCFA касается горизонтального отражения, тогда часть SC гарантирует следующее.

Предложение 8.101. Пауки, определенные как в (8.103), для \dagger -SCFA компонуются следующим образом:



Доказательство (набросок). Достаточно показать, что любую связную диаграмму, состоящую из $(\circlearrowleft, \circlearrowright, \circlearrowleft^\dagger, \circlearrowright^\dagger)$, можно трансформировать в каноническую форму, используя только уравнения алгебры Фробениуса:

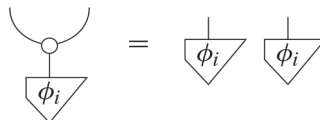


В частности, любых двух связных пауков можно трансформировать в каноническую форму, которая будет одним большим пауком. Доказательство можно провести индукцией по количеству кружочков на диаграмме. \square

Обратите внимание, что ни в одном определении из этого раздела не используется структура векторного пространства, поэтому все они имеют смысл в любой инволютивной симметричной моноидальной категории.

Алгебраическое представление пауков дает нам возможность применять стандартные теоремы алгебры, чтобы доказать, что они всегда определяют ортонормированный базис.

Теорема 8.102. Для любой \dagger -SCFA множество состояний $\{\phi_i\}$ такое, что:



образует ОНБ. Таким образом, всякое семейство пауков однозначно определяет (и однозначно определяется) ОНБ.

Доказательство (набросок). Доказательство проводится в два этапа. Сначала нужно показать, что алгебраическая часть \dagger -SCFA всегда является полупростой.

Полупростые алгебры (которые мы здесь не определяем) хорошо изучены, особенно в конечномерных пространствах, благодаря *теореме Веддербёрна*. Из этой теоремы, в частности, следует, что любая ассоциативная алгебра, являющаяся полупростой и *коммукативной*, изоморфна прямой сумме экземпляров тривиальной алгебры над \mathbb{C} :

$$\begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \end{array} \cong \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \end{array} \oplus \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \end{array} \oplus \dots \oplus \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \end{array} \quad (8.104)$$

Эта «тривиальная алгебра» может показаться странной, т. к. обычно мы не рисуем провода для \mathbb{C} . На самом деле

$$\begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \end{array} := \boxed{\phantom{\text{---}}}$$

Очевидно, что эта алгебра ассоциативна, а в роли единицы выступает также пустая диаграмма. Алгебра (8.104) всегда имеет базис, состоящий из копируемых состояний, который выглядит следующим образом:

$$\diamond 0 \oplus \dots \oplus \diamond 0 \oplus \diamond 1 \oplus \diamond 0 \oplus \dots \oplus \diamond 0$$

Тогда того факта, что $(\text{---})^\dagger = \text{---}$, достаточно, чтобы доказать, что любой базис, состоящий из копируемых состояний, должен быть ортогональным, и более того:

$$\begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \\ \text{---} \\ | \\ \circ \\ \text{---} \\ | \\ \text{---} \end{array} = \text{---}$$

означает, что он должен состоять из нормированных состояний. □

8.6.2. Некоммукативные пауки*

В теореме 8.102 мы видели, что \dagger -SCFA однозначно определяет ОНБ. А что, если опустить некоторые буквы в акрониме «SCFA»? Если опустить букву S (специальная), то вместо ОНБ мы получим ортогональные базисы. А если опустить \dagger , но оставить S, то получатся произвольные базисы. Это весьма интересно. Но если взяться за букву C (коммукативная), то будет еще интереснее. Мы, впрочем, не станем совсем отказываться от коммукативности, а заменим ее более слабым условием.

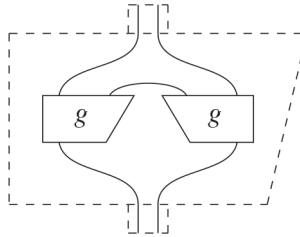
Определение 8.103. Инволютивной специальной *симметричной* алгеброй Фробениуса (\dagger -SSFA) называется алгебра Фробениуса, удовлетворяющая таким дополнительным условиям:

$$\begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \end{array} = \left(\begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \end{array} \right)^\dagger \quad \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \\ \text{---} \\ | \\ \circ \\ \text{---} \\ | \\ \text{---} \end{array} = \text{---} \quad \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \circ \\ \text{---} \\ \text{---} \end{array}$$

Предложение 8.106. Линейное отображение Φ является квантовым тогда и только тогда, когда существует линейное отображение f такое, что:

$$\Phi := \text{Diagram} \tag{8.106}$$

Доказательство. Правая часть (8.106) уже имеет вид квантового отображения. Обратно, любое квантовое отображение принимает вид

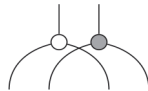


для некоторого g . Это можно привести к виду (8.106), положив:

$$f := \text{Diagram}$$

Тогда числа в (8.106) сокращаются с получающейся окружностью. □

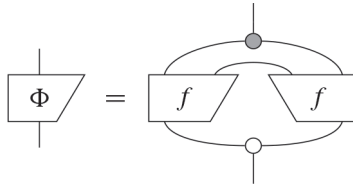
Возможно, не сразу понятно, что мы выиграли, – ведь эквивалентная форма квантового отображения (8.106) сложнее той, с которой мы начали. Однако теперь условие, при котором отображение является классическим или квантовым, – это равенство (8.105), а меняется только алгебра. Иными словами, классические и квантовые типы можно рассматривать на равных основаниях. Более того, если имеются две \dagger -SSFA над системами A и B , то



дает нам \dagger -SSFA над системой $A \otimes B$. Так что с помощью (8.105) мы дополнительно можем трактовать \otimes -композиции классических и квантовых систем единообразно, как наши базовые типы. Вся информация о том, какие части системы классические, а какие – квантовые, тогда будет закодирована в результирующей алгебре.

Поэтому имеет смысл считать, что типом является не просто гильбертово пространство A , а пара (A, \circ) , состоящая из A и \dagger -SSFA над A . Руководствуясь этим отображением, мы определим новую процессную теорию на основе старой.

Определение 8.107. В процессной теории **CP***[линейные отображения] типами являются пары (A, \circ) , состоящие из гильбертова пространства A и \dagger -SSFA над A , а процессами из (A, \circ) в (B, \bullet) – линейные отображения Φ из A в B вида:

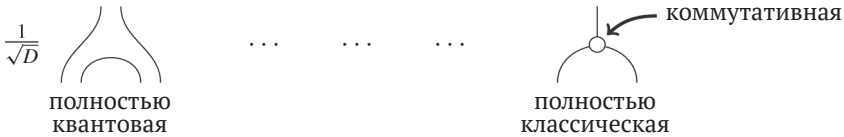


для некоторого линейного отображения f .

На самом деле КК-отображения – это в точности те отображения в **CP***[линейные отображения], типами которых являются \otimes -композиции классических и квантовых систем, т. е.

КК-отображения \subset CP*[линейные отображения].

Полная процессная теория **CP***[линейные отображения] содержит как «полностью классические» и «полностью квантовые» системы, так и промежуточные.



В состав «промежуточных» входят \otimes -композиции классических и квантовых систем, а также более общие полуклассические (иногда их называют «суперселектированными») системы, являющиеся прямыми суммами квантовых систем. Тот факт, что прямая сумма – общая форма систем в теории **CP***[линейные отображения], следует из теоремы Веддербёрна, которая мельком упоминалась в доказательстве теоремы 8.102.

Отметим, что единственное, что мы взяли из процессной теории **линейных отображений** при определении теории **CP***[линейные отображения], – тот факт, что она допускает струнные диаграммы. Поэтому в ту же игру «добавь CP*» можно сыграть и с другими процессными теориями (или моноидальными категориями) и посмотреть, что из этого выйдет. Иногда получаются удивительные результаты! Например, **CP***[отношения] дает процессную теорию, в которой типами являются *группоиды* (математические объекты, обобщающие группы), а отображениями – отношения, сохраняющие структуру группоидов.

8.6.3. Волосатые пауки*

В разделах 8.2.4 и 8.3.1 мы упоминали о пауках для несамосопряженных ОНБ. И как же они могут выглядеть? В замечании 8.40 мы сказали, что одно из решений – просто опустить равенства

$$\begin{array}{ccc}
 \text{cup with dot} = \text{cup} & & \text{cap with dot} = \text{cap} \\
 \text{---} & & \text{---} \\
 \text{---} & & \text{---}
 \end{array} \quad (8.107)$$

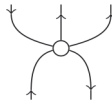
или «поправить» их, чтобы учесть сопряжение. На самом деле мы уже проделали это для некоторых «двуногих» пауков в разделе* 4.6.2:



Мы можем вставить кружочки:



и добавить дополнительные ноги:



В разделе 4.6.2 мы использовали стрелки, чтобы отличить систему A от двойственной ей системы A^* . У этого соглашения был полезный побочный эффект, заключающийся в том, что тип сопряженного базисного состояния отличается от типа самого состояния:

$$\begin{array}{ccc}
 \text{triangle } i \text{ with dot} & \text{и} & \text{triangle } i \\
 \text{---} & & \text{---} \\
 \text{---} & & \text{---}
 \end{array} := \text{cup with } i \text{ triangle}$$

и аналогично тип адьюнкта отличается от типа транспонированного состояния. Поэтому стрелки на ногах «волосатого» паука говорят, какие базисные состояния или эффекты следует сопрягать:

$$\text{spider} := \sum_i \begin{array}{ccc} \text{triangle } i & \text{triangle } i & \text{triangle } i \\ \text{---} & \text{---} & \text{---} \\ \text{---} & \text{---} & \text{---} \end{array}$$

По определению, мы имеем такие поправленные равенства крышек и чашек (8.107):

$$\begin{array}{ccc}
 \text{cup with dot} = \text{cup} & & \text{cap with dot} = \text{cap} \\
 \text{---} & & \text{---} \\
 \text{---} & & \text{---}
 \end{array}$$

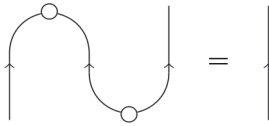
Кроме того, всякий раз, как у паука есть одна «входящая» нога и одна «исходящая» нога, он является проводом:



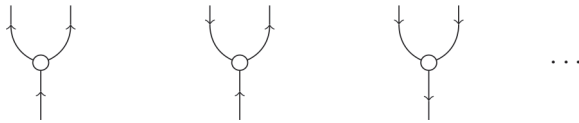
Теперь правила игры таковы, что пауки могут «дрыгать ногами», только когда ориентации ног совпадают. Отметим, в частности, что появился новый вид чашек и крышек:



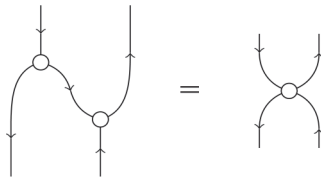
который по-прежнему удовлетворяет уравнениям разгибания:



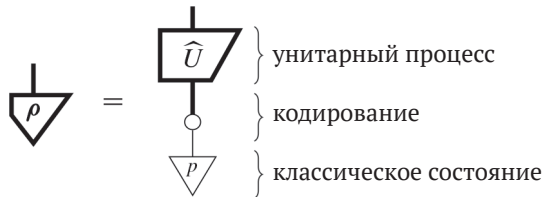
Аналогично есть несколько вариантов старого доброго копирующего паука:



которые могут сливаться с другими волосатыми пауками, например:



В замечании 8.57 мы утверждали, что необходимость унитарного процесса в разложении



любого квантового состояния ρ вызвана ограничением, что ОНБ должны быть самосопряженными. Теперь, полагая

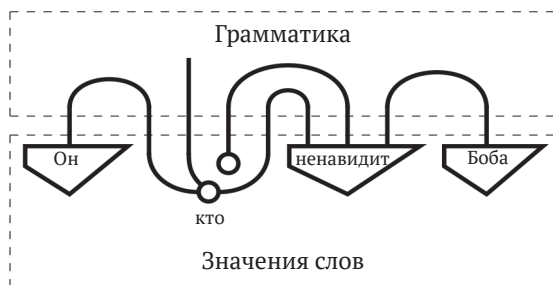
$$| \quad := \quad ||$$

мы можем опустить \hat{U} и получить идеальную симметрию между разложениями «классическое как квантовое» и «квантовое как классическое»:



8.6.4. Пауки как слова*

В разделе* 6.6.3 мы говорили, что предложения можно представлять с помощью диаграмм. Пауки тоже играют роль в этой пьесе, поскольку их можно использовать для представления относительных местоимений:



Здесь паук комбинирует «он» с «ненавидит Боба», чтобы вернуть нечто, обладающее обоими свойствами, то есть, вероятно, мужчину, который ненавидит Боба. Таким образом, пауками полна не только эта книга, но и вообще любая!

8.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Диаграммное представление классических данных инициировано в работе Coecke and Pavlovic (2007), где даны полностью диаграммные, хотя и без пауков, определения управляемых унитарных процессов, измерений фон Неймана и телепортации. Переход к паукам произошел в работе Coecke and Paquette (2008). Гораздо раньше, в работе Davies and Lewis (1970), классические данные, порождаемые квантовыми измерениями, были также представлены в терминах ОНБ. Однако не было проведено различие между пространствами, в которых представлялись классические данные, и теми, в которых описывались квантовые системы. Парадигма двойных и одиночных проводов и ранняя форма получающихся при этом классически-квантовых отображений впервые появились в работе Coecke et al. (2010a). Представление измерений ОНБ в виде гибридных пауков впервые выполнено в работе Coecke et al. (2012).

«Bastard»¹ – так первоначально называлась вокальная группа Motörhead, Лемми сменил название, после того как ему сказали, что группа с названием Bastard никогда не пробьется в программу Top of the Pops. Впрочем, для наших пауков это не важно, тем более что и программы-то этой уже не существует. Покойтесь с миром, Лемми и Лил Филти.

В настоящее время есть несколько других диаграммных представлений квантовой теории, например Chiribella et al. (2010) и Hardy (2012). Однако в них данные всегда рассматриваются не в терминах диаграмм. С другой стороны, идея о фундаментальном значении очищения как характерной особенности квантовой теории (см. раздел 8.2.2) была выдвинута в работах Chiribella et al. (2010, 2011). Изучение связи между различимостью и копируемостью в процессных теориях было предпринято в работе Chiribella (2014).

Плотное кодирование впервые предложено в работе Bennett and Wiesner (1992), а его диаграммное представление появилось в работе Coecke and Pavlovic (2007). В статье Coecke and Paquette (2008) дано диаграммное доказательство теоремы Наймарка о дилатации, но оно было без необходимости усложнено по сравнению с изложенным в этой книге. Диаграммное представление байесовской инверсии в примере* 8.27 заимствовано из работы Coecke and Spekkens (2012).

Понятие алгебры Фробениуса введено в работе Brauer and Nesbitt (1937), но впервые представлено в его современной теоретико-категорной форме в работе Carboni and Walters (1987). Тот факт, что у специальных коммутативных алгебр Фробениуса имеются канонические формы (т. е. пауки), которые «сливаются» воедино, следует из «народной теоремы», связывающей алгебры Фробениуса с геометрическими объектами, называемыми *кобордизмами*. Стандартная книга на эту тему – Kock (2004). Явное доказательство «паучьей» формы специальных коммутативных алгебр Фробениуса было дано с использованием дистрибутивных законов в работе Lack (2004), в которой то, что мы называем пауками, представлено в виде коспанов (cospan) функций между конечными множествами. Тот факт, что пауки характеризуют базисы, взят из работы Coecke et al. (2013c). Авторы этой работы опираются на спектральную теорию C^* -алгебр, чтобы показать, что допускающие копирование состояния образуют базис, тогда как наше изложение основано на (гораздо более старой) теореме классификации Веддербёрна (1906). Полнота диаграмм пауков доказана в работе Kissinger (2014b).

Связь между инволютивными алгебрами Фробениуса и C^* -алгебрами (см. замечание 8.104) взята из работы Vicary (2011). CP^* -построение, категорная конструкция, давшая начало процессной теории **CP^* [линейные отображения]** из раздела 8.6.2, приведена в работе Coecke et al. (2013a). Аксиоматизация этой конструкции, аналогичная аксиоматизации **квантовых отображений** из раздела* 6.6.2, была разработана в статье Cunningham and Heunen (2015); связь между этой процессной теорией и квантовой логикой (см. раздел* 7.6.2) обсуждается в работе Coecke et al. (2013b). Характеристика классических и квантовых систем в терминах теоретико-информационных ограничений с использованием CP^* -построения приведена в работе Heunen and Kissinger (2016), где обобщаются результаты по C^* -алгебрам, полученные в работе Clifton et al. (2003).

¹ В оригинальном тексте «гибридные пауки» называются «bastard spiders». Отсюда и этот пассаж по поводу группы «Bastard». – *Прим. перев.*

Существует также целый пласт работ, ставящих целью классифицировать пауков в теории **отношений**, а не **линейных отображений**. На самом деле это не так уж странно, если принять во внимание, что в работе Carboni and Walters (1987) алгебры Фробениуса были введены для аксиоматизации теории **отношений**. Это направление началось работой Coecke and Edwards (2011), где было замечено, что существуют неожиданные пауки, которые не возникают из ОНБ. После этого Павлович (Pavlovic, 2009) классифицировал всех пауков в теории **отношений**, а в работе Neunen et al. (2012b) этот результат был обобщен на некоммутативные алгебры Фробениуса.

В контексте значений слов в естественном языке описание относительных местоимений в терминах пауков появилось в работе Sadrzadeh et al. (2013, 2014). Более поздние результаты в этом направлении, где еще сильнее подчеркивается структурная связь с квантовой теорией, можно найти в работах Piedeleu et al. (2015), Balkir et al. (2016) и Bankova et al. (2016).

Последние фразы введения к этой главе и раздела* 8.6.4 отсылают к комическому роману ужасов Дэвида Вонга «This Book Is Full of Spiders»¹.

¹ Эта книга полна пауков. – *Прим. перев.*

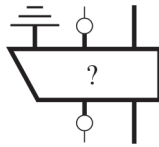
Глава 9

Изображение фаз и дополнительности

Объединившись, паутины могут спеленать и льва.

– Эфиопская поговорка

В предыдущей главе на сцену вышли пауки. Поначалу казалось, что их роль сводится лишь к пересылке классических данных или к транзиту на «планету Квантум» и обратно, а все по-настоящему интересное, целиком квантовое, происходит внутри какого-то общего квантового процесса:

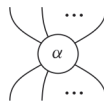


Поскольку мы не можем применить ни одно из наших шикарных правил вроде слияния пауков, этот «черный ящик» оказывается диаграммным тупиком. Настоящая глава посвящена «вскрытию» таких ящиков. Мы уже приоткрывали их в разделе 8.2.5, где показали, что все линейные отображения, а стало быть, и все квантовые отображения, состоят из пауков и изометрий – «черных ящиков». Теперь откроем их до конца.

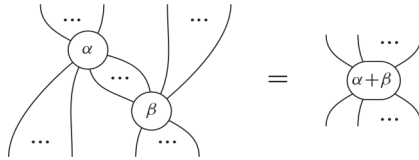
Что мы найдем внутри? Страшный кошмар арахнофобов: еще больше пауков, а как же иначе! В отличие от жизни здесь, на Земле, где роль членистоногих сведена преимущественно к пище или удобрению, в этой книге они являются доминирующим и, собственно говоря, единственным видом!

Действительно, дочитав книгу до конца, мы сможем строить произвольные отображения из одних лишь пауков. Но прежде нам еще нужно повысить разнообразие популяции пауков. Основанием для этих (на сей раз последних) добавлений в графический язык служат два важных понятия квантовой теории: *фазы* и *дополнительность* (или взаимная несмещенность).

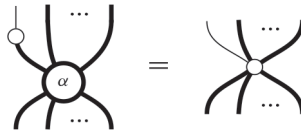
Фазы – это «украшения», которые может переносить паук:



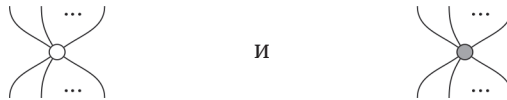
У этих украшений есть две важные черты. Во-первых, когда пауки сливаются, их украшения объединяются:



Во-вторых, украшения не способны пережить переход из квантовой области в классическую. Когда украшенный квантовый паук делает попытку установить любой контакт с классической областью, его украшения исчезают:



Как и было возведено в предыдущей главе, мы также будем рассматривать пауков разных цветов:



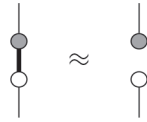
которые будут представлять разные ОНБ. Разноцветные пауки уже не могут сливаться, но все-таки должны сохранять способность к простым взаимодействиям. На самом деле способ их взаимодействия прямо противоположен слиянию. Если пауки одного и того же семейства любят друг друга, то *дополнительные пауки* терпеть не могут чужих, и разгорающиеся из-за этого войны пауков приводят к серьезным травмам – утрате конечностей:

(9.1)

То есть пауки одного семейства сливаются, а когда дополнительные пауки «дрыгают ногами», ноги отваливаются (но всегда парами). Если взять существенную часть приведенного выше равенства

(9.2)

и записать его в терминах гибридных пауков:



то напрашивается очевидное операционное прочтение дополнительного базиса:

(кодирование в \circ) ЗАТЕМ (измерение в \bullet) = (никакой передачи данных).

Хотя дополнителность, похоже, говорит о том, чего мы «не можем сделать», равенство (9.2) оказывается весьма мощным. В частности, в разделе 9.2.6 мы коротко опишем, как воспользоваться дополнителностью для *квантовой криптографии*. А еще более полезны следующие равенства:



которым удовлетворяют особенно интересные пары *сильно дополнителных пауков*. Несмотря на то что эти новые уравнения вышли на поле квантовых исследований совсем недавно, они ни в коем случае не являются специальными, а давно уже используются в разных разделах чистой математики, где определяют *биалгебру*.

Эти новые уравнения обладают большой доказательной силой, настолько большой, что в сочетании с законами слияния (украшенных) пауков образуют основу системы уравнений, называемой *ZX-исчислением*, которая является *полной* для доказательства равенств между широким классом квантовых отображений, именуемых **отображениями Клиффорда**. ZX-исчисление станет нашим швейцарским ножом в следующих главах, когда мы будем изучать приложения к квантовым вычислениям, основаниям квантовой теории и теориям (квантовых) ресурсов.

9.1. УКРАШЕННЫЕ ПАУКИ

Итак, начнем разговор об украшениях.

9.1.1. Несмещенность и фазовые состояния

Начиная с этого момента, мы будем обозначать семейство пауков (или, эквивалентно, ОНБ, по теореме 8.41) просто кружочком соответствующего цвета, например \circ .

Определение 9.1. Нормированное чистое состояние называется *несмещенным* для \circ , если имеет место равенство

$$\begin{array}{c} \circ \\ | \\ \triangle \\ \psi \end{array} = \frac{1}{D} \circ \tag{9.3}$$

или эквивалентно:

$$\begin{array}{c} | \\ \circ \\ \swarrow \quad \searrow \\ \psi \quad \psi \end{array} = \frac{1}{D} \begin{array}{c} | \\ \circ \end{array} \quad (9.4)$$

Что это означает? В левой части (9.3) мы видим измеряемое квантовое состояние $\widehat{\psi}$, а в правой части (9.3) – равномерное распределение вероятностей. Поэтому смысл равенства заключается в том, что измерение $\widehat{\psi}$ должно давать равномерно распределенные исходы, или иными словами: квантовое состояние $\widehat{\psi}$ не предрасположено ни к какому исходу измерения, т. е. является «несмещенным».

Мы можем также переформулировать определение 9.1 в терминах правила Борна:

$$\begin{array}{c} \triangle i \\ | \\ \widehat{\psi} \end{array} \stackrel{(8.6)}{=} \begin{array}{c} \triangle i \\ | \\ \circ \\ | \\ \widehat{\psi} \end{array} \stackrel{(9.3)}{=} \frac{1}{D} \begin{array}{c} \triangle i \\ | \\ \circ \end{array} = \frac{1}{D}$$

Это означает, что правило Борна дает одинаковые вероятности всех исходов. Обратное тоже верно.

Упражнение 9.2. Покажите, что нормированное чистое состояние является *несмещенным* для измерения ОНБ, если для всех i имеет место равенство:

$$\begin{array}{c} \triangle i \\ | \\ \widehat{\psi} \end{array} = \frac{1}{D}$$

Пример 9.3. Можно задаться вопросом, какой аналог есть у этого понятия в теории вероятностей. Там распределение вероятностей называется «несмещенным», если все «исходы» i встречаются с одинаковой вероятностью. Конечно, существует только одно такое распределение – равномерное.

Таким образом, понятие несмещенного распределения вероятностей не дает нам ничего нового. Но очевидно, что несмещенность квантовых состояний что-то новое все же несет, иначе мы не стали бы ее определять. Чтобы убедиться в том, что для измерения ОНБ существует много несмещенных состояний, рассмотрим матричную форму такого состояния. Пользуясь соответствием (8.32), левую часть (9.4) можно записать в виде произведения Адамара состояния ψ на сопряженное к нему. Стало быть, в матричной форме равенство (9.4) принимает вид:

$$\begin{pmatrix} \overline{\psi^0} \psi^0 \\ \vdots \\ \overline{\psi^{D-1}} \psi^{D-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{D} \\ \vdots \\ \frac{1}{D} \end{pmatrix},$$

т. е. для всех i имеем

$$\overline{\psi^i} \psi^i = \frac{1}{D}.$$

В разделе 6.1.2 мы видели, что числа, удовлетворяющие условию

$$\overline{\psi^i} \psi^i = 1,$$

всегда можно записать в виде $e^{i\alpha}$ для некоторого угла $\alpha \in [0, 2\pi)$. Следовательно, существуют комплексные фазы $\alpha_1, \dots, \alpha_D$ такие, что

$$\begin{pmatrix} \psi^0 \\ \vdots \\ \psi^{D-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{D}} e^{i\alpha_0} \\ \vdots \\ \frac{1}{\sqrt{D}} e^{i\alpha_{D-1}} \end{pmatrix}. \tag{9.5}$$

То есть действительно несмещенных квантовых состояний много!

Появление коэффициентов $1/\sqrt{D}$ в правой части равенства (9.5) связано с наличием $1/D$ в равенстве (9.3), а это следует из нормировки квантового состояния $\widehat{\psi}$:

От этих чисел можно избавиться, если вместо того чтобы нормировать $\widehat{\psi}$, положить

Эти ненормированные несмещенные состояния $\widehat{\psi}$ будут играть столь важную роль в диаграммном языке, что мы дадим им специальное название.

Определение 9.4. *Фазовым состоянием* для \circ называется чистое состояние $\widehat{\psi}$, удовлетворяющее условиям:

Для фазовых состояний равенство (9.5) заменяется таким:

$$\begin{pmatrix} \psi^0 \\ \vdots \\ \psi^{D-1} \end{pmatrix} = \begin{pmatrix} e^{i\alpha_0} \\ \vdots \\ e^{i\alpha_{D-1}} \end{pmatrix} \tag{9.7}$$

Поскольку дублирование устраняет глобальные фазы (см. предложение 6.6), мы можем предположить без ограничения общности, что $\alpha_0 = 0$ (иначе просто умножим все состояние на $e^{-i\alpha_0}$). Следовательно, фазовое состояние $\vec{\psi}$ однозначно определяется списком остальных $D - 1$ комплексных фаз:

$$\vec{\alpha} := (\alpha_1, \dots, \alpha_{D-1}).$$

Поэтому, начиная с этого момента, будем обозначать фазовые состояния так:

$$\begin{array}{c} | \\ \circ \\ \vec{\alpha} \end{array} \quad (9.8)$$

Соглашение 9.5. Поскольку наша нотация для фаз инвариантна относительно горизонтального отражения, мы будем обозначать сопряжение знаком минус:

$$\begin{array}{c} | \\ \circ \\ \vec{\alpha} \end{array} \xrightarrow{(-)} \begin{array}{c} | \\ \circ \\ -\vec{\alpha} \end{array}$$

Транспонирование будет обозначаться так:

$$\begin{array}{c} \vec{\alpha} \\ \circ \\ | \end{array}$$

И значит, для адъюнкции применяется следующее обозначение:

$$\begin{array}{c} \vec{\alpha} \\ \circ \\ | \end{array}$$

В разделе 9.1.4 станет ясно, почему выбрана такая нотация.

Определяющее равенство (9.6) для фазовых состояний теперь принимает вид:

$$\begin{array}{c} | \\ \circ \\ \begin{array}{c} | \\ \circ \\ \vec{\alpha} \end{array} \end{array} = \begin{array}{c} | \\ \circ \end{array} \quad (9.9)$$

или эквивалентно:

$$\begin{array}{c} | \\ \circ \\ \begin{array}{cc} \circ & \circ \\ \vec{\alpha} & -\vec{\alpha} \end{array} \end{array} = \begin{array}{c} | \\ \circ \end{array} \quad (9.10)$$

В силу (9.9) данные фазы $\vec{\alpha}$ полностью уничтожаются, когда вступают в контакт с классическим миром посредством измерения. Таким образом:

фаза := данные, уничтожаемые при квантово-классическом переходе.

Если ОНБ-состояния представляют чисто классические данные, то фазовые состояния – противоположное понятие: они в высшей мере неклассические, или

«максимально квантовые». Это вполне согласуется с тем фактом, что несмещенные, а значит, и фазовые состояния не имеют сколько-нибудь осмысленного классического аналога (см. пример 9.3). Поэтому не должно вызывать удивления, что они играют важнейшую роль во многих квантовых особенностях, не имеющих классических аналогов. Мы еще разовьем тему существенной неклассичности фаз в следующем разделе.

Но прежде посмотрим, где находятся фазовые состояния на сфере Блоха. В случае, когда размерность $D = 2$, фазовое состояние зависит только от одной комплексной фазы α . В таком случае имеем:

$$\begin{array}{c} | \\ \circ \\ \bar{\alpha} \end{array} \leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix} \quad (9.11)$$

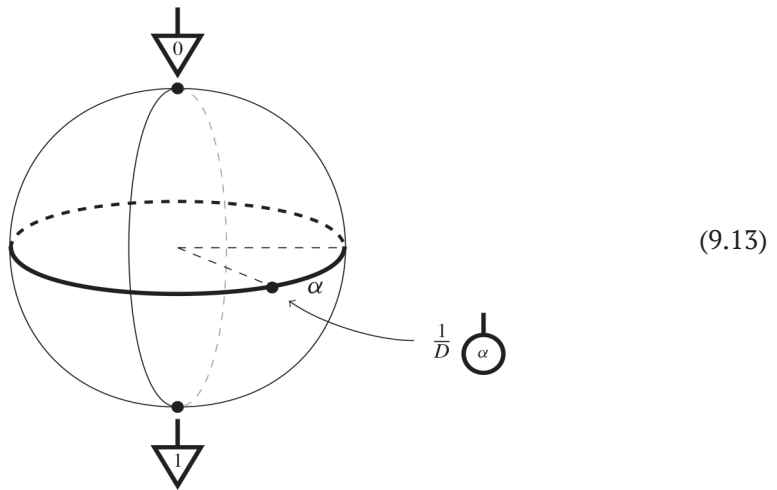
так что форма фазового состояния упрощается до

$$\begin{array}{c} | \\ \circ \\ \alpha \end{array} = \text{double} \left(\begin{array}{c} | \\ \nabla \\ 0 \end{array} + e^{i\alpha} \begin{array}{c} | \\ \nabla \\ 1 \end{array} \right) \quad (9.12)$$

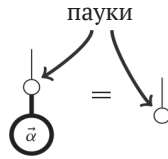
Напомним (см. раздел 6.1.2), что любое двумерное чистое состояние можно следующим образом записать в координатах на сфере Блоха:

$$\text{double} \left(\cos \frac{\theta}{2} \begin{array}{c} | \\ \nabla \\ 0 \end{array} + \sin \frac{\theta}{2} e^{i\alpha} \begin{array}{c} | \\ \nabla \\ 1 \end{array} \right)$$

Тогда состояния вида (9.12) – это в точности те, для которых $\theta = \pi/2$. Иными словами, они находятся на экваторе сферы Блоха:

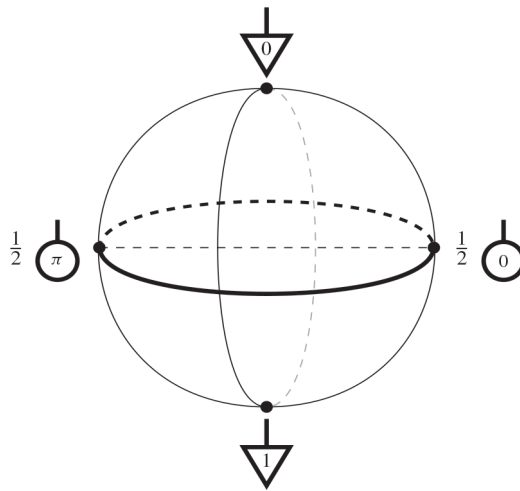


Замечание 9.6. В большинстве учебников по квантовой теории фазы вводятся геометрически. Но мы определили фазовые состояния, пользуясь только языком пауков и не прибегая к другим компонентам **линейных отображений**:



Таким образом, они являются неотъемлемой частью диаграммного языка. Отсюда в том числе следует, что они имеют смысл во многих других процессных теориях, и мы увидим это в разделе 11.2.2.

Пример 9.7. Сравнивая представление фазовых состояний на сфере Блоха с картинкой из упражнения 6.7, мы видим, что состояния, входящие в состав X -базиса, на самом деле являются фазами для \odot :



Отсюда имеем:

$$\begin{array}{c} \downarrow \\ 0 \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} | \\ \odot \\ 0 \end{array} \qquad \begin{array}{c} \downarrow \\ 1 \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} | \\ \odot \\ \pi \end{array}$$

Это можно рассматривать как первый признак нашествия пауков, которое будет продолжаться на всем протяжении этой главы.

Упражнение* 9.8. D -мерное обобщение этого ОНБ, состоящего из фаз, называется *базисом Фурье*:

$$\left\{ \frac{1}{\sqrt{D}} \begin{array}{c} | \\ \odot \\ \bar{\kappa}_j \end{array} \right\}_j, \quad \text{где} \quad \begin{array}{c} | \\ \odot \\ \bar{\kappa}_j \end{array} := \sum_k e^{\frac{2\pi i}{D} jk} \begin{array}{c} | \\ \nabla \\ k \end{array}$$

Докажите, что базис Фурье действительно является ОНБ. В вычислениях может помочь формула суммы геометрической прогрессии:

$$\sum_{k=0}^{D-1} r^k = \frac{r^D - 1}{r - 1}.$$

9.1.2. Фазовые пауки

Поскольку фазы – это «максимально квантовые» данные, то мы будем использовать их преимущественно для «украшения» квантовых пауков. Чтобы украсить квантового паука, мы просто подключим фазовое состояние к одной из его ног.

Определение 9.9. *Фазовым пауком* называется чистое квантовое отображение вида

$$\begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} := \begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} \quad (9.14)$$

Отметим, что в силу предложения 8.33 не имеет значения, какую ногу выбрать. И не важно, подключается ли фазовое состояние к входу или транспонированное фазовое состояние к выходу:

$$\begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} = \begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} = \begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array}$$

Отсюда сразу следует

Предложение 9.10. Результатом транспонирования фазового паука является фазовый паук с такой же фазой. В частности, если у фазового паука одинаковое количество входов и выходов, то он является самотранспонированным.

Воспользовавшись матричной формой фазового состояния:

$$\begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} = \text{double} \left(\sum_j e^{i\alpha_j} \begin{array}{c} \dots \\ \vdots \\ \nabla_j \\ \vdots \\ \dots \end{array} \right)$$

и обобщенным правилом копирования (8.38), получаем матричную форму паука:

$$\begin{array}{c} \dots \\ \vdots \\ \textcircled{\bar{\alpha}} \\ \vdots \\ \dots \end{array} = \text{double} \left(\sum_j e^{i\alpha_j} \begin{array}{c} \dots \\ \vdots \\ \nabla_j \dots \nabla_j \\ \vdots \\ \dots \end{array} \right)$$

Как и раньше, мы можем удалить глобальную фазу и считать, что $\alpha_0 = 0$. Поэтому в двумерном случае это равенство упрощается до:

$$\begin{array}{c} \dots \\ \vdots \\ \textcircled{\alpha} \\ \vdots \\ \dots \end{array} = \text{double} \left(\begin{array}{c} \dots \\ \vdots \\ \nabla_0 \dots \nabla_0 \\ \vdots \\ \dots \end{array} + e^{i\alpha} \begin{array}{c} \dots \\ \vdots \\ \nabla_1 \dots \nabla_1 \\ \vdots \\ \dots \end{array} \right)$$

Всякий раз как украшенный квантовый паук пытается вступить в контакт с классической областью, он теряет свои украшения:

Теорема 9.11. При измерении любой ноги фазового паука ее фаза исчезает:

$$\text{Spider with } \bar{\alpha} \text{ and dot} = \text{Spider with dot} \quad (9.15)$$

Доказательство. Применив слияние гибридных пауков, получаем:

$$\text{Spider with } \bar{\alpha} \text{ and dot} \stackrel{(9.14)}{=} \text{Spider with } \bar{\alpha} \text{ and dot} = \text{Spider with } \bar{\alpha} \text{ and dot} \stackrel{(9.9)}{=} \text{Spider with dot} = \text{Spider with dot} \quad \square$$

В разделе 8.3.2 мы показали, что декогеренция – спутник классичности в том смысле, что инвариантные относительно декогеренции входы и выходы ведут себя так же, как классические входы и выходы. Поэтому следует ожидать, что декогеренция также окажется довольно деструктивной.

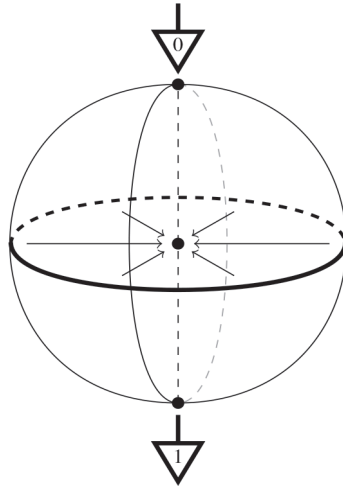
Следствие 9.12. Декогеренция стирает фазы:

$$\text{Spider with } \bar{\alpha} \text{ and dot} = \text{Spider with dot} \quad (9.16)$$

Само фазовое состояние – частный случай фазового паука, когда равенство (9.16) сводится к:

$$\text{Vertical line with dot and } \bar{\alpha} = \text{Vertical line with dot} = \text{Horizontal line with dot}$$

В разделе 8.3.2 мы показали, что изобразить декогеренцию в двумерной системе можно посредством проецирования на среднюю линию шара Блоха. Это дает геометрическую картину того, как декогеренция уничтожает фазы. Все фазовые состояния на экваторе проецируются в центральное, т. е. максимально смешанное, состояние:



Упражнение 9.13. Докажите более общее утверждение – когда фазовый паук сливается с любым гибридным пауком, фаза исчезает:

(9.17)

9.1.3. Слияние фазовых пауков

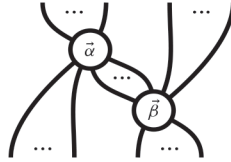
Итак, мы теперь знаем, что происходит, когда фазовый паук сливается с гибридным, но как насчет слияния двух фазовых пауков? Применяя правило слияния квантовых пауков, получаем:

Правая часть снова является фазовым пауком.

Лемма 9.14. Пусть $\vec{\alpha}$ и $\vec{\beta}$ – фазы. Тогда

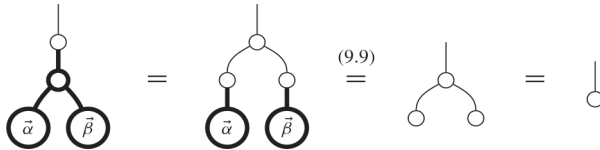
(9.18)

– фазовое состояние, и потому



– фазовый паук.

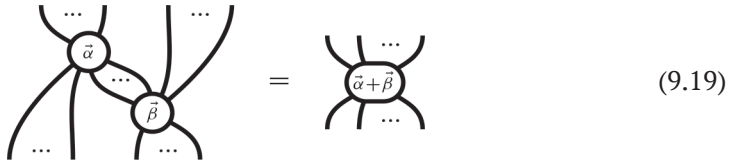
Доказательство. Применив правило слияния гибридных пауков, получаем:



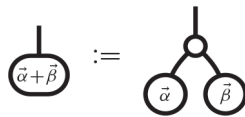
Поэтому для состояния (9.18) действительно имеет место равенство (9.9). \square

Введя новую нотацию для этой комбинированной фазы, получаем следующую теорему.

Теорема 9.15. Фазовые пауки сливаются следующим образом:



где использовано сокращение



Очевидно, что порядок $\vec{\alpha}$ и $\vec{\beta}$ не имеет значения:



и мы можем обобщить эту нотацию на n фаз, получив тем самым «украшенный» вариант следствия 8.35.

Следствие 9.16. Любая связная диаграмма, состоящая только из фазовых пауков, сама является фазовым пауком, фаза которого равна сумме фаз составляющих пауков:

$$\begin{array}{c} \text{Spider with 5 legs } \tilde{\alpha}_1, \dots, \tilde{\alpha}_5 \end{array} = \begin{array}{c} \text{Spider with 1 leg } \sum \tilde{\alpha}_i \end{array} \quad (9.20)$$

где мы использовали сокращение

$$\begin{array}{c} \text{Spider with 1 leg } \sum \tilde{\alpha}_i \end{array} := \begin{array}{c} \text{Spider with } n \text{ legs } \tilde{\alpha}_1, \dots, \tilde{\alpha}_n \end{array}$$

Так почему же мы решили записывать это «фазосмешение» в виде суммы? Давайте посмотрим, что происходит с базовыми линейными отображениями. Прежде всего заметим, что при умножении двух комплексных фаз углы складываются:

$$e^{i\alpha} e^{i\beta} = e^{i(\alpha+\beta)}.$$

Затем, выразив (9.18) в виде произведения Адамара (8.32), получаем:

$$\begin{array}{c} \text{Spider with 2 legs } \tilde{\alpha}, \tilde{\beta} \end{array} \Leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha_1} e^{i\beta_1} \\ \vdots \\ e^{i\alpha_{D-1}} e^{i\beta_{D-1}} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i(\alpha_1+\beta_1)} \\ \vdots \\ e^{i(\alpha_{D-1}+\beta_{D-1})} \end{pmatrix}$$

Поэтому результирующая фаза действительно является поэлементной суммой двух исходных фаз:

$$\vec{\alpha} + \vec{\beta} := (\alpha_1 + \beta_1, \dots, \alpha_{D-1} + \beta_{D-1}).$$

В двумерном случае эту формулу можно упростить:

$$\begin{array}{c} \text{Spider with 2 legs } \alpha, \beta \end{array} \Leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha} e^{i\beta} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i(\alpha+\beta)} \end{pmatrix} \Leftrightarrow \begin{array}{c} \text{Spider with 1 leg } \alpha + \beta \end{array}$$

И в заключение этого раздела приведем аналог следствия 8.35.

Следствие 9.17. Если диаграмма, получающаяся в результате композиции фазовых пауков, связана, то она зависит только от:

- количества входов и выходов;
- полной суммы фаз.

9.1.4. Фазовая группа

В предыдущем разделе мы видели, что пауков можно использовать для определения «суммы» фазовых состояний. В этом разделе мы увидим, что множество фазовых состояний образует *коммутативную группу*. Вы наверняка встречали такие группы в алгебре, но на всякий случай напомним.

Определение 9.18. *Коммутативной группой* называется множество A , наделенное:

- групповой операцией *сложения*, которая возвращает сумму $a + b \in A$ для любых двух элементов $a, b \in A$;
- выделенным элементом $0 \in A$, называемым *единицей*;
- операцией *обращения*, которая возвращает элемент $-a \in A$ для любого элемента $a \in A$.

При этом для любых $a, b, c \in A$ выполняются следующие свойства:

$$a + (b + c) = (a + b) + c, \quad a + b = b + a, \quad a + 0 = a, \quad -a + a = 0.$$

Эти свойства обычно называют *ассоциативностью*, *коммутативностью*, *унитальностью* и *правилом обращения*.

Рассматривая фазовые состояния как элементы группы:

$$\begin{array}{c} | \\ \circ \\ \bar{\alpha} \end{array} \leftrightarrow a$$

мы уже нашли кандидата на роль операции сложения:

$$\begin{array}{c} | \\ \circ \\ \diagup \quad \diagdown \end{array} \leftrightarrow + \qquad \begin{array}{c} | \\ \circ \\ \circ \quad \circ \\ \bar{\alpha} \quad \bar{\beta} \end{array} \leftrightarrow a + b$$

Осталось только найти единицу и определить обратный элемент.

Лемма 9.19. Пусть $\bar{\alpha}$ – фаза. Тогда

$$\begin{array}{c} | \\ \circ \end{array} \qquad \begin{array}{c} | \\ \circ \\ \bar{-\alpha} \end{array}$$

являются фазовыми состояниями.

Доказательство. Применение правила слияния пауков дает:

$$\begin{array}{c} | \\ \circ \\ \circ \end{array} = \begin{array}{c} | \\ \circ \\ \circ \quad \circ \end{array} = \begin{array}{c} | \\ \circ \end{array}$$

Поэтому условие (9.9) удовлетворяется. Чтобы показать, что сопряженное фазовое состояние снова является фазовым состоянием, применим операцию сопряжения к обеим частям (9.9):

$$\begin{array}{c} \text{---} \\ | \\ \bigcirc \\ / \quad \backslash \\ \bigcirc \quad \bigcirc \\ \bar{-\alpha} \quad \bar{\alpha} \\ \underbrace{\hspace{10em}} \\ -\bar{\alpha} + \bar{\alpha} \end{array} = \underbrace{\begin{array}{c} \text{---} \\ | \\ \bigcirc \\ \underbrace{\hspace{1em}} \\ \bar{0} \end{array}} \tag{9.21}$$

что и завершает доказательство. □

Таким образом, используя только правила слияния пауков и определение не-смещенности, мы показали, что фазовые состояния всегда образуют группу. В частности, мы нигде не упоминали явную форму фаз

$$\begin{array}{c} \text{---} \\ | \\ \bigcirc \\ \bar{\alpha} \end{array} := \text{double} \left(\sum_j e^{i\alpha_j} \begin{array}{c} \downarrow \\ j \end{array} \right)$$

Упражнение 9.21. Пользуясь свойствами комплексных чисел

$$e^{i0} = 1, \quad \overline{e^{i\alpha}} = e^{-i\alpha},$$

покажите, что $\bar{0}$ и $-\bar{\alpha}$ можно явно записать в виде:

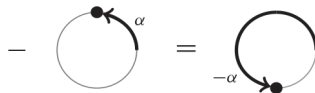
$$\bar{0} := (0, \dots, 0) \quad \text{и} \quad -\bar{\alpha} := (-\alpha_1, \dots, -\alpha_{D-1})$$

соответственно.

В случае $D = 2$ мы можем представить фазу всего одним углом. Тогда элементы фазовой группы представляются углами $\alpha \in [0, 2\pi)$, а операция сложения сводится к сложению углов по модулю 2π :



Обратный элемент – это просто угол с противоположным знаком:



По очевидным причинам, эту группу иногда называют *группой круга*. В другой терминологии ее также называют группой $U(1)$, потому что фазы – то же самое, что унитарные матрицы размера 1×1 :

$$e^{i\alpha} \leftrightarrow (e^{i\alpha}).$$

Для более высокой размерности мы просто получаем больше экземпляров $U(1)$, т. е. фазовая группа всегда имеет вид:

$$\underbrace{U(1) \times \dots \times U(1)}_{D-1} .$$

9.1.5. Фазовые вентили

Мы уже рассмотрели один важный пример фазовых пауков – фазовые состояния. Теперь изучим другой пример, который будет играть важную роль в оставшейся части книги.

Определение 9.22. *Фазовым вентиляем* называется квантовый процесс вида:

$$\begin{array}{c} \circ \\ | \\ \text{---} \alpha \end{array} := \begin{array}{c} \circ \\ | \\ \text{---} \circ \\ \quad \backslash \\ \quad \quad \circ \end{array} \quad (9.22)$$

Как и для любых фазовых пауков, адъюнкция (или, эквивалентно, сопряжение) фазового вентиля меняет знак фазы на минус:

$$\begin{array}{c} \circ \\ | \\ \text{---} \alpha \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \circ \\ \quad \backslash \\ \quad \quad \circ \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \alpha \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} \alpha \end{array}$$

Как следствие получаем следующее

Предложение 9.23. Фазовые вентили унитарны.

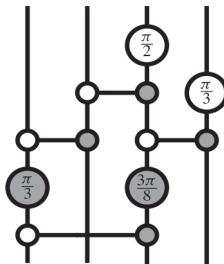
Доказательство. Применяя слияние пауков, получаем:

$$\begin{array}{c} \circ \\ | \\ \text{---} \alpha \\ \circ \\ | \\ \text{---} \alpha \end{array} = \begin{array}{c} \circ \\ | \\ \text{---} 0 \end{array} = \begin{array}{c} \circ \\ | \end{array} = |$$

Композиция в другом порядке тоже дает тождественное отображение. □

Таким образом, фазовые вентили – главные примеры *квантовых вентиляей* (см. раздел 5.3.4 и пример 6.13).

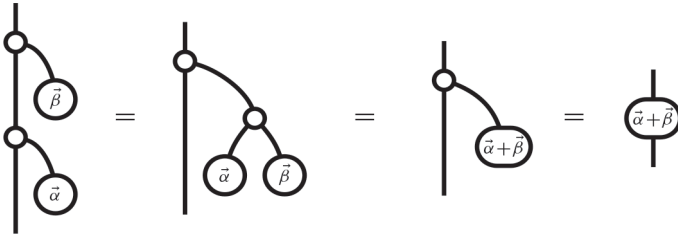
Пример 9.24. Возвращаясь к тому месту, на котором мы остановились в примере 6.13, можно сказать, что фазовые вентили позволяют записывать квантовые схемы, не имеющие классических аналогов:



Множество квантовых вентиляей *универсально*, т. е. любой унитарный процесс можно получить как квантовую схему, содержащую только вентили из этого мно-

жества. А в разделе 12.1.3 мы покажем, что универсальным является множество, состоящее лишь из квантового вентиля CNOT и классических вентилях. Следовательно, фазовые вентили играют центральную роль в квантовых вычислениях.

Поскольку фазовые вентили – частный случай фазовых пауков, групповая структура, описанная в предыдущих разделах, переносится и на фазовые вентили, например:



Следствие 9.25. Для любого семейства пауков \mathcal{O} множество фазовых вентилях



образует коммутативную группу, в которой:

- операция сложения определена как



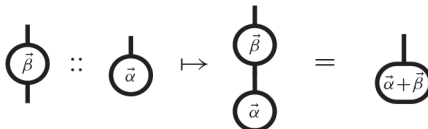
- единица определена как



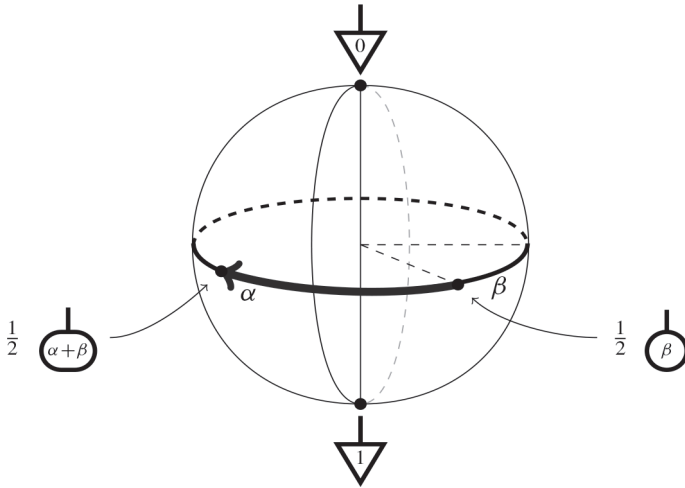
- обратный элемент определен как



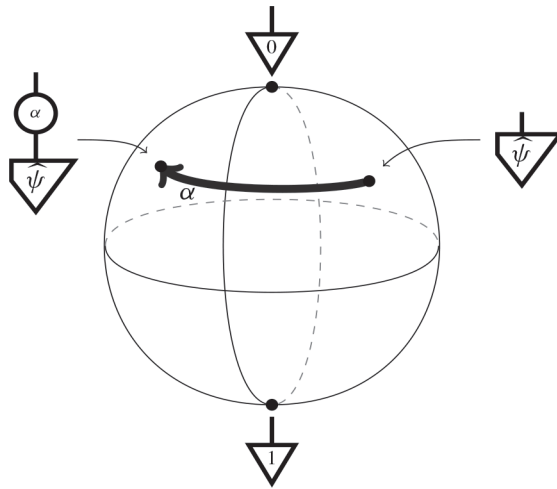
Так что же все-таки делают эти фазовые вентили? Это можно выяснить, посмотрев, как они воздействуют на фазовые состояния:



Как видим, фазовый вентиль с фазой $\vec{\beta}$ переводит фазовое состояние с фазой $\vec{\alpha}$ в другое фазовое состояние с фазой $\vec{\alpha} + \vec{\beta}$. В двумерном случае это соответствует повороту сферы Блоха вокруг оси, определяемой двумя базисными состояниями:



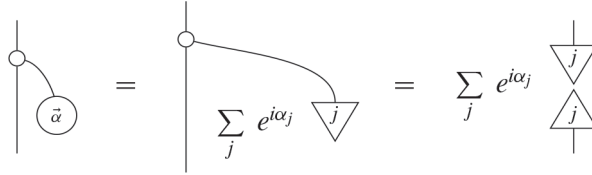
Поскольку фазовые вентиля унитарны, а унитарные отображения соответствуют поворотам сферы Блоха (см. предложение 7.2), отсюда сразу следует, что фазовые вентиля поворачивают все состояния вокруг оси Z:



Неудивительно, что матрицы фазовых вентиляей тесно связаны с матрицами ассоциированных с ними фазовых состояний. Для

$$\begin{array}{|c} \vec{\alpha} \\ \hline \end{array} := \sum_j e^{i\alpha_j} \begin{array}{|c} j \\ \hline \end{array}$$

(где мы положили $\alpha_0 := 0$) получаем:



Следовательно, для фазового состояния

$$\bar{\alpha} \leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha_1} \\ \vdots \\ e^{i\alpha_{D-1}} \end{pmatrix}$$

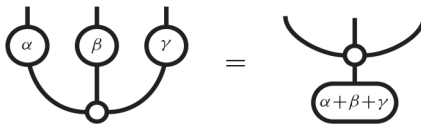
матрица ассоциированного фазового вентиля равна:

$$\bar{\alpha} \leftrightarrow \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & e^{i\alpha_1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\alpha_{D-1}} \end{pmatrix}$$

Для $D = 2$ матрица фазового отображения имеет вид:

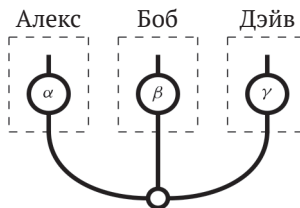
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

Пример 9.26. В примере 8.70 мы уже встречали трехсистемное ГХЦ-состояние. Если применить фазовый вентиль к каждой системе, то получим:



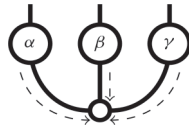
На первый взгляд, это вполне невинное приложение слияния фазовых пауков, но его физическая интерпретация прямо-таки шокирует!

Предположим, что три стороны, выполняющие три фазовых вентиля:

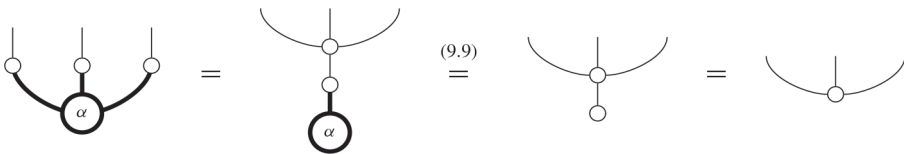


находятся так далеко друг от друга, что даже свету требуется много времени для путешествия между ними.

Хотя углы α , β и γ выбраны независимо и в очень отдаленных точках, результирующее состояние зависит только от суммы всех трех фаз. Например, если бы мы переставили эти фазы местами, то результирующее состояние никак не изменилось бы. Это говорит о том, что процессы взаимодействуют на очень большом расстоянии. Диаграмма буквально показывает, что ситуация выглядит так, будто все три фазы движутся назад во времени, чтобы встретиться друг с другом.



и, в отличие от обсуждения в разделе 4.4.3, где участвовали (некаузальные) крышки, в данном случае все процессы каузальные. Конечно, все это происходит на уровне квантового состояния, и наивное измерение уничтожит фазы, отсюда и вся магия:

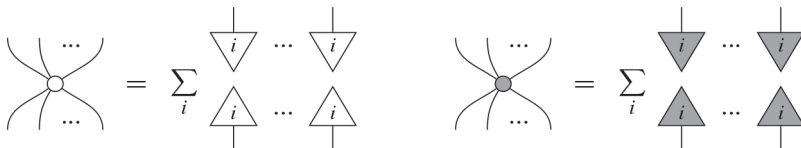


Ниже, в разделе 9.3.3, мы еще раз вернемся к этой истории и покажем, что при другом выборе измерений магия не пропадает.

9.2. Многоцветные пауки

Пауки одного и того же вида благополучно спариваются и смешивают свои фазы. Однако в земле пауков не везде царит мир и благодать. Сейчас мы введем пауков другого вида и продемонстрируем, какая бойня начинается при столкновении видов.

Как и в разделе 5.3.5, мы будем представлять два разных ОНБ, а теперь и ассоциированных с ними пауков разными цветами:



Это позволит рассматривать операции измерения и кодирования в двух разных базисах и, частности, изучать, как эти операции взаимодействуют.

9.2.1. Дополнительные пауки

Концепция фазового состояния (или несмещенности) имеет очень четкую интерпретацию как «квантовость в чистом виде» и приводит к появлению диаграммных созданий, именуемых фазовыми пауками. Простое диаграммное правило,

касающиеся взаимодействия пауков разных цветов, дает родственную и, пожалуй, еще более важную концепцию.

Определение 9.27. Пауки \circ и \bullet называются *дополнительными*, если

$$\begin{array}{c} | \\ \bullet \\ | \\ \circ \\ | \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \\ | \\ \circ \\ | \end{array} \quad (9.23)$$

или эквивалентно:

$$\begin{array}{c} | \\ \circ \\ | \\ \bullet \\ | \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \\ | \\ \circ \\ | \end{array} \quad (9.24)$$

И что же это означает? В левой части (9.23) мы кодируем классические данные в белом базисе, а затем измеряем в сером. Тогда (9.23) говорит, что это эквивалентно простому удалению классического входа:



и выводу равномерного распределения вероятностей:



Таким образом, классические данные на входе исчезают и заменяются случайными. В итоге:

$(\text{кодирование в } \circ) \text{ ЗАТЕМ (измерение в } \bullet) = (\text{нет потока данных}). \quad (9.25)$

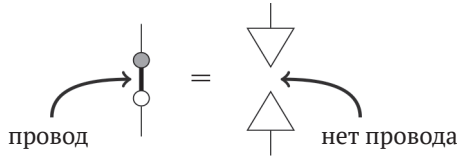
Замечание 9.28. Отметим, что равномерное распределение вероятностей, получающееся в результате \bullet -измерения, представлено в виде \bullet -паука. Мы еще вернемся к этому вопросу в разделе 9.2.4.

Условие (9.25) означает, что белый базис – очень плохой способ кодировать классические данные относительно серого измерения. Например, если закодировать классическое значение i как i -е состояние белого ОНБ квантовой системы и измерить его белым же измерением, то мы гарантированно получим исход i . С другой стороны, если измерить его серым измерением, то мы с одинаковой вероятностью можем получить любой исход, т. е. не будем иметь никакой информации о закодированном значении. По-другому ту же мысль можно выразить, сказав, что если мы имеем максимальную информацию о системе в одном базисе (т. е. она находится в чистом ОНБ-состоянии), то не имеем никакой информации о ней в другом базисе.

Пример* 9.29. Хорошо известно проявление этого феномена в квантовой механике: если положение квантовой системы известно точно, то о ее импульсе нельзя сказать ничего. Обычно положение рассматривается как непрерывная величина, что вынуждает переходить к бесконечномерным системам. Однако фундамен-

тальный принцип, сформулированный для дискретной версии дополнителности, сохраняется и в этом случае.

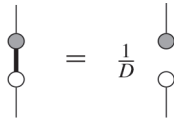
Хотя равенство (9.23) потребовало произвести разделение на конкретные эффект и состояние, а именно (белое) удаление, сопровождаемое (серым) равномерным распределением вероятностей, фактически достаточно сказать, что левая часть просто разделяется:



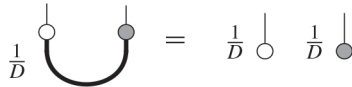
Таким образом, (9.25) можно принять в качестве основной формулировки принципа дополнителности. Но можно привести еще несколько вариаций на эту тему.

Предложение 9.30. Следующие утверждения для \circ и \bullet эквивалентны:

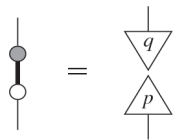
i) дополнителность:



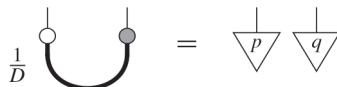
ii) дополнительные измерения состояния Белла дают равномерное распределение вероятностей для двух классических систем:



iii) существование эффекта p и состояния q таких, что:



iv) существование состояний p и q таких, что:



Доказательство. Эквивалентность (i) и (ii) тривиальна, как и эквивалентность (iii) и (iv), а поскольку из (i) следует (iii), остается только показать, что из (iii) следует (i). Сначала мы можем показать, что q совпадает с \bullet с точностью до некоторого числа λ :

и чуточка дополнителности:

$$(9.23) \quad \text{Diagram} = \frac{1}{D}$$

и еще капелка слияния пауков:

$$\frac{1}{D} \quad \text{Diagram} = \frac{1}{D} \quad \text{Diagram}$$

□

Вторая личина дополнителности предназначена для классических пауков. Здесь мы рассматриваем ● как классические отображения для ○ или наоборот (см. раздел 9.3.5 ниже).

Предложение 9.32. Для дополнителных ○ и ● имеем:

$$(9.28) \quad \text{Diagram} = \frac{1}{D} \quad \text{Diagram}$$

Доказательство почти такое же, просто нужно заменить (9.23) на (9.24). Третья личина дополнителности не связана напрямую ни с измерениями, ни с классическими данными. Тем не менее она весьма полезна в квантовых протоколах и алгоритмах. Это просто дублированная форма (9.28).

Предложение 9.33. Для дополнителных ○ и ● имеем:

$$(9.29) \quad \text{Diagram} = \frac{1}{D^2} \quad \text{Diagram}$$

Читая этот раздел, вы, наверное, обратили внимание на постоянно выскакивающие D . Что ж, у нас есть как плохие, так и хорошие новости. Плохая новость в том, что это практически неизбежно. Если мы перенормируем пауков, так чтобы избавиться от этих чисел, то правило слияния будет выглядеть просто кошмарно.

Упражнение* 9.34. Как будет выглядеть правило слияния пауков, если перенормировать пауков, так чтобы имело место равенство

$$\text{Diagram} = \text{Skull} \quad \text{Diagram}$$

Ну а хорошая новость состоит в том (см. раздел 3.4.3), что эти числа в общем-то можно игнорировать. Поэтому уравнение дополнительности можно переписать в таком виде:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \end{array} \tag{9.30}$$

а производные правила «разъединения» пауков принимают вид:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \approx \begin{array}{c} \dots \\ \diagup \\ \circ \\ \diagdown \\ \dots \end{array} \begin{array}{c} \dots \\ \diagdown \\ \bullet \\ \diagup \\ \dots \end{array} \tag{9.31}$$

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \approx \begin{array}{c} \dots \\ \diagup \\ \circ \\ \diagdown \\ \dots \end{array} \begin{array}{c} \dots \\ \diagdown \\ \bullet \\ \diagup \\ \dots \end{array} \tag{9.32}$$

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \quad \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \approx \begin{array}{c} \dots \\ \diagup \\ \bullet \\ \diagdown \\ \dots \end{array} \begin{array}{c} \dots \\ \diagdown \\ \circ \\ \diagup \\ \dots \end{array} \tag{9.33}$$

Лучше, не правда ли? К тому же проигнорированные числа можно восстановить.
Предложение 9.35. Для пауков \circ и \bullet имеем:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} \approx \begin{array}{c} \bullet \\ | \\ \circ \end{array} \implies \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

Доказательство. Предполагая, что

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \end{array} = \lambda \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

и выполнив композицию с кружочками на входе и на выходе, как при доказательстве предложения 9.30, получаем:

$$D = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \\ | \\ \circ \end{array} = \lambda \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \circ \\ | \\ \circ \end{array} = \lambda D^2$$

так что $\lambda = 1/D$.

□

называются *взаимно несмещенными*, если любое состояние одного ОНБ не смещено относительно другого ОНБ, т. е. для любых i, j имеет место равенство

$$\begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} = \frac{1}{D} \tag{9.37}$$

Замечание 9.39. Равенство (9.37), определяющее взаимно несмещенные ОНБ, можно записать и в дублированной форме, которая кому-то может показаться знакомой:

$$\left| \begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} \right| = \frac{1}{\sqrt{D}}$$

Теорема 9.40. Пауки \circ и \bullet являются дополнительными

$$\begin{array}{c} \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

тогда и только тогда, когда ассоциированные с ними ОНБ являются взаимно несмещенными:

$$\forall i, j : \begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} = \frac{1}{D} \tag{9.38}$$

Доказательство. Для дополнительных \circ и \bullet из (9.36) уже следует, что ассоциированные ОНБ взаимно несмещенные. Обратно, если два ОНБ взаимно несмещенные, то получаем:

$$\begin{array}{c} \triangleup_j \\ | \\ \bullet \\ | \\ \circ \\ | \\ \triangleleft_i \end{array} \stackrel{(8.6)}{=} \begin{array}{c} \triangleup_j \\ \downarrow \\ \triangleleft_i \end{array} \stackrel{(9.23)}{=} \frac{1}{D} \stackrel{(8.13)}{=} \frac{1}{D} \begin{array}{c} \triangleup_j \\ | \\ \bullet \\ | \\ \circ \\ | \\ \triangleleft_i \end{array}$$

Поэтому элементы матриц в левой и правой частях уравнения дополнительности (9.23) совпадают на этих базисах, а значит, уравнение удовлетворяется всюду.

Эта связь с взаимной несмещенностью дает еще целый ряд альтернативных характеристик дополнительности.

Следствие 9.41. Следующие утверждения эквивалентны для \circ и \bullet :

i) дополнительность:

$$\begin{array}{c} \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

ii) для всех i :

$$\begin{array}{c} | \\ \bullet \\ \nabla \\ i \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \end{array} \quad (9.39)$$

iii) для всех i существует такая фаза $\vec{\kappa}$, что:

$$\begin{array}{c} | \\ \nabla \\ i \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \\ \kappa \end{array} \quad (9.40)$$

iv) для всех j :

$$\begin{array}{c} | \\ \circ \\ \nabla \\ j \end{array} = \frac{1}{D} \begin{array}{c} | \\ \circ \end{array} \quad (9.41)$$

v) для всех j существует такая фаза $\vec{\kappa}$, что:

$$\begin{array}{c} | \\ \nabla \\ j \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \\ \kappa \end{array} \quad (9.42)$$

v) взаимная несмещенность:

$$\forall i, j : \begin{array}{c} \triangle \\ j \\ | \\ \nabla \\ i \end{array} = \frac{1}{D}$$

Пример 9.42. У характеристики дополнителности в терминах взаимной несмещенности есть, среди прочего, одно преимущество: легко проверить, что пара ОНБ индуцирует дополнительных пауков. Например, Z -базис и X -базис, который, как мы видели ранее, можно выразить через Z -базис:

$$\begin{array}{c} | \\ \nabla \\ 0 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \nabla \\ 0 \end{array} + \begin{array}{c} | \\ \nabla \\ 1 \end{array} \right) \quad \begin{array}{c} | \\ \nabla \\ 1 \end{array} := \frac{1}{\sqrt{2}} \left(\begin{array}{c} | \\ \nabla \\ 0 \end{array} - \begin{array}{c} | \\ \nabla \\ 1 \end{array} \right)$$

действительно являются взаимно несмещенными:

$$\begin{array}{c} \triangle \\ j \\ | \\ \nabla \\ i \end{array} = \frac{1}{2}$$

Поэтому они индуцируют дополнительных пауков, а значит, мы вправе представить их с помощью дополнительных цветов:

$$\begin{array}{c} | \\ \circ \\ | \end{array} := \text{измерение } Z; \quad \begin{array}{c} | \\ \bullet \\ | \end{array} := \text{измерение } X.$$

Упражнение 9.43. Для установления эквивалентности в теореме 9.40 мы опирались на явное подключение белого и серого базисных состояний. А теперь докажете эквивалентность (i) и (ii) выше, подключая только состояния из одного базиса.

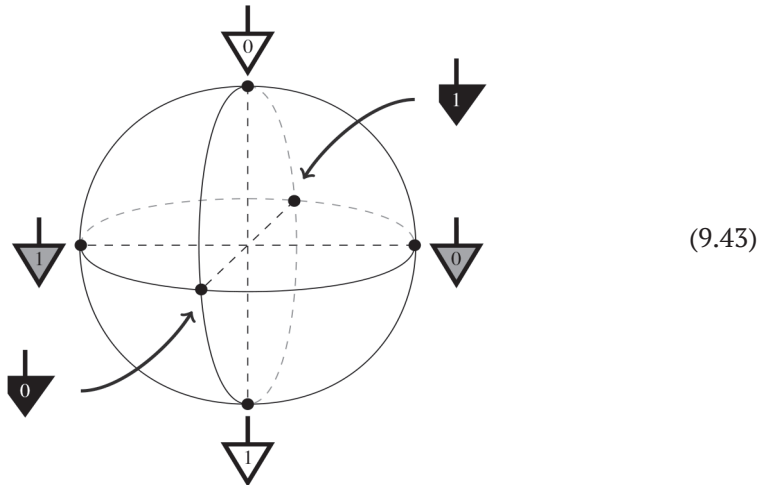
Пример 9.44. Множество ОНБ называется *попарно взаимно несмещенным*, если любая пара различных ОНБ из этого множества является взаимно несмещенной. С точностью до одного общего унитарного отображения существует три попарно взаимно несмещенных ОНБ для кубитов: *Z*-базис, *X*-базис и *Y*-базис:

$$\downarrow_0 := \frac{1}{\sqrt{2}} \left(\downarrow_0 + i \downarrow_1 \right) \quad \downarrow_1 := \frac{1}{\sqrt{2}} \left(\downarrow_0 - i \downarrow_1 \right)$$

Для любых i, j имеем:

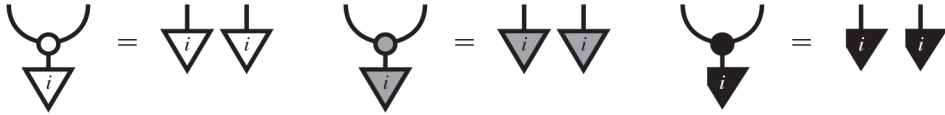
$$\begin{array}{c} \uparrow_j \\ \downarrow_i \end{array} = \begin{array}{c} \uparrow_j \\ \downarrow_i \end{array} = \begin{array}{c} \uparrow_j \\ \downarrow_i \end{array} = \frac{1}{2}$$

и потому эти ОНБ действительно попарно взаимно несмещенные. (Отметим, что хотя *Y*-базис не состоит из самосопряженных базисных состояний, наше определение взаимной несмещенности легко обобщается на этот случай.) На сфере Блоха они помечают три главные оси:



Множество попарно взаимно несмещенных базисов называется *максимальным*, если его нельзя расширить. Определение размера максимальных множеств для любой размерности – чрезвычайно трудная нерешенная задача, по сложности сравнимая с проблемой классификации SIC-POVM, упомянутой в разделе 7.4.2. В двумерном случае максимальные множества всегда имеют размер 3, как множество, показанное выше. Вообще, если $D = p^N$ для некоторого простого числа p , то размер максимального множества равен $p^N + 1$. Однако на момент написания этой книги для других размерностей, например $D = 6$, ответ оставался неизвестным.

На рисунке (9.43) мы изобразили базисные состояния некоторых очень важных измерений на сфере Блоха. В диаграммных терминах характеристическое свойство такого базисного состояния состоит в том, что оно копируется соответствующими пауками:



Поскольку эти базисные состояния удовлетворяют нескольким условиям взаимной несмещенности, то в силу следствия 9.41 мы знаем также, что каждое из них является фазовым состоянием для своих дополнительных пауков, что дает еще несколько полезных равенств. Разберемся, что представляют собой эти фазы для всех шести состояний.

В примере 9.7 мы видели, что

$$\begin{matrix} \downarrow \\ 0 \end{matrix} = \frac{1}{2} \begin{matrix} \circ \\ 0 \end{matrix} \qquad \begin{matrix} \downarrow \\ 1 \end{matrix} = \frac{1}{2} \begin{matrix} \circ \\ \pi \end{matrix} \qquad (9.44)$$

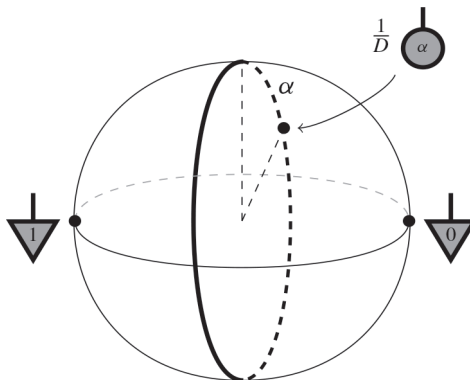
а сравнивая (9.43) с (9.13), получаем также:

$$\begin{matrix} \blacktriangledown \\ 0 \end{matrix} = \frac{1}{2} \begin{matrix} \circ \\ \frac{\pi}{2} \end{matrix} \qquad \begin{matrix} \blacktriangledown \\ 1 \end{matrix} = \frac{1}{2} \begin{matrix} \circ \\ -\frac{\pi}{2} \end{matrix} \qquad (9.45)$$

Конечно, мы можем сделать нечто подобное в терминах X-фазовых состояний, которые, согласно равенству (9.12), в матричной форме имеют вид:

$$\begin{matrix} \circ \\ \alpha \end{matrix} = \text{double} \left(\begin{matrix} \downarrow \\ 0 \end{matrix} + e^{i\alpha} \begin{matrix} \downarrow \\ 1 \end{matrix} \right)$$

Эти серые фазовые состояния лежат на экваторе в плоскости, перпендикулярной оси, проходящей через дублированные серые базисные состояния:

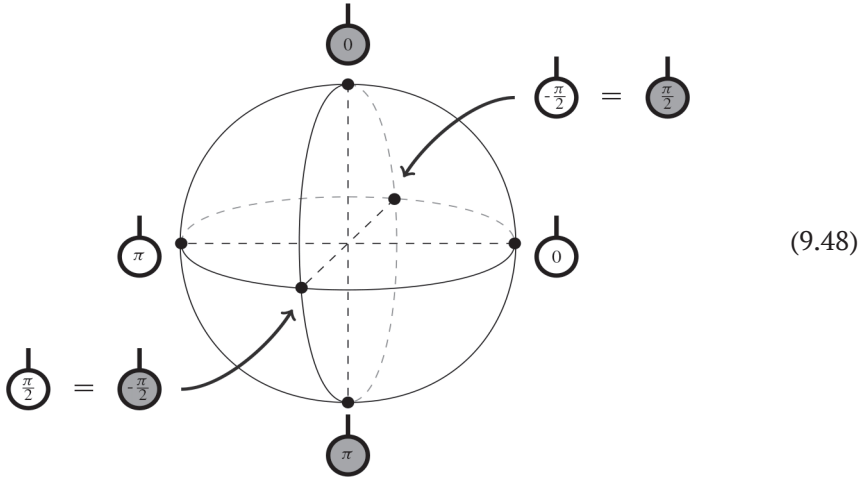


и сравнение с (9.43) дает:

$$\begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ 0 \end{array} \qquad \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ \pi \end{array} \qquad (9.46)$$

$$\begin{array}{c} \downarrow \\ \blacktriangledown \\ 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ -\frac{\pi}{2} \end{array} \qquad \begin{array}{c} \downarrow \\ \blacktriangledown \\ 1 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ \frac{\pi}{2} \end{array} \qquad (9.47)$$

То же самое можно было бы сделать для \bullet , но мы остановимся на этом, поскольку ниже увидим, что для наших целей достаточно пар дополнительных пауков (см. теорему 9.66). Подводя итог всему вышесказанному, мы изобразим фазовые состояния, представляющие базисные состояния (с точностью до множителя $\frac{1}{2}$), на сфере Блоха:



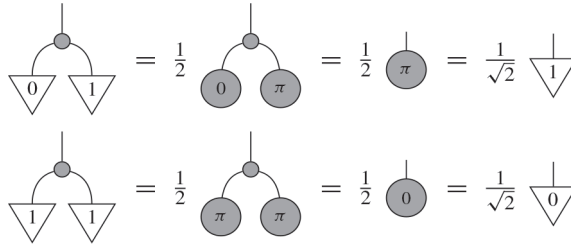
Пример 9.45. В разделе 5.3.5 мы заметили, что адьюнкт отображения X-копирования ведет себя как операция XOR в Z-базисе, точнее:

$$\begin{array}{c} \circ \\ \curvearrowright \end{array} = \frac{1}{\sqrt{2}} \begin{array}{|c|} \hline \text{XOR} \\ \hline \end{array}$$

Теперь этот факт можно проверить, воспользовавшись слиянием фазовых пауков:

$$\begin{array}{c} \circ \\ \curvearrowright \\ \triangle \quad \triangle \\ 0 \quad 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ \curvearrowright \\ \circ \quad \circ \\ 0 \quad 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ 0 \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \triangle \\ 0 \end{array}$$

$$\begin{array}{c} \circ \\ \curvearrowright \\ \triangle \quad \triangle \\ 1 \quad 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ \curvearrowright \\ \circ \quad \circ \\ \pi \quad 0 \end{array} = \frac{1}{2} \begin{array}{c} \circ \\ \pi \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \triangle \\ 1 \end{array}$$



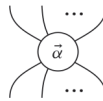
9.2.3. От дополнителности к вентилю CNOT

В предыдущих главах мы предполагали существование «черных ящиков», обладающих полезными свойствами (например, измерения и управляемые унитарные процессы). Теперь, когда в нашем распоряжении имеются разнообразные пауки:

- классические, квантовые и гибридные пауки:



- фазовые пауки:



- дополнительные пауки:



мы можем приступить к конструированию подобных объектов. Для начала покажем, что пара дополнительных пауков всегда индуцирует унитарное квантовое отображение. В случае дополнительной пары Z и X из примера 9.42 это унитарное отображение является вентиляем CNOT, с которым мы познакомились в разделе 5.3.4:

$$\begin{array}{c}
 \begin{array}{|c|} \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline 0 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline 0 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline 0 \\ \hline \end{array} + \begin{array}{|c|} \hline 1 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline \end{array}
 \end{array} \tag{9.49}$$

Нотация, которой мы пользовались для обозначения вентиля CNOT:



содержит белый и серый кружочки, что ясно указывает в направлении двух семейств пауков. Но что означает горизонтальная линия?

Лемма 9.46.

$$\begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} \quad (9.50)$$

Доказательство опирается на тот факт, что

$$\begin{array}{c} \circ \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \circ \end{array} = \begin{array}{c} \bullet \\ \text{---} \end{array}$$

Сначала докажем первое из равенств (9.50):

$$\begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array} = \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array}$$

Доведение доказательства до конца оставляем в качестве упражнения. □

Упражнение 9.47. Закончите доказательство леммы 9.46.

Итак, поскольку способ перехода от белого кружочка к серому с помощью провода не играет роли, мы можем изображать его просто горизонтальной прямой. Отсюда непосредственно вытекает

Лемма 9.48. Для пауков \circ и \bullet отображение



всегда является самоадьюнктным.

И мы действительно восстанавливаем вентиль CNOT, по крайней мере с точностью до числа.

Упражнение 9.49. Покажите, что если в качестве \circ и \bullet выбрать пауков для Z-базиса и X-базиса, как в примере 9.42, то

$$\sqrt{2} \begin{array}{c} \circ \quad \bullet \\ \text{---} \end{array}$$

не является вентилем CNOT (9.49).

Тот факт, что \circ и \bullet индуцируют унитарное отображение, дает нам еще один набор характеристик дополнителности.

Предложение 9.50. Следующие утверждения эквивалентны для \circ и \bullet :

i) пауки являются дополнительными:

$$\begin{array}{c} \bullet \\ \text{---} \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ \text{---} \\ \circ \end{array}$$

ii) следующее линейное отображение унитарно:

$$\sqrt{D} \begin{array}{c} \circ \\ | \\ \circ \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \quad (9.51)$$

iii) следующее квантовое отображение унитарно:

$$D \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \quad (9.52)$$

Доказательство. Сначала покажем, что из (i) следует (ii). Поскольку отображение (9.51) самоадьюнктное, достаточно показать, что его композиция с самим собой – тождественное отображение:

$$\begin{array}{c} \sqrt{D} \\ \circ \\ | \\ \sqrt{D} \\ \circ \end{array} \begin{array}{c} | \\ \bullet \\ | \\ \bullet \\ | \end{array} = D \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} \stackrel{(9.28)}{=} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \begin{array}{c} | \\ | \\ | \end{array}$$

Импликация (ii) ⇒ (iii) получается путем дублирования условий унитарности. Обратнo, если отображение (9.52) унитарно, то (9.51) является унитарным в силу теоремы 6.20. Таким образом, достаточно показать, что из (ii) следует (i):

$$\begin{array}{c} \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \circ \\ | \\ \sqrt{D} \\ \circ \\ | \\ \sqrt{D} \\ \circ \\ | \\ \bullet \end{array} = \frac{1}{D} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \bullet \\ | \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

где первый шаг – это просто правило слияния пауков (плюс жонглирование числами), а на втором использована унитарность отображения (9.51). □

Упражнение 9.51. Дайте альтернативное доказательство того, что (i) влечет (iii), показав сначала каузальность (iii).

Замечание 9.52. В разделе 12.2 мы увидим, что дополнителность эквивалентна унитарности отображения

$$\begin{array}{c} | \\ \hline \widehat{U}_f \\ \hline | \end{array} := D \begin{array}{c} | \\ \bullet \\ | \end{array} \begin{array}{c} | \\ \circ \\ | \end{array} \begin{array}{c} | \\ \widehat{f} \\ | \end{array}$$

для любого (дублированного) функционального отображения f (см. определение 8.13). Тогда предложение 9.50 становится просто частным случаем, когда f – тождественное отображение. Хотя \widehat{f} может и не быть каузальным (а стало быть, квантовым процессом), \widehat{U}_f всегда является квантовым процессом. Такой унитар-

ный квантовый процесс \hat{U}_f называется *квантовым оракулом* и входит важнейшей составной частью во многие квантовые алгоритмы.

9.2.4. «Цвета» классических данных

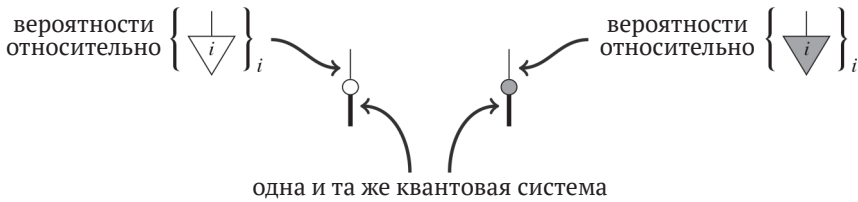
Внимательный читатель, вероятно, обратил внимание, что мы упустили из виду важный момент, касающийся многоцветных пауков и классических проводов. Рассмотрим матричную форму процессов измерения для двух разных пауков:



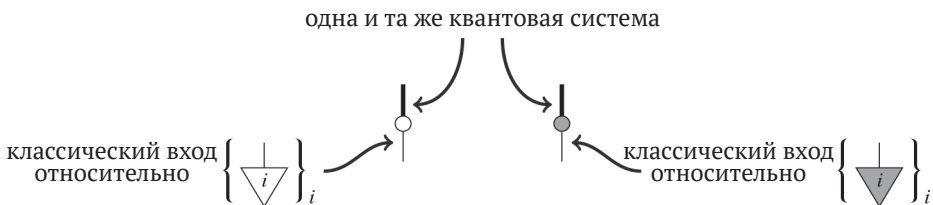
Понятно, что оба измерения порождают классические состояния, но эти состояния выглядят не совсем одинаковыми:



То есть классические состояния кодируются в разных ОНБ. Это не ошибка, так и должно быть. Числа, составляющие распределение вероятностей, – абсолютно бесполезная информация, если мы не знаем, вероятностями чего они являются. В двух классических состояниях выше ОНБ говорит, что такое числа p_i – это вероятности исходов конкретного измерения. Вообще, классический провод несет описание того, как получены классические данные, т. е. в результате какого измерения:



Аналогично для кодирования имеем:



Итог – классические провода несут дополнительную информацию о базисе, в котором закодированы классические данные. Эту информацию можно было бы сделать явной, например пометив провода следующим образом:

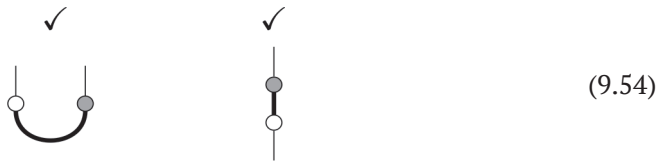


но на самом деле это необязательно, потому что тип всегда понятен из контекста. И самое главное – любой толстый провод, подключенный к гибриднему пауку, несет классические данные того же «цвета».

Как и для любых других системных типов, мы не разрешаем соединять провода разных типов:



С другой стороны, оба эти измерения применяются к квантовым системам одного и того же типа, поэтому, например, следующие композиции разрешены:



Из (9.53) мы можем извлечь золотое правило: гибридные пауки разного цвета никогда не должны соединяться классическими проводами. С другой стороны, иногда бывает, что классический паук одного цвета является допустимым классическим отображением для другого цвета. Мы уже встречали такой пример в предложении 5.88, где видели, что вентиль XOR в белом базисе является сопоставлением в сером базисе. В таком случае линейное отображение вида



могло бы быть допустимым КК-отображением. Однако отображение



нарушает золотое правило, поскольку теперь гибридные пауки соприкасаются с классическим проводом одного типа.

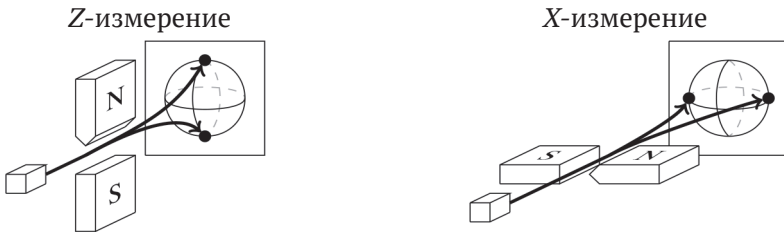
Замечание 9.53. Можно было бы вместо этого зафиксировать один базис для классических выходов и определить измерения ОНБ с помощью одного кружочка и унитарного отображения, как мы поступили в разделе 8.4.1:



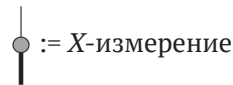
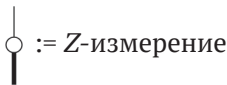
Однако, как мы уже видели в трех предшествующих разделах, представление классических данных в разных базисах существенно упрощает диаграммы и вычисления.

9.2.5. Дополнительные измерения

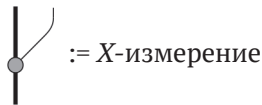
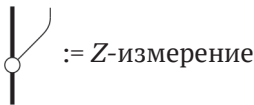
Теперь мы воспользуемся дополнительностью, чтобы продемонстрировать некоторые интересные квантовые особенности. Вернемся к прибору Штерна–Герлаха, который изучали в разделах 7.1.1 и 7.1.2. Напомним, что мы могли бы производить измерения в разных ОНБ, просто повернув весь прибор:




Из примера 9.42 мы также знаем, что Z - и X -измерения можно описать с помощью дополнительных пауков:

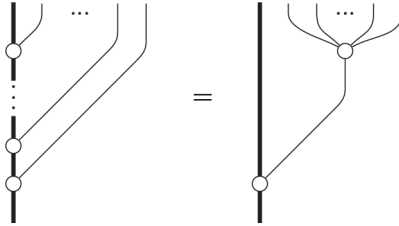


относительно Z - и X -базиса из примера 9.42. Если вместо того чтобы позволить частицам соударяться с экраном, мы разрешим им проходить дальше, то получим дополнительные невозможные измерения (см. раздел 8.4.1):

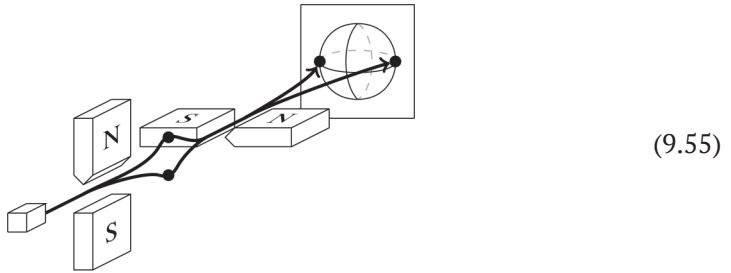


Если мы притворимся, что ничего не знаем о квантовых измерениях, то могло бы случиться так, что частицы, порожденные , имеют « Z -свойство», которое говорит, как они отклоняются при Z -измерении, и « X -свойство», которое сообщает об отклонении при X -измерении, и что вышеупомянутые операции соответ-

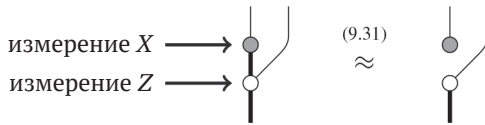
ствуют просто «наблюдению» этих свойств. Когда мы производим эти измерения изолированно, такая интерпретация кажется оправданной. Например, сколько бы раз мы ни «наблюдали Z -свойство», результат будет одинаковый:



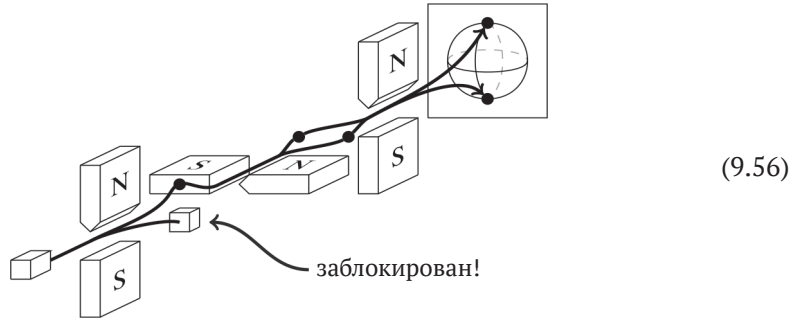
Но стоит нам начать комбинировать Z - и X -измерения, как эта идея об «измерении как наблюдении» разбивается вдребезги. Сначала предположим, что мы производим Z -измерение раньше X -измерения:



На диаграммах экспериментальная установка (9.55) принимает вид:

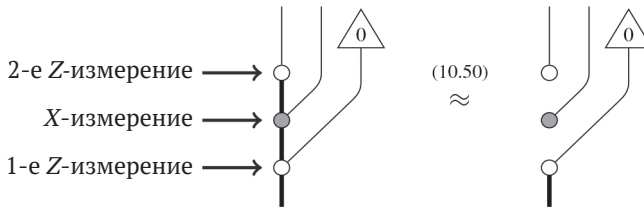


Это значит, что X -измерение всегда порождает равномерное распределение вероятностей вне зависимости от того, каково состояние на входе в прибор. Если бы мы просто наблюдали эти вероятности в лаборатории, не имея полного контроля над входными состояниями, то могли бы и не сообразить, насколько это странно. Быть может, наш источник частиц порождает частицы, для которых значение X в половине случаев равно 0, а в другой половине – 1. Однако мы определенно сможем убедиться в странности происходящего, если добавим третий прибор Штерна–Герлаха:



(9.56)

и заблокируем один из выходов первого Z -измерения. Предположим, что это выход, соответствующий исходу 1; частица соударяется с экраном, стоящим в конце, только если первое измерение дает 0. Мы можем ограничиться лишь сценариями, в которых первое измерение дает исход 0, следующим образом:



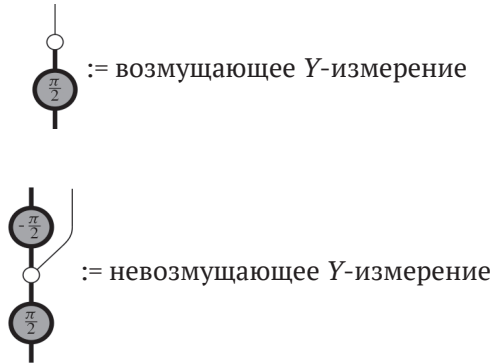
(10.50)

Даже если мы пропускаем только частицы, которые дают 0 в первом Z -измерении, то к моменту, когда Z будет измеряться во второй раз, мы получим не 0, а равномерное распределение вероятностей! Конечно, это происходит только благодаря измерению X посередине. Описанная установка – одна из самых знаменитых демонстраций того, что в квантовой теории измерения совершенно не похожи на простое «наблюдение» некоторого свойства системы. Тот факт, что одно измерение оказывает такое влияние на исходы другого измерения, называется *несовместимостью измерений*. Поскольку дополнительные измерения превращают исходы друг друга в белый шум, они *максимально несовместимы*.

Помимо желания продемонстрировать одно из самых поразительных физических проявлений «истинно квантовой» особенности принципа дополнительности, мы включили этот пример еще и для того, чтобы показать фантастическую эффективность диаграммных рассуждений с привлечением пауков! Каждый из приведенных выше аргументов потребовал только одного применения правила разъединения пауков.

Благодаря такой простоте мы легко можем рассматривать и другие подобные ситуации. Из примера 9.44 мы знаем, что и Y -измерения должны быть максимально несовместимы с X - и Z -измерениями, поэтому таким же способом можно будет вывести аналогичные результаты, касающиеся Y -измерений. Один из способов сделать это – ввести третий цвет, но даже это не обязательно. Достаточно добавить кое-какие украшения.

Аналогично Y -измерение можно представить с помощью X -фазовых вентиляей:



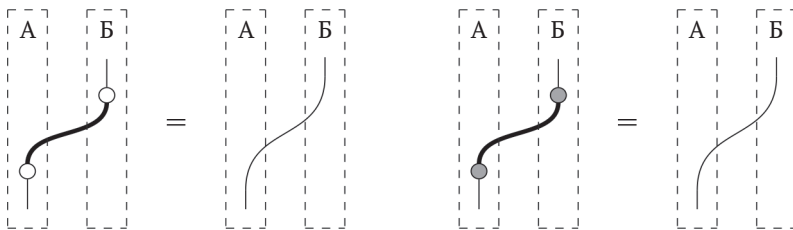
и те же результаты, можно, конечно, вывести и в этой альтернативной форме.

9.2.6. Квантовое распределение ключей

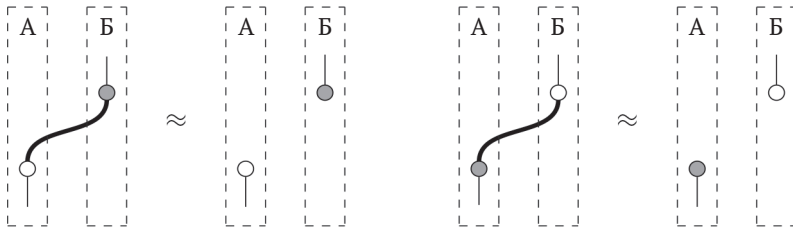
Очень близко к нашему анализу несовместимости, представленному в предыдущем разделе, примыкает квантовое распределение ключей (КРК). В частности, мы увидим, как можно использовать дополнительную пару измерений для выработки общего секрета (например, криптографического ключа), разделяемого Алексом и Бобом таким образом, что они всегда смогут выявить подслушивание (что и оправдывает термин «секрет»). Самый известный протокол КРК называется BB84. Собственно квантовая часть протокола очень проста. Для описания протокола мы будем использовать биты и кубиты, но он прекрасно работает при $D > 2$. Требуется только дополнительность.

Итак, у Алекса имеется набор случайных битов, которые он хочет передать Бобу. Ему не особенно важно, все ли биты дошли. Его вполне устроит, если дойдет достаточное количество битов, чтобы можно было выработать криптографический ключ, который затем будет использоваться для «настоящей» секретной связи с Бобом.

Для этого Алекс и Боб сначала фиксируют пару дополнительных пауков \circ и \bullet , и Алекс с одинаковой вероятностью выбирает, кодировать ли свои классические данные \circ -кодировщиком или \bullet -кодировщиком. Затем Боб с одинаковой вероятностью выбирает \circ -измеритель или \bullet -измеритель. Если оба решения согласованы, то Боб получает бит Алекса:

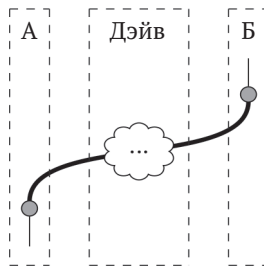


Если же решения не согласованы, то Боб получит шум, т. е. равномерное распределение:



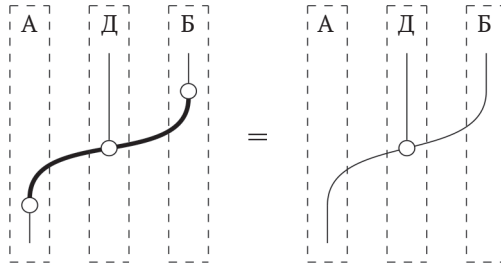
Они повторяют эту процедуру для всех битов, которые Алекс хочет передать Бобу, понимая, что в 50 % случаев Боб получает бит Алекса, а в остальных 50 % – мусор. Затем, чтобы понять, что получено в действительности, Алекс и Боб просто объявляют цвета паука, использованного для кодирования и измерения каждого бита. Если для некоторого бита цвета совпали, то полученное значение правильно, остальные можно отбросить. Поскольку выбор кодировщика Алексом и выбор измерителя Бобом были случайны и не имеют ничего общего с ключом, который они стремятся выработать, они могут раскрыть эти данные публично, не опасаясь, что какой-то условный додо узнает закрытый ключ.

С другой стороны, что, если некий Дэйв все-таки прослушивает канал, по которому Алекс передает свои квантовые системы Бобу?

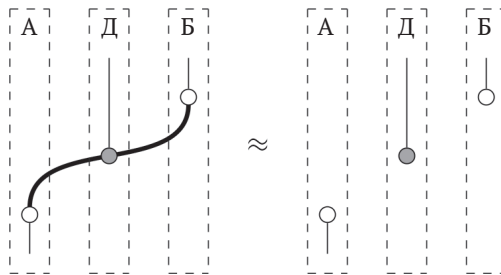


Если бы было возможно клонировать квантовую систему, Дэйв сохранял бы копию каждого состояния, которое Алекс передает Бобу, а затем, после того как Алекс и Боб объявят свои базисы, Дэйв мог бы просто измерить свою копию и получить сообщение. Но, как мы знаем из главы 4, это невозможно, поэтому лучшее, что может сделать Дэйв, – произвести какое-то измерение.

Сначала для простоты предположим, что Дэйв также выбирает измерения между \circ и \bullet . Будем рассматривать только случаи, когда Алекс и Боб собираются сохранить переданный Алексом бит, т. е. когда они оба выбрали либо \circ , либо \bullet . Поскольку Алекс выбирает свои базисы для кодирования случайно, то Дэйв не может рассчитывать ни на что большее, кроме измерения в правильном базисе в половине случаев. Если это произойдет, то он получит копию бита Алекса:

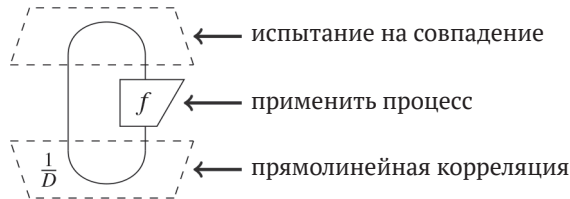


Но в оставшейся половине случаев Боб получит шум, как если бы он неправильно выбрал измеритель:



Вместо того чтобы правильно получать бит Алекса в половине случаев, Боб иногда получает шум, поэтому вероятность получения Бобом правильного бита снижается. Это наводит на мысль о простой стратегии обнаружения подслушивания. Время от времени Алекс и Боб случайным образом выбирают несколько запасных битов (которые Алекс послал, но использовать их никто не собирается) и сравнивают их. Если правильно получено существенно меньше, чем 50 % битов, значит, кто-то подслушивает, поэтому они прерывают сеанс.

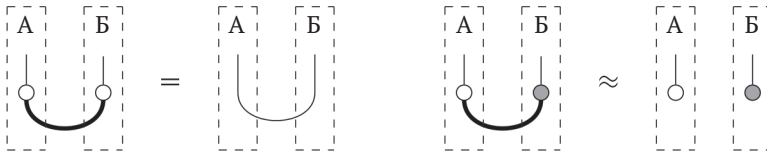
Упражнение* 9.55. Какова все же вероятность, что Боб получит переданный Алексом бит, если Дэйв подслушивает? Заметьте, что если на вход процесса подается классическое состояние, имеющее равномерное распределение, то вероятность, что он породит выход, равный входу, можно вычислить по правилу Борна:



Замечание 9.56. Можно показать, что Дэйва удастся обнаружить, даже если ему разрешено выполнять произвольные квантовые процессы, а не только измерения \circ и \bullet . Однако анализ несколько усложняется (см. ссылки в разделе 9.7).

Одно из преимуществ графического представления состоит в том, что мы можем просто согнуть провода и получить, на первый взгляд, другой протокол. Предположим, что Алекс не посылает Бобу системы по квантовому каналу, а вместо этого Алекс и Боб разделяют общее состояние Белла. Тогда если оба выбирают

измерение случайно, то будет иметь место прямолинейная корреляция, когда измерения одинаковы, и отсутствие корреляции, если они различны:

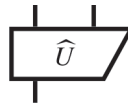


Это дает упрощенную версию другого протокола КРК, который называется E91. Но хотя фактические шаги протокола разнятся, результат получается такой же. В конечном итоге Алекс и Боб получают прямолинейно коррелированную последовательность случайных битов. А поскольку мы работаем, по существу, с теми же диаграммами, то обнаружить прослушивание можно точно так же, как и раньше. Однако у прочтения BB84 «сбоку» есть дополнительные преимущества. Во-первых, Алекс и Боб не обязаны непрерывно находиться в (квантовом) контакте, чтобы выработать общий ключ. Они просто должны установить какие-то разделяемые состояния Белла в какой-то момент, а затем «использовать их по полной» по мере необходимости. Во-вторых, Алекс и Боб могут удостовериться, что имеют настоящие состояния Белла (а не подделанные кем-то), проверив, что исходы их измерений действительно демонстрируют квантовую нелокальность. Мы подробно обсудим это в разделе 11.1.

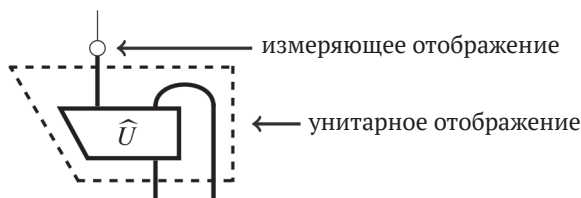
Замечание* 9.57. В полной версии протокола E91 Алекс и Боб для проверки на нелокальность включают третье измерение и проверяют, что корреляции между исходами их измерений нарушают *неравенство Белла*. Его нарушение как раз и гарантирует нелокальность. Изящество этой техники заключается в том, что разделять нужно только исходы для «мусорных» битов, т. е. тогда, когда результаты измерений расходятся, поэтому нет нужды жертвовать полезными битами для контроля безопасности.

9.2.7. Телепортация с дополнительными измерениями

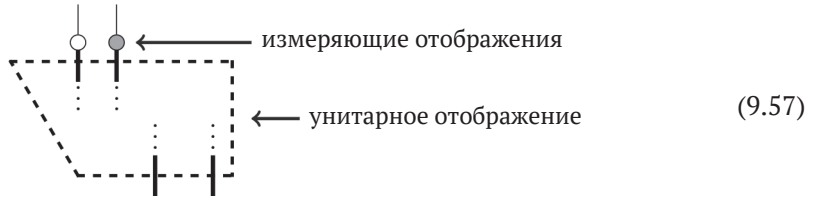
Как и было обещано, мы можем заменить «черный ящик»



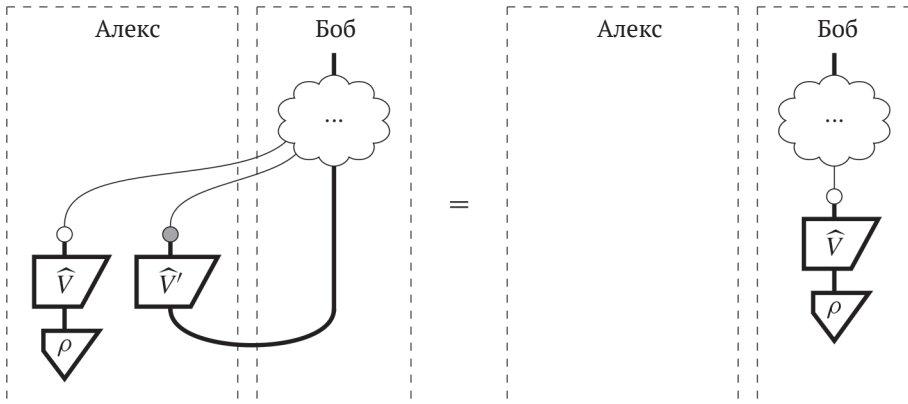
применяемый в телепортации, чем-нибудь, построенным исключительно с помощью пауков. Телепортация основывается на том, что Алекс сначала производит совместное измерение двух своих систем:



Если размерность квантовых систем равна D , то классический провод будет принимать D^2 различных значений. Поэтому мы могли бы с тем же успехом представить его двумя классическими проводами, каждый из которых может принимать D значений:



(Из того, что мы использовали два разных цвета, можно сделать вывод, что будет дальше.) Чтобы телепортация состоялась, это измерение не должно быть \otimes -разделимым, иначе Боб в лучшем случае получит какой-то декогерентный вариант состояния Алекса, поскольку затем все придется передавать по классическому проводу:



Учитывая, что у нас имеется дополнительная пара пауков, мы можем попытаться использовать индуцированное унитарное отображение из предложения 9.50



для порождения неразделимого измерения. Вот первая попытка:

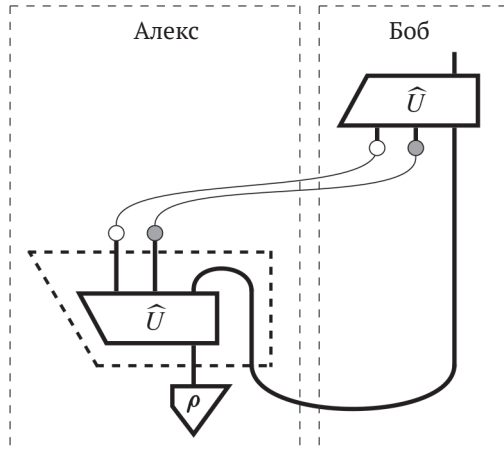


Нет, так не работает! Применение CNOT вообще никак не изменило измерения! В частности, оно осталось разделенным. Но поскольку мы пробуем заниматься наукой, поэкспериментируем еще. Что, если подключить индуцированное унитарное отображение по-другому?

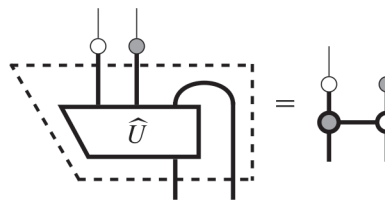


(9.58)

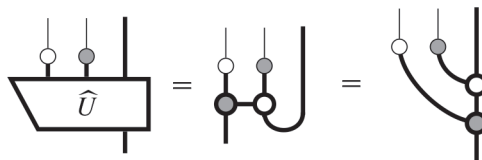
Перевернутый вариант, конечно, тоже унитарный, поэтому (9.58) по-прежнему является измерением ОНБ, и очевидного \otimes -разделения не видно. Это, конечно, не доказывает, что оно вообще не разделяется, но мы будем знать, что это так, если удастся получить работающий протокол телепортации. Поэтому попробуем «заполнить блоки» на этой диаграмме телепортации:



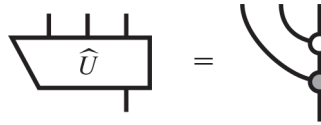
Поскольку кандидат на роль измерения Алекса у нас уже есть, осталось только найти отображение \hat{U} , необходимое для построения корректировки Боба. Это сводится к решению следующего уравнения:



Перегибая провод в обеих частях, получаем:



поэтому решением будет

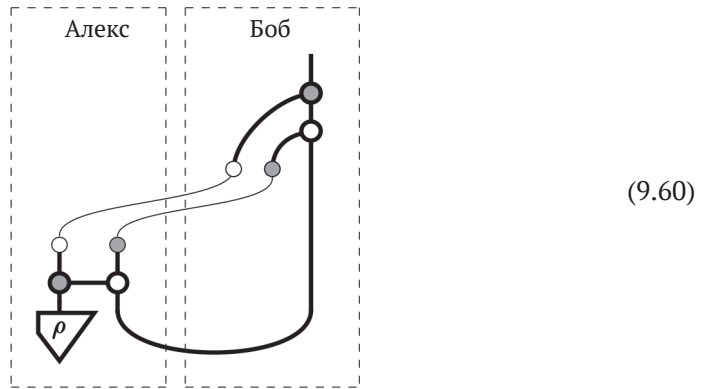


Отсюда получаем корректировку



Упражнение 9.58. Докажите, что отображение (9.59) каузальное и управляемое унитарное (с точностью до числа).

Заполнение блоков дает следующий потенциальный протокол телепортации:



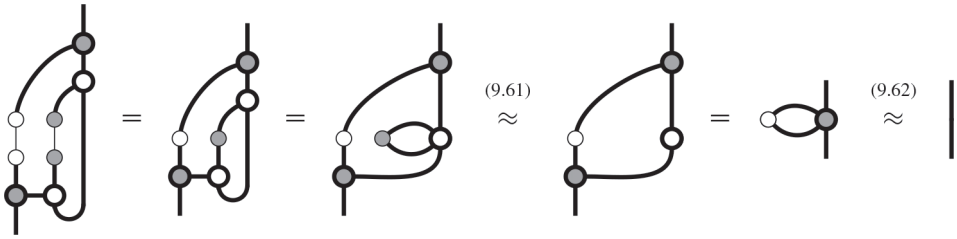
Осталось только показать, что этот протокол действительно работает при нашем выборе \hat{U} . Применяя правила слияния пауков и дополнительность, мы можем показать, что (9.60) и в самом деле осуществляет квантовую телепортацию. В частности, нам понадобится следующий факт:



в котором использовано слияние гибридных пауков и правило разъединения квантового паука. Просто поменяв цвета местами, мы также получаем:

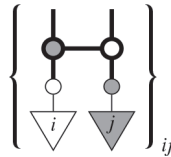


Отсюда мы делаем вывод, что этот вариант телепортации работает:



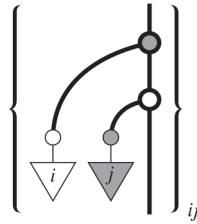
Упражнение 9.59. Покажите, что если \circ и \bullet представляют Z - и X -базисы соответственно, то:

1) состояние Белла имеет вид:



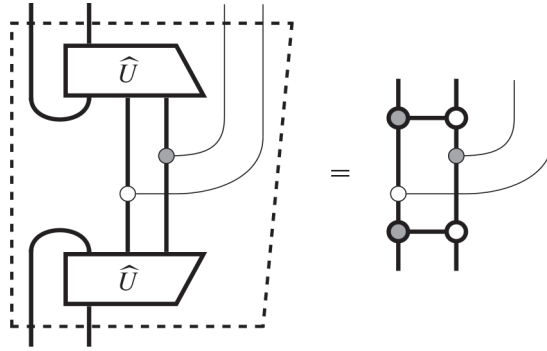
(числа игнорируются), и, следовательно, (9.58) является измерением ортонормированного базиса Белла;

2) отображения Белла имеют вид:



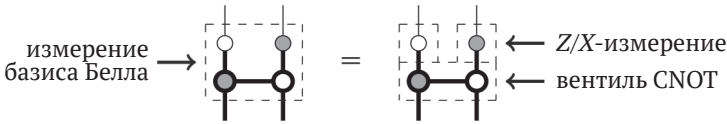
Итак, (9.60) дает нам полное и при этом чисто диаграммное представление того самого протокола квантовой телепортации, который мы изучаем на протяжении всей книги, но теперь у нас есть еще и общий рецепт «заполнения» блоков. Нужно лишь найти дополнительную пару пауков для любой размерности, а протокол телепортации (9.60) (вместе с доказательством его корректности!) останется неизменным.

Такой же подход годится для плотного кодирования и перекоммутации запутывания. В последнем случае требуемое невозмущающее измерение принимает вид:



Упражнение 9.60. Докажите корректность протоколов плотного кодирования и перекоммутации запутывания, пользуясь только правилами слияния и разъединения пауков.

Как мы неоднократно убеждались, одну и ту же диаграмму можно прочитать несколькими способами. Так обстоит дело и в случае диаграммы (9.58):



Для наших целей, т. е. чтобы сбросить покров тайны с квантовых особенностей, это различие несущественно, но для человека, который реализует квантовые процессы в лаборатории, оно может стать решающим. Например, бывает очень трудно произвести неразделимое измерение двух систем; проще реализовать квантовый вентиль CNOT и измерения одной системы, именно так и реализуется большинство квантовых систем в лабораторных условиях.

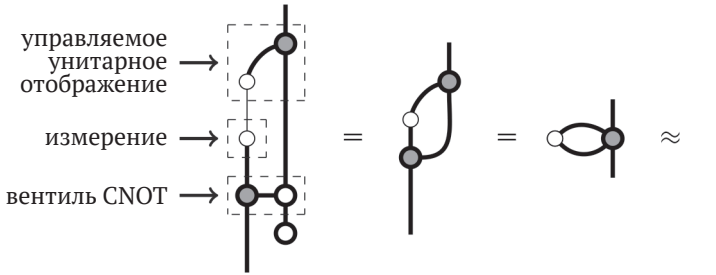
Пример 9.61. Квантовая телепортация позволяет перенести состояние с одной системы на другую, используя:

- вспомогательную систему;
- состояние Белла;
- квантовый вентиль CNOT;
- два измерения одной системы и
- две корректировки одной системы.

Можно задаться вопросом, существует ли способ сделать то же самое с меньшим объемом ресурсов. Да, существует. На самом деле нам необходимы лишь:

- \bigcirc -состояние;
- квантовый вентиль CNOT;
- одно измерение одной системы и
- одна корректировка одной системы.

А никакой вспомогательной системы не нужно вовсе. Вот как это выглядит:



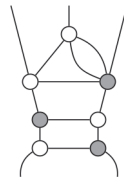
Таким образом, вместо двух систем, подготовленных в состоянии Белла, нам нужна только одна система, подготовленная в 0-фазном состоянии. Но за это приходится заплатить тем, что, в отличие от телепортации, для переноса состояния исходная и целевая системы должны находиться в одном месте, чтобы CNOT можно было применить к обеим, поскольку на данный момент не существует такой штуки, как «нелокальный вентиль CNOT».

Поучительно также сравнить это доказательство корректности с доказательством для протокола телепортации; в частности, это доказательство практически совпадает с последними двумя шагами доказательства для телепортации.

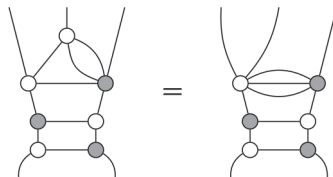
9.3. Сильная дополнителность

Мы уже достигли серьезного прогресса в доказательстве различных фактов путем применения одних лишь простых диаграммных правил, например слияния (фазовых) пауков и разъединения пауков. Но насколько мощна система описанных до сих пор правил? Иначе говоря, какого рода диаграммы можно упростить, применяя только эти правила?

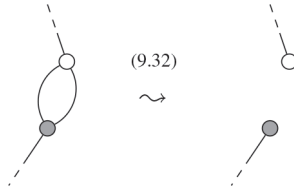
Пусть имеется умеренно сложная диаграмма, включающая дополнительных пауков:



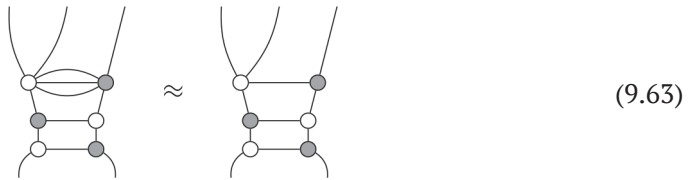
и мы хотим приступить к ее упрощению. Можно, конечно, применить правила слияния пауков, чтобы слить все кружочки одного цвета:



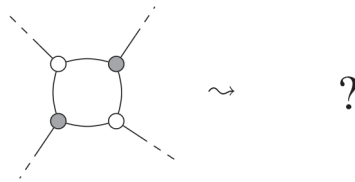
После этого мы получаем диаграмму, в которой встречаются циклы пауков чередующихся цветов, от которых хотелось бы избавиться. Количество пауков в цикле, конечно, всегда четное, т. е. можно задаться вопросом, как поступать с 2-циклами, 4-циклами и т. д. Для 2-циклов можно просто применить дополнтельность:



Это позволит немного уменьшить сложность рассматриваемого примера:



Но теперь нам мешают назойливые 4-циклы, поскольку к ним не применимо ни одно из известных правил:



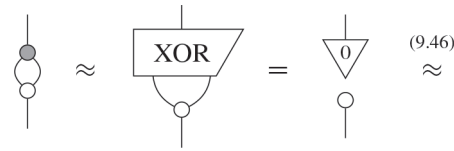
Иначе можно сказать, что отсутствие применимых правил означает, что мы достигли *нормальной формы*, или попросту «уперлись в тупик». И что делать? Сдаться? Вместо этого мы попробуем найти «недостающие правила», чтобы можно было продолжить.

9.3.1. Недостающие правила

Временно сосредоточимся на пауках Z и X . В примере 9.45 мы напомнили, что эта пара пауков обладает характерным свойством: адъюнкт отображения X -копирования ведет себя как операция XOR в Z -базисе:



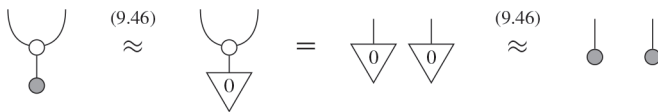
С одной стороны, это дает возможность по-другому взглянуть на то, почему эти пауки дополнтельные, просто проведя аналогию с классическими битами. А именно XOR любого бита с самим собой всегда дает нулевой бит, поэтому копирование с последующим XOR – то же самое, что игнорирование входа и вывод нуля:



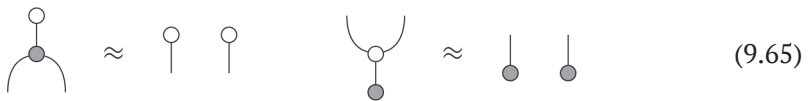
Помимо этого свойства, есть еще одно, на первый взгляд не связанное с ним следствие: серый кружочек определяет функциональное отображение (см. определение 8.13) для белого базиса, основанное, конечно, на функции XOR. В предложении 8.19 из предыдущей главы мы кратко охарактеризовали функциональные отображения в терминах копирования и удаления. Применяя это предложение к XOR, получаем:



а мы уже видели, что \bullet -паук с одним выходом является с точностью до числа частей \circ -ОНБ, так что



Заменяя первые два равенства X-пауками, получаем:



Теперь становится очевидным, что роли, которые играют в этих равенствах Z и X, взаимозаменяемы, т. е. равенства остаются в силе, если каждый цвет заменить противоположным, одновременно применив к каждому равенству адьюнкцию. Из последних двух равенств также следует еще одно, связывающее двух одноногих пауков:



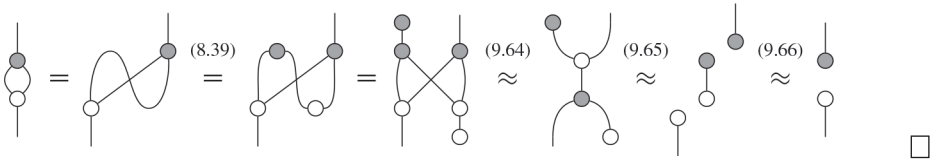
которое попросту означает, что приведенное выше число отлично от нуля.

Упражнение 9.62. Покажите, что пауки, удовлетворяющие условию (9.65), удовлетворяют также (9.66).

На первый взгляд, (9.64) и (9.65) кажутся «случайным» свойством Z и X , но если мы рассмотрим эти равенства для произвольной пары пауков, то увидим, что из (9.64) и (9.65) следует дополнителность.

Теорема 9.63. Из равенств (9.64) и (9.65) следует дополнителность.

Доказательство. В силу предложения 9.35 достаточно установить справедливость уравнения дополнителности с точностью до \approx . Имеем:



Таким образом, равенства (9.64) и (9.65) описывают очень специальные пары дополнителных пауков, заслуживающие отдельного названия.

Определение 9.64. Пара пауков \circ и \bullet называется сильно дополнителной, если выполняются следующие условия:

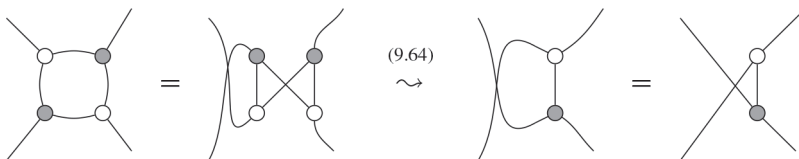
$$\begin{array}{c} \bullet \\ \circ \end{array} \begin{array}{c} \bullet \\ \circ \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \circ \\ \bullet \end{array} \quad (9.67)$$

$$\begin{array}{c} \circ \\ \bullet \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \circ \\ \circ \end{array} \quad \begin{array}{c} \circ \\ \bullet \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \bullet \\ \bullet \end{array} \quad (9.68)$$

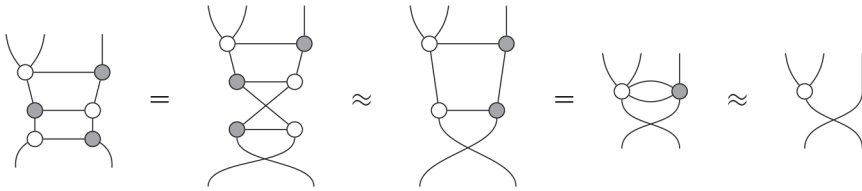
Хотя числа не очень существенны, для полноты мы все же включили их в приведенные выше равенства. Как и в случае дополнителности, они уже однозначно определены версиями без чисел.

Упражнение 9.65. Докажите, что, как и в предложении 9.35, числа в определении 9.64 однозначно определены равенствами (9.64) и (9.65). Обратите внимание, насколько здесь важно, что \approx означает эквивалентность с точностью до положительного числа (см. замечание 9.36).

Ну и какое отношение все это имеет к нашей вступительной беседе о 4-циклах? Да самое прямое, потому что левая часть равенства (9.67) – не что иное, как 4-цикл с «подвывертом»:



Итак, мы теперь знаем, что делать с 4-циклом, и продолжим с того места, где остановились, – с равенства (9.63):



Вот так-то лучше!

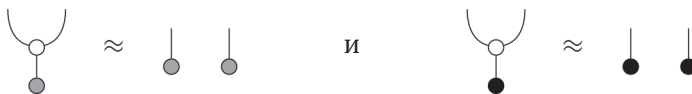
С одной стороны, дополнителность мы вводили с помощью предельно четкой канонической интерпретации, а в случае сильной дополнителности ничего столь же наглядного нет. Но, несмотря на отсутствие канонической интерпретации, сильная дополнителность будет иметь важные последствия в оставшейся части этой главы (и всей книги). Некоторые из этих последствий мы рассмотрим в следующем разделе. Ни одно из них не имеет места для общих (не сильно) дополнителных пар пауков.

9.3.2. Моногамия сильной дополнителности

В примере 9.44 мы заметили, что для большинства размерностей максимальное число попарно дополнителных пауков (или взаимно несмещенных ОНБ) неизвестно. Поскольку сильная дополнителность налагает более строгие ограничения на то, каких пауков можно связывать, это число должно быть меньше. На самом деле можно показать, что сильно дополнителные пауки появляются только парами.

Теорема 9.66. Попарно сильно дополнителными могут быть самое большее два паука. Иначе говоря, для любой нетривиальной системы, если обе пары \circ/\bullet и \circ/\bullet сильно дополнителные, пара \bullet/\bullet не может быть сильно дополнителной.

Доказательство. Предположим, что обе пары \circ/\bullet и \circ/\bullet сильно дополнителные. Тогда



Следовательно, по теореме 8.18



с точностью до числа являются состояниями \circ -ОНБ. Поэтому они должны быть равны (с точностью до числа) или ортогональны. Теперь предположим, что \bullet/\bullet тоже сильно дополнителны. Тогда в силу (9.66)

$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \approx \boxed{} \neq 0$$

поэтому



Но тогда

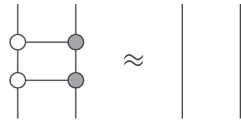


что для нетривиальной системы невозможно. Поэтому ни в какой нетривиальной системе не может быть трех попарно сильно дополнительных пауков. □

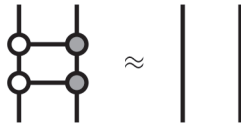
9.3.3. Лики сильной дополнителности

Ранее мы приводили несколько эквивалентных операционных характеристик дополнителности: в терминах измерения после кодирования в определении 9.27, в терминах измерения двух систем, находящихся в состоянии Белла, в предложении 9.30, и в терминах вентилей CNOT в предложении 9.50. Поскольку из сильной дополнителности следует дополнителность, все эти характеристики сохраняют силу и для сильно дополнительных пар, но очевидно, что следствий будет гораздо больше. В этом разделе мы рассмотрим наиболее важные.

В предложении 9.50 мы узнали, что дополнителность сводится к унитарности для обобщенных вентилей CNOT:

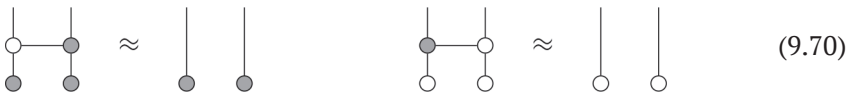


или, эквивалентно, в терминах обобщенных квантовых вентилей CNOT:



Это равенство можно рассматривать как равенство между квантовыми схемами (см. примеры 6.13 и 9.24). Понятие сильной дополнителности можно сформулировать аналогично.

Предложение 9.67. Сильная дополнителность эквивалентна:



Дублируя равенство (9.69), получаем:



Следовательно, три вентиля CNOT образуют перекоммутацию:

$$\begin{array}{c} \circ \\ \text{---} \\ \bullet \\ \text{---} \\ \circ \\ \text{---} \\ \bullet \end{array} \approx \begin{array}{c} \circ \\ \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} \quad \begin{array}{c} \bullet \\ \text{---} \\ \circ \\ \text{---} \\ \bullet \end{array} \approx \begin{array}{c} \bullet \\ \text{---} \\ \circ \\ \text{---} \\ \bullet \end{array} \quad (9.72)$$

Упражнение 9.68. Покажите, что в предположении дополнителности равенства (9.69) и (9.71) действительно эквивалентны равенствам (9.72).

Мы начали исследование сильной дополнителности, стремясь избавиться от 4-циклов, поэтому можно было бы подумать, что сильная дополнителность ни к чему, кроме 4-циклов, не применима. Но оказывается, что из нее следуют равенства для гораздо более общего семейства диаграмм. В качестве простого примера объединим уравнения копирования

$$\begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} \approx \begin{array}{c} \circ \\ \circ \end{array} \quad \begin{array}{c} \text{---} \\ \circ \\ \text{---} \\ \bullet \end{array} \approx \begin{array}{c} \bullet \\ \bullet \end{array}$$

с правилом слияния пауков, чтобы доказать n -арную версию правил копирования:

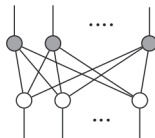
$$\begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} = \begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} \approx \begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} \approx \dots \approx \begin{array}{c} \circ \\ \circ \end{array} \dots \begin{array}{c} \circ \\ \circ \end{array}$$

Предложение 9.69. Из сильной дополнителности следует:

$$\begin{array}{c} \text{---} \\ \bullet \\ \text{---} \\ \circ \end{array} \approx \begin{array}{c} \circ \\ \circ \end{array} \dots \begin{array}{c} \circ \\ \circ \end{array} \quad \begin{array}{c} \text{---} \\ \circ \\ \text{---} \\ \bullet \end{array} \approx \begin{array}{c} \bullet \\ \bullet \end{array} \dots \begin{array}{c} \bullet \\ \bullet \end{array} \quad (9.73)$$

Более сложный пример касается диаграмм следующего вида.

Определение 9.70. Полной двудольной диаграммой пауков называется диаграмма, обладающая тем свойством, что каждый паук одного цвета соединен с каждым пауком другого цвета и никаких других соединений нет:



Хотя, на первый взгляд, связность этой диаграммы очень высока, мы можем, воспользовавшись сильной дополнителностью, упростить ее до двух пауков, связанных одиночным проводом.

Теорема 9.71. Сильная дополнителность \circ и \bullet эквивалентны:

(9.74)

Доказательство. Мы докажем это утверждение, используя два рассуждения по индукции. Сначала рассмотрим частный случай, когда $n = 2$, а m произвольно:

(9.75)

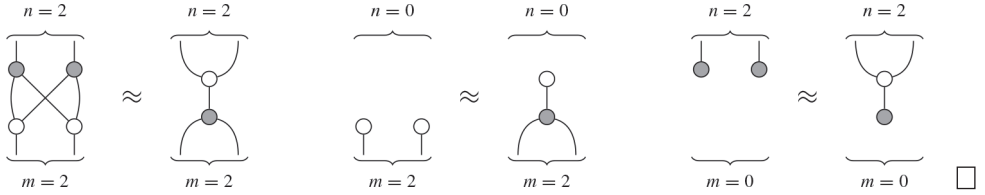
и проведем индукцию по m . Для базы индукции $m = 0$ это просто:

$m = 0$ $m = 0$

Теперь предположим, что (9.75) справедливо для m , и докажем, что оно верно и для $m + 1$:

Таким образом, (9.75) доказано. Теперь можно доказать (9.74) индукцией по n . Базовый случай – это простое m -арное копирование, для которого мы все доказали в предложении 9.69. Предположим, что равенство (9.74) верно для n , и докажем, что оно верно для $n + 1$. Доказательство является почти зеркальным отражением предыдущего, только мы используем (9.75) – «усиленную» версию (9.64):

Обратно, все три сильно дополнителных правила из (9.64) и (9.65) являются частными случаями (9.74):



Кроме того, ограничение равенства (9.74) на случай $m = 0$ дает одно из правил «мультикопирования» из предложения 9.69, если читать его справа налево:

(9.76)

и аналогично ограничение на случай $n = 0$ дает:

(9.77)

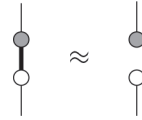
Замечание* 9.72. На первый взгляд может показаться, что мы просто извлекли равенства (9.74), как кролика из шляпы. К счастью, это не так, а вытекает из того, что для любой сильно дополнителной пары следующие отображения:



образуют алгебраическую структуру, называемую *биалгеброй*, где приставка «би» относится к тому факту, что участвуют как алгебра, так и коалгебра (см. замечания 3.17 и 8.22). Определяющая аксиома является своеобразной коммутативностью умножения (т. е. алгебры) и коумножения (т. е. коалгебры):

Эти структуры хорошо изучены, и относящиеся к ним равенства можно конструировать с помощью техники *подсчета путей*. Подробнее это описано в разделе* 9.6.2.

Теорема 9.71 дает эквивалентное представление сильной дополнителности. Но ни одно из приведенных до сих пор представлений сильной дополнителности не похоже на оригинальное определение дополнителности, в которое входили как классические, так и квантовые системы:



Путем простого комбинирования некоторых дублированных частей (9.74) в КК-отображения сильная дополнительность дает нам новые равенства, позволяющие рассуждать о классически-квантовом взаимодействии. Следующий факт будет играть главенствующую роль в выводе квантовой нелокальности в разделе 11.1.

Следствие 9.73. Из сильной дополнительности \circ и \bullet следует:

(9.78)

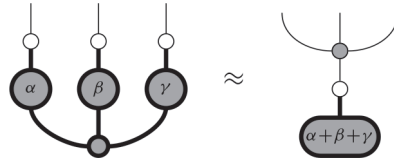
Доказательство. Применяя теорему 9.71, получаем:

где первое равенство – это просто раскрытие дублирования, а третье – повторное дублирование. □

\bullet -паук в левой части (9.78) – квантовый процесс, тогда как \bullet -паук в правой части здесь рассматривается как операция над классическими данными. В разделе 9.3.5 мы увидим, что точно делает этот процесс. А пока можно интерпретировать равенство (9.78) следующим образом: если сначала применить заданного квантового \bullet -паука и \circ -измерить все его выходы, то получится то же самое, как если бы сначала произвели \circ -измерение, а затем применили классического \bullet -паука. Конечно, этому свойству недостает концептуальной кристалльности (обычной) дополнительности, но все равно оно очень полезно.

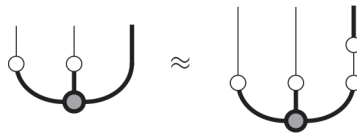
Пример 9.74. В примере 9.26 мы видели удивительное взаимодействие фаз с ГХЦ-состоянием. Но попытка произвести измерение того же цвета, что и фазы, попросту уничтожает фазы. С другой стороны, если произвести измерение, цвет которого сильно дополняет цвет фаз, то картина будет совершенно иной:

Теперь все три измерения заменены одним, за которым следует некое классическое отображение. А поскольку фаза не смещена относительно \bullet и \circ , то она не исчезает. Более того, как мы увидим в разделе 11.1, при специальном выборе фаз измерений α, β и γ в равенстве

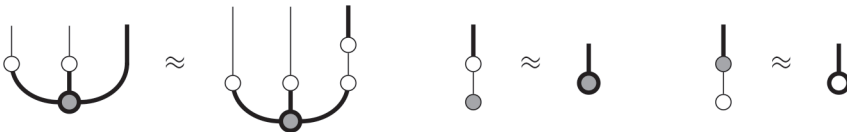


останется даже неопровержимое доказательство этого удивительного «движения назад» фазовых данных, и можно будет предсказать существование взаимодействий между удаленными квантовыми системами, необъяснимое простыми вероятностными корреляциями, т. е. квантовую нелокальность.

Упражнение 9.75. Покажите, что из сильной дополнителности следует равенство



Можете ли вы предложить интерпретацию этого равенства? Обратно, покажите, что из этого равенства следует сильная дополнителность (это не так просто!):



9.3.4. Классическая подгруппа

В разделе 9.2.2 мы видели, что для дополнительной пары пауков базисные состояния одного цвета принадлежат фазовой группе (см. раздел 9.1.4) другого цвета. В этом разделе мы дадим другую характеристику сильной дополнителности в терминах специальной роли, которую базисные состояния одного цвета играют в фазовой группе другого цвета. И хотя эта характеристика совершенно не похожа на данную в определении 9.64, доказать их эквивалентность окажется на удивление просто.

В примере 9.7 мы видели, что состояния X -базиса можно представить в виде фазовых состояний относительно Z -базиса:



и наоборот – состояния Z -базиса можно представить как X -фазовые состояния:



Мы также видели, что групповую операцию можно вычислить с помощью слияния пауков (см. теорему 9.20):

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \text{0} \quad \text{0} \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \\ \text{0} \end{array} = \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \pi \quad \pi \end{array} \tag{9.79}$$

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \pi \quad \text{0} \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \\ \pi \end{array} = \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \circ \quad \circ \\ \text{0} \quad \pi \end{array} \tag{9.80}$$

Отметим, что результатом всех групповых операций является одно из двух фазовых состояний, с которых мы начинали. Это означает, что фазовые состояния, составляющие (с точностью до числа) Z -базис, замкнуты относительно групповой операции в X -фазовой группе. Они также содержат единицу X -фазовой группы и обращения всех элементов Z -базиса (поскольку, согласно (9.79), все они самообратные). Таким образом, они образуют *подгруппу* фазовой группы. На самом деле это стандартный результат теории групп: конечное подмножество группы, замкнутое относительно групповой операции, автоматически является подгруппой, поэтому даже не нужно было проверять наличие единицы и обратных элементов. Очевидно, что это справедливо и в случае, если пауки Z и X поменяются ролями.

Пример 9.76. Для Z - и X -базисов фазовая группа – это группа круга $U(1)$, а классическая подгруппа совпадает с двухэлементной циклической группой \mathbb{Z}_2 , которую можно представить как два поворота: на нулевой угол и на 180° :

$$\left\{ \begin{array}{c} \circlearrowleft \\ \bullet \text{0} \end{array}, \begin{array}{c} \circlearrowright \\ \pi \end{array} \right\} \subseteq \left\{ \begin{array}{c} \circlearrowleft \\ \alpha \end{array} \right\} \tag{9.81}$$

Структура этой подгруппы – прямое следствие сильной дополнтельности. Более того, она эквивалентна сильной дополнтельности.

Теорема 9.77. Пауки \circ и \bullet являются сильно дополнтельными тогда и только тогда, когда базисные состояния \circ образуют подгруппу фазовой группы \bullet , и наоборот. Рассматривая базисные состояния как классические исходы (см. раздел 8.1.1), мы называем эту подгруппу фазовой группы *классической подгруппой*.

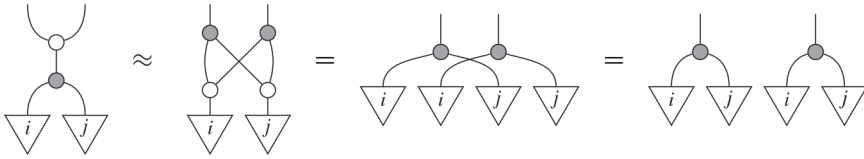
Доказательство. В предположении, что \circ и \bullet сильно дополнтельные, мы покажем, что \bullet -сумма двух \circ -базисных состояний

$$\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \triangle \quad \triangle \\ i \quad j \end{array} \tag{9.82}$$

снова является \circ -базисным состоянием. Напомним, что по теореме 8.18

$$\begin{array}{c} \bullet \\ | \\ \triangle \\ \psi \end{array} \in \left\{ \begin{array}{c} \bullet \\ | \\ \triangle \\ i \end{array} \right\}_i \text{ тогда и только тогда, когда } \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \triangle \quad \triangle \\ \psi \end{array} \stackrel{(*)}{=} \begin{array}{c} \bullet \\ | \\ \triangle \\ \psi \end{array} \begin{array}{c} \bullet \\ | \\ \triangle \\ \psi \end{array}$$

Доказательство того, что (9.83) является \circ -базисным состоянием, проведем следующим образом:

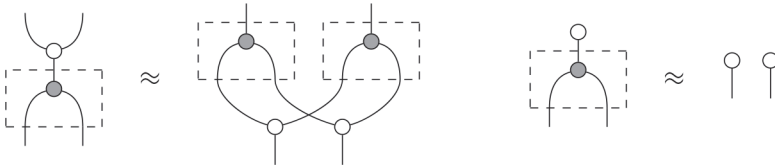


Таким образом, \circ -базис является конечным подмножеством фазовой группы, замкнутым относительно групповой операции, а потому, согласно стандартному результату из теории групп, образует подгруппу.

Доказательство обратного утверждения вытекает из тех же соображений, которыми мы в разделе 9.3.1 обосновывали уравнения сильной дополнителности, с использованием поведения XOR. Повторим это рассуждение для общего случая. Поскольку \circ -базисные состояния образуют подгруппу \bullet -фазовой группы, то операция \bullet -суммы переводит каждую пару \circ -базисных состояний в другое \circ -базисное состояние (с точностью до числа):

(9.83)

В частности, это означает, что \bullet -сумма является (с точностью до числа) функциональным отображением. Поэтому в силу предложения 8.19 отсюда следует, что



Наконец, любая подгруппа содержит единицу группы, поэтому классическая подгруппа должна содержать единицу \bullet -фазовой группы. Следовательно, единица серой фазовой группы является \circ -базисным состоянием, а потому

□

Соглашение 9.78. Мы будем использовать греческие буквы κ, κ' и т. д. для обозначения фазовых состояний, принадлежащих классической подгруппе, а буквы $\alpha, \beta, \gamma, \dots$ – для обозначения общих фазовых состояний. То есть фазовые группы и их классические подгруппы двух цветов изображаются так:

$$\left\{ \begin{array}{c} \circ \\ \bullet \\ \kappa \end{array} \right\}_{\kappa} \subset \left\{ \begin{array}{c} \circ \\ \bullet \\ \alpha \end{array} \right\}_{\alpha}$$

Но что здесь такое:

$$\begin{array}{c} | \\ \bullet \\ \pi \end{array} \quad (9.87)$$

Из того, что

$$\begin{array}{c} \bullet \\ \pi \\ \circ \\ 0 \end{array} = \begin{array}{c} \bullet \\ \pi \end{array} \qquad \begin{array}{c} \bullet \\ \pi \\ \bullet \\ \pi \end{array} = \begin{array}{c} \bullet \\ 0 \end{array}$$

следует, что (9.87) – *квантовый вентиль NOT* на состояниях \circ -базиса, поэтому (9.86) – действительно квантовый вентиль CNOT. Разумеется, то же рассуждение с тонкими проводами доказывает аналогичный факт для классического вентиля CNOT.

В равенстве (9.84) участвуют копирующие пауки и фазовые состояния. Его можно распространить на копирующих пауков и фазовые отображения.

Предложение 9.81. Для сильно дополнительных \circ и \bullet имеют место равенства

$$\begin{array}{c} \circ \\ \bullet \\ \vec{k} \end{array} = \begin{array}{c} \circ \\ \vec{k} \end{array} \begin{array}{c} \circ \\ \vec{k} \end{array} \qquad \begin{array}{c} \bullet \\ \circ \\ \vec{k} \end{array} = \begin{array}{c} \bullet \\ \vec{k} \end{array} \begin{array}{c} \bullet \\ \vec{k} \end{array} \quad (9.88)$$

Мы называем это правилом *k-копирования отображений*.

Доказательство. Имеем:

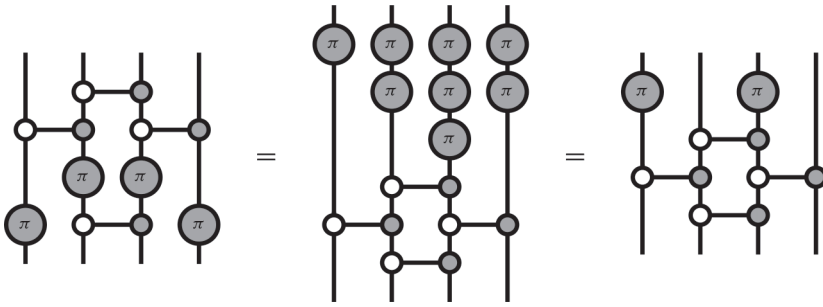
$$\begin{array}{c} \circ \\ \bullet \\ \vec{k} \end{array} = \begin{array}{c} \circ \\ \bullet \\ \vec{k} \end{array} \stackrel{(9.67)}{=} D \begin{array}{c} \bullet \\ \circ \\ \bullet \\ \vec{k} \end{array} \stackrel{(9.84)}{=} \begin{array}{c} \bullet \\ \vec{k} \end{array} \begin{array}{c} \bullet \\ \vec{k} \end{array} = \begin{array}{c} \bullet \\ \vec{k} \end{array} \begin{array}{c} \bullet \\ \vec{k} \end{array}$$

Заметим, что это точное равенство, поскольку в дублированной версии (9.67) имеется множитель D , а в точном аналоге (9.84) – множитель $1/D$. \square

Пример 9.82. В силу (9.88) вентиль NOT можно протолкнуть за вентиль CNOT:

$$\begin{array}{c} \circ \\ \bullet \\ \pi \end{array} \begin{array}{c} \circ \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \pi \end{array} \begin{array}{c} \bullet \\ \pi \end{array} = \begin{array}{c} \bullet \\ \pi \end{array} \begin{array}{c} \bullet \\ \pi \end{array}$$

Поэтому если схема состоит только из вентилях NOT и CNOT, то все вентили NOT можно переместить в один конец схемы:



В равенства (9.84) входят неукрашенные пауки одного цвета и фазовые вентили другого цвета. Мы можем преобразовать их в равенство, содержащее только фазовые вентили обоих цветов.

Предложение 9.83. Для сильно дополнительных \circ и \bullet имеет место равенство

$$\begin{array}{c} \circ \\ \kappa \\ \bullet \\ \kappa' \end{array} = \frac{1}{\sqrt{D}} \begin{array}{cc} \circ & \bullet \\ \kappa & \kappa' \\ \bullet & \circ \\ \kappa' & \kappa \end{array} \quad (9.89)$$

или, эквивалентно, равенство, получающееся дублированием:

$$\begin{array}{c} \circ \\ \kappa \\ \bullet \\ \kappa' \end{array} = \begin{array}{c} \bullet \\ \kappa' \\ \circ \\ \kappa \end{array} \quad (9.90)$$

Мы называем это правилом κ - κ' -коммутативности.

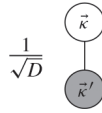
Доказательство. Сначала заметим, что

$$\begin{array}{c} \circ \\ \vec{\kappa} \\ \bullet \\ \vec{\alpha} \end{array} = \begin{array}{c} \circ \\ \vec{\kappa} \\ \bullet \\ \vec{\alpha} \end{array} \stackrel{(9.84)}{=} \frac{1}{\sqrt{D}} \begin{array}{cc} \circ & \circ \\ \vec{\kappa} & \vec{\kappa} \\ \bullet & \bullet \\ \vec{\alpha} & \vec{\alpha} \end{array} \quad (9.91)$$

Мы опираемся на недублированный вариант (9.88), который, как легко показать, выполняется точно (т. е. без глобальной фазы):

$$\begin{array}{c} \circ \\ \vec{\kappa} \\ \bullet \\ \vec{\kappa}' \end{array} = \begin{array}{c} \circ \\ \vec{\kappa} \\ \bullet \\ \vec{\kappa}' \end{array} \stackrel{(9.88)}{=} \begin{array}{c} \circ \\ \vec{\kappa} \\ \bullet \\ \vec{\kappa}' \end{array} \stackrel{(9.91)}{=} \frac{1}{\sqrt{D}} \begin{array}{cc} \circ & \circ \\ \vec{\kappa} & \vec{\kappa}' \\ \bullet & \bullet \\ \vec{\kappa}' & \vec{\kappa} \end{array} = \frac{1}{\sqrt{D}} \begin{array}{cc} \circ & \bullet \\ \vec{\kappa} & \vec{\kappa}' \\ \bullet & \circ \\ \vec{\kappa}' & \vec{\kappa} \end{array}$$

Для дублированного варианта нужно показать, что



является глобальной фазой, и это действительно так:

$$\text{double} \left(\frac{1}{\sqrt{D}} \begin{array}{c} \text{white circle } \vec{k} \\ \text{grey circle } \vec{k}' \end{array} \right) = \frac{1}{D} \begin{array}{c} \text{white circle } \vec{k} \\ \text{grey circle } \vec{k}' \end{array} \stackrel{(9.40, 9.42)}{=} D \begin{array}{c} \text{white triangle } j \\ \text{grey triangle } i \end{array} \stackrel{(9.38)}{=} \text{dashed box}$$

Упражнение 9.84. Покажите, что равенства (9.64), (9.84), (9.88), (9.90) и (9.92) эквивалентны. (Указание и предупреждение: для доказательства некоторых утверждений нужно будет использовать тот факт, что если два отображения совпадают на базисе, то они равны. Но, как было сказано в замечании 5.11, в этом случае пренебрегать числами нельзя!)

Следствие 9.85. Каждое из равенств (9.84), (9.88), (9.90) и (9.92) – в паре с равенствами (9.65) – дает альтернативное определение сильной дополнителности.

Замечание* 9.86. Отметим, что мы решили включить равенство (9.89) в недублированной форме, с нетривиальной комплексной фазой. Тот факт, что фазовые отображения в (9.89) коммутативны только с точностью до фазы, – вариант канонических соотношений коммутирования (точнее, соотношений Вейля). Канонические соотношения коммутирования были первым инструментом, которым физики воспользовались для опробования дополнителности в квантовой теории.

В доказательстве предложения 9.83 мы обнаружили еще одно следствие сильной дополнителности, а именно что фазовые состояния в классической подгруппе «иммунны» к фазовым состояниям другого цвета.

Предложение 9.87. Для сильно дополнителных \circ и \bullet имеют место равенства:

Мы называем это *правилом k-исключения*.

Доказательство. Нужно просто продублировать и отразить равенство (9.91). \square

У предложения 9.83 также имеется старший брат, который утверждает, что фазовые отображения в классической подгруппе могут обходить фазы другого цвета.

Упражнение 9.88. Покажите, что для сильно дополнителных \circ и \bullet имеет место

где



– фазовые состояния для \circ и \bullet соответственно (как следует из обозначений).

Упражнение 9.89. Для сильно дополнительных \circ и \bullet покажите, что для любого \vec{k} функция $\vec{k}(-)$, определенная в упражнении 9.88, является гомоморфизмом групп, т. е.



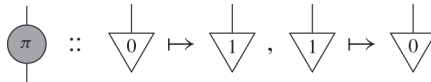
Покажите далее, что отображение

$$\vec{k} \mapsto \vec{k}(-)$$

является действием группы, т. е.



Пример 9.90. В двумерном случае классическая подгруппа состоит из двух элементов: 0 и π . Из упражнения 9.89 мы знаем, что 0 действует тривиально. В разделе 9.3.4 мы видели, что π действует как вентиль NOT для элементов \circ -базиса:



Следовательно, для \circ -фазовых состояний:

$$\pi \circlearrowleft \left(\begin{matrix} 1 \\ e^{i\alpha} \end{matrix} \right) \mapsto \left(\begin{matrix} e^{i\alpha} \\ 1 \end{matrix} \right) = e^{i\alpha} \left(\begin{matrix} 1 \\ e^{-i\alpha} \end{matrix} \right)$$

Таким образом, после дублирования π меняет знак фазы, т. е.

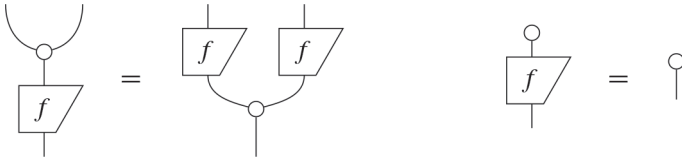
(9.94)

где второе равенство получается заменой ролей \circ и \bullet .

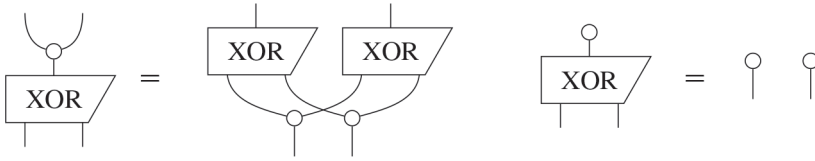
9.3.5. От пауков к отображениям четности

В предыдущей главе мы ввели пауков как операции над классическими данными. В этом разделе мы увидим, что сильная дополнительность дает много новых операций над классическими данными.

В предложении 8.19 мы встретились с характеристикой функциональных отображений как линейных отображений f , удовлетворяющих условиям:



В разделе 9.3.1 мы воспользовались этими равенствами, чтобы обосновать уравнения сильной дополнителности, когда в качестве f берется операция XOR:



которая возникает (с точностью до числа) как X -паук (см. предложение 5.88). Легко видеть, что этот путь к функциональным отображениям применим к любым сильно дополнителным парам пауков.

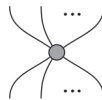
Предложение 9.91. Для сильно дополнителных \circ и \bullet



является функциональным отображением (с точностью до числа) для \circ .

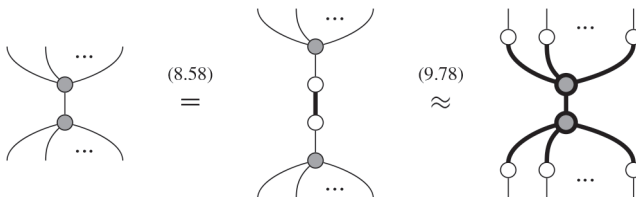
На самом деле если вспомнить, что функциональные отображения – это частный случай более общих классических отображений (см. раздел 8.2.1), то предыдущее предложение обобщается на всех \bullet -пауков.

Предложение 9.92. Для сильно дополнителных \circ и \bullet



является классическим процессом (с точностью до числа) для \circ .

Доказательство. Имеем:



Правая диаграмма состоит только из \circ -измерителя, \circ -кодировщика и чистых квантовых отображений, поэтому, по определению 8.3, она является КК-отобра-

жением и, в частности, классическим отображением (т. е. КК-отображением без квантовых входов-выходов). Поэтому \bullet -паук равен КК-отображению с точностью до числа. Поскольку это число положительно (см. замечание 9.36), этот \bullet -паук является КК-отображением. Каузальность следует из уравнения «обобщенного копирования» для сильно дополнительных пауков:

$$\begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} = \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \stackrel{(9.77)}{\approx} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \approx \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \begin{array}{c} \circ \\ \vdots \\ \circ \end{array} \quad \square$$

Мы сможем составить лучшее представление об этих новых классических процессах, посмотрев, что они делают на базисных состояниях и эффектах в двумерном случае. Для этого полезно рассматривать базисные состояния и эффекты как элементы, принадлежащие классической подгруппе:

$$\begin{array}{c} \downarrow \\ i \end{array} \approx \begin{array}{c} \bullet \\ \kappa \end{array} \qquad \begin{array}{c} \uparrow \\ i \end{array} \approx \begin{array}{c} \bullet \\ \kappa \end{array}$$

для $\kappa \in \{0, \pi\}$, так что:

$$\begin{array}{c} \triangleleft i'_1 \quad \triangleleft i'_2 \quad \dots \quad \triangleleft i'_n \\ \vdots \\ \bullet \\ \vdots \\ \triangleright i_1 \quad \triangleright i_2 \quad \dots \quad \triangleright i_m \end{array} \approx \begin{array}{c} \bullet \kappa'_1 \quad \bullet \kappa'_2 \quad \dots \quad \bullet \kappa'_n \\ \vdots \\ \bullet \\ \vdots \\ \bullet \kappa_1 \quad \bullet \kappa_2 \quad \dots \quad \bullet \kappa_m \end{array} = \sum \kappa_i + \sum \kappa'_i \quad (9.95)$$

Чтобы понять, какие из них отличны от нуля, нужно знать, какие «фазовые числа» (т. е. фазовые пауки без ног), взятые из классической подгруппы, не равны нулю.

Лемма 9.93. Для сильно дополнительных \circ и \bullet

$$\begin{array}{c} \bullet \\ \kappa \end{array} \neq 0 \iff \kappa = 0$$

где первый 0 означает нулевое число, а второй – единицу фазовой группы.

Доказательство. Возьмем в качестве (классического) \bullet -фазового состояния с фазой 0 первое состояние \circ -ОНБ (которое ниже помечено как '0'). Тогда

$$\begin{array}{c} \bullet \\ \kappa \end{array} = \begin{array}{c} \bullet \kappa \\ \bullet \end{array} \approx \begin{array}{c} \triangleleft i \\ \downarrow \\ \triangleright 0 \end{array}$$

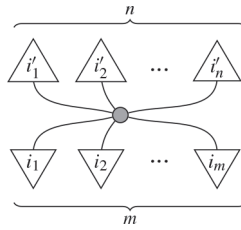
В силу ортонормированности это число отлично от нуля, только если $i = 0$, т. е. $\kappa = 0$. □

Таким образом, элемент матрицы отличен от нуля тогда и только тогда, когда

$$\sum_i \kappa_i + \sum_i \kappa'_i = 0.$$

В таком случае он равен некоторому положительному числу p .

Упражнение 9.94. Чему равно p , т. е. число



в терминах m и n ?

В двумерном случае классическая подгруппа равна \mathbb{Z}_2 (см. пример 9.76). Тогда групповая сумма равна 0 тогда и только тогда, когда количество единиц четно, так что

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \approx \sum_{i_1 \dots i_m i'_1 \dots i'_n} \oplus (i_1 \dots i_m i'_1 \dots i'_n) \begin{array}{c} \downarrow \quad \dots \quad \downarrow \\ \triangle_{i'_1} \quad \dots \quad \triangle_{i'_n} \\ \triangle_{i_1} \quad \dots \quad \triangle_{i_m} \\ \uparrow \quad \dots \quad \uparrow \end{array}$$

где \oplus – функция четности:

$$\oplus(i_1 \dots i_m i'_1 \dots i'_n) := \begin{cases} 1 & \text{если количество единиц четно} \\ 0 & \text{если количество единиц нечетно} \end{cases}$$

То есть в этой сумме встречаются только члены с четным количеством 1-состояний. Вот пример *четного состояния*:

(9.96)

Другой пример такого рода – *отображение четности*, которое возвращает 0-состояние, если количество 1-состояний четно, и 1-состояние, если оно нечетно:

(9.97)

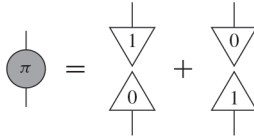
Если украсить \bullet -пауков числом π , то четность инвертируется, так что мы получаем:

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \approx \sum_{i_1 \dots i_m i'_1 \dots i'_n} \bar{\oplus}(i_1 \dots i_m i'_1 \dots i'_n) \begin{array}{c} \downarrow \quad \dots \quad \downarrow \\ \triangle_{i'_1} \quad \dots \quad \triangle_{i'_n} \\ \triangle_{i_1} \quad \dots \quad \triangle_{i_m} \\ \uparrow \quad \dots \quad \uparrow \end{array}$$

где $\overline{\oplus}$ – функция нечетности:

$$\overline{\oplus}(i_1 \dots i_m i'_1 \dots i'_n) := \begin{cases} 1 & \text{если количество единиц нечетно} \\ 0 & \text{если количество единиц четно} \end{cases}$$

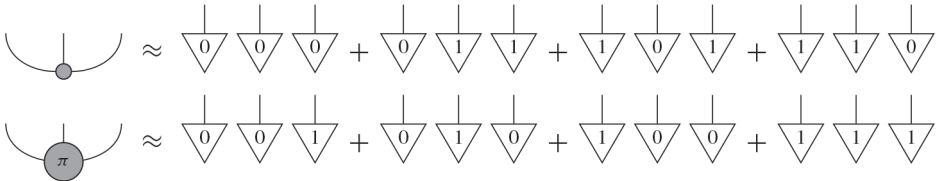
Частным случаем является классический вентиль NOT:



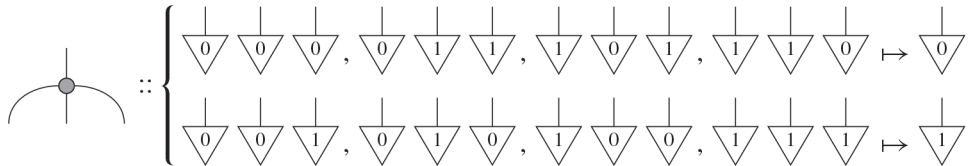
поскольку в каждом члене присутствует ровно одна 1. Другой пример – нечетное состояние:

(9.98)

Пример 9.95. В случае трех систем имеем:



Эти два частных случая в сочетании с трехсистемной функцией четности



будут играть важную роль в выводе квантовой нелокальности.

Помимо новых классических отображений, которые можно построить из ●-пауков, мы теперь можем построить еще больше, комбинируя ○-пауков и ●-пауков, например классический вентиль CNOT:



9.3.6. Классификация сильной дополнительности

В примере 9.44 мы подчеркнули, как мало на самом деле известно о классификации дополнительных измерений. Даже вопрос о том, сколько попарно дополнительных измерений существует в 6-мерном случае, остается открытым (точнее, черной дырой, которая затягивает специалистов по квантовой информатике).

где каждое $k_i = p_i^{n_i}$ для некоторого простого числа p_i и целого n_i , т. е. все k_i – степени простых чисел. Имея эту характеристику, мы точно знаем, как построить все сильно дополнителъные пары для любой размерности.

Пример 9.96. В двумерном случае существует только пара Z/X , которая соответствует циклической группе «четности» \mathbb{Z}_2 , тогда как для размерности 36 существует четыре различные сильно дополнителъные пары, соответствующие четырем способам разложить число 36 в произведение степеней простых чисел:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \quad \mathbb{Z}_4 \times \mathbb{Z}_9.$$

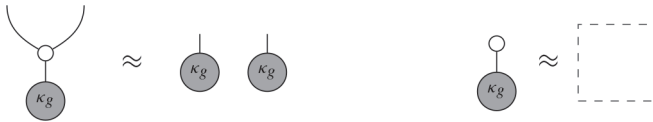
Что ж, прекрасно, сильно дополнителъные пары полностью классифицированы. Полезно ли это? Да! Из равенства (9.99), в частности, следует, что:



где $g + h$ и 0 – групповая операция и единица G соответственно. Поэтому G оказывается классической подгруппой, ассоциированной с сильно дополнителъной парой \circ/\bullet . То есть мы имеем множество \bullet -фаз:

$$\left\{ \begin{array}{c} | \\ \triangle \\ g \end{array} \right\}_{g \in G} \cong \left\{ \begin{array}{c} \bullet \\ \kappa_g \end{array} \right\}_{g \in G}$$

которое является классическим для \circ (с точностью до числа):



и кодирует G посредством \bullet :



А так как сильная дополнителъность симметрична относительно \circ/\bullet , то мы также получаем кодирование G в классической подгруппе \circ -фаз:



Таким образом, мы можем полностью закодировать эту группу (двумя способами), пользуясь сильно дополнителъной парой пауков. Теперь если мы захотим

изучить эту группу (а еще лучше – построить какие-нибудь квантовые процессы, которые изучат ее за нас!), то сможем воспользоваться этой парой пауков. Именно это мы и сделаем в разделе 12.2.4, где приведем квантовый алгоритм решения задачи о скрытой подгруппе.

Замечание 9.97. Внимательный читатель, вероятно, заметил, глядя на определение (9.99), что из обычного уравнения паука

$$\text{[Diagram: A cup with a dot on its bottom edge]} = \text{[Diagram: A simple cup]}$$

следует, что $g = -g$ для всех $g \in G$! Это, конечно, справедливо не для всех коммутативных групп, а только для групп вида:

$$\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_N$$

Когда $g \neq -g$, мы все равно получаем пауков, но необязательно соответствующих самосопряженным ОНБ (см. раздел* 8.6.3). В этом случае линейное отображение

$$\text{[Diagram: A square with a diagonal line and a dot]} := \text{[Diagram: A cup with a dot on its top edge]}$$

будет равно не простому проводу, а функциональному отображению, которое сопоставляет каждому элементу группы обратный к нему элемент. Это подробно обсуждается в разделе* 9.6.1.

9.4. ZX-исчисление

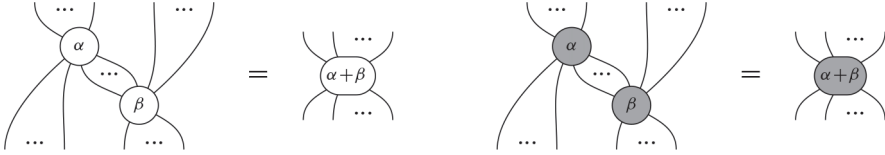
В этом разделе мы специализируем диаграммные создания и их взаимодействия, разработанные ранее в этой главе, на частный случай кубитов. В этом контексте возникают два вопроса:

- 1) какие КК-отображения можно выразить, используя только фазовых Z - и X -пауков? В частности, можно ли выразить все такие отображения?
- 2) какие равенства между КК-отображениями можно доказать с помощью *графического исчисления*, т. е. фиксированного набора диаграммных равенств, выбранных из тех, что мы уже встречали, и, возможно, каких-то новых?

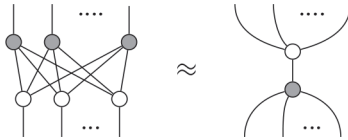
Ответ на первый вопрос – решительное да! Точнее, мы можем построить любое линейное отображение из m копий \mathbb{C}^2 в n копий \mathbb{C}^2 , используя только фазовых Z - и X -пауков. В частности, можно построить любое квантовое отображение кубитов только с помощью дублирования, а поскольку в нашем распоряжении имеются пауки, то можно также построить любое КК-отображение битов и кубитов.

Ответ на второй вопрос не столь уверенный – мы пока не знаем. Но это очень трудная задача. Однако если ограничить фазы кратными $\pi/2$, то получается важная подтеория **чистых квантовых отображений**, называемая теорией **отображений Клиффорда**. В главе 11 мы покажем, что подтеория **отображений Клиффорда** уже дает достаточно квантовых отображений для доказательства не-локальности квантовой теории.

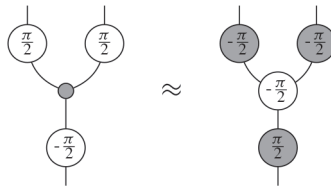
В этой процессной теории для доказательства всего на свете достаточно всего четырех равенств (технически четырех семейств равенств)! Первые два равенства говорят, как комбинируются пауки одного цвета. Это, конечно, просто (недублированные) правила слияния пауков, с которыми мы уже знакомы:



Третье равенство говорит, как пауки разного цвета могут коммутировать со слиянием:



что по теореме 9.71 эквивалентно строгой дополнителности. Четвертое равенство новое. Оно говорит, как преобразовать пауков одного цвета в пауков другого цвета:



Если остальные уравнения справедливы для сильно дополнительных пар при любой размерности, то это означает нечто специфическое для кубитов. Действительно, в следующем разделе мы увидим, что это правило тесно связано с геометрией сферы Блоха.

Интересно, что ключ к ответу на оба вопроса, касающихся квантового пикторализма, следует искать в литературе по квантовым вычислениям! В самом деле, первый вопрос оказывается связан с наборами квантовых вентилях, необходимыми для построения универсального вычислительного устройства, а для второго доказательство полностью опирается на результаты основанного на измерениях квантового вычисления.

Замечание 9.98. В этом разделе мы работаем почти исключительно с одиночными проводками. Это оставляет в нашем распоряжении самые универсальные из наших правил, т. к. частные случаи с участием квантовых и гибридных пауков можно получить сворачиванием и раскрытием квантовых проводков. Поэтому мы будем регулярно использовать недублированные версии (спасибо следствию 6.18) некоторых установленных ранее дублированных равенств. Отметим, что если не возникает недоразумений, то мы по-прежнему будем называть одиночные проводка, получающиеся раскрытием дублированных, кубитами.

9.4.1. ZX-диаграммы универсальны

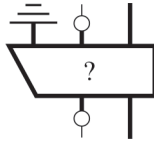
В преддверии специализации для кубитов определим новый тип диаграмм.

Определение 9.99. ZX-диаграммой называется струнная диаграмма, состоящая только из Z- и X-пауков:

$$\begin{array}{c} \text{Spider } \alpha \\ \text{with } \dots \text{ legs} \end{array} := \begin{array}{c} \downarrow 0 \dots \downarrow 0 \\ \uparrow 0 \dots \uparrow 0 \end{array} + e^{i\alpha} \begin{array}{c} \downarrow 1 \dots \downarrow 1 \\ \uparrow 1 \dots \uparrow 1 \end{array} \quad (9.100)$$

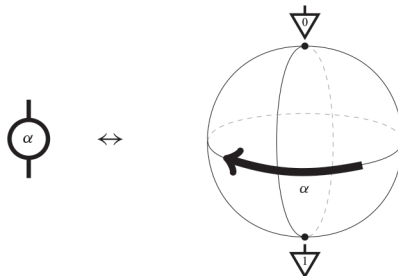
$$\begin{array}{c} \text{Spider } \alpha \\ \text{with } \dots \text{ legs} \end{array} := \begin{array}{c} \downarrow 0 \dots \downarrow 0 \\ \uparrow 1 \dots \uparrow 1 \end{array} + e^{i\alpha} \begin{array}{c} \downarrow 1 \dots \downarrow 1 \\ \uparrow 0 \dots \uparrow 0 \end{array} \quad (9.101)$$

Таким образом, для ZX-диаграмм разрешены не произвольные процессы, а только те, которые можно построить из этих двух видов фазовых пауков. Но вместо того чтобы рассматривать это как удаление всех остальных блоков из языка, мы можем считать это «заполнением блоков»:

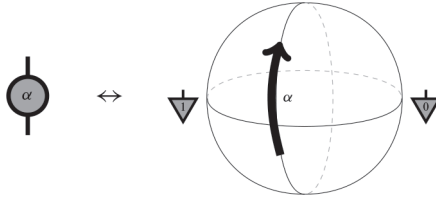


ZX-диаграммы гораздо выразительнее обычных струнных диаграмм или диаграмм с кружочками, поскольку у нас есть фазы и пауки двух цветов. В этом разделе мы увидим, что этого достаточно для построения любого чистого квантового отображения, переводящего кубиты в кубиты. Если еще добавить отбрасывание или (в более общем случае) гибридных пауков, то можно будет построить соответственно любое квантовое или КК-отображение (ку)битов.

Сначала покажем, как можно использовать ZX-диаграммы для конструирования произвольных унитарных отображений одного кубита. Напомним, что унитарные отображения кубитов соответствуют вращениям сферы Блоха. Мы уже знаем о двух весьма полезных семействах вращений: Z-фазовые вентили, которые дают повороты вокруг оси Z:

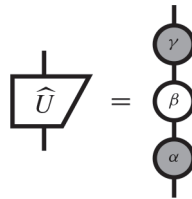


и X -фазовые вентили, дающие повороты вокруг оси X :



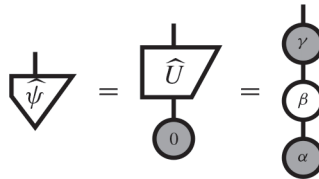
На самом деле известно, что любое вращение сферы можно представить в виде композиции трех поворотов относительно пары ортогональных осей. Применяя это свойство к унитарным квантовым отображениям, получаем следующий результат:

Предложение 9.100. Для любого унитарного квантового отображения \widehat{U} одного кубита существуют фазы α, β и γ такие, что \widehat{U} можно записать в виде:



Это называется *эйлеровым разложением* \widehat{U} , а фазы α, β, γ – углами Эйлера.

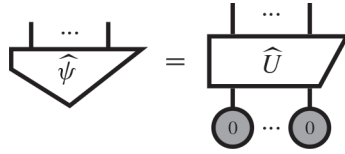
Поскольку мы можем выполнить любое унитарное отображение, возможно получить произвольное состояние одного кубита, начав с некоторого фиксированного состояния и преобразовав его в желаемое состояние $\widehat{\psi}$, которое теперь выражается в виде ZX-диаграммы, например:



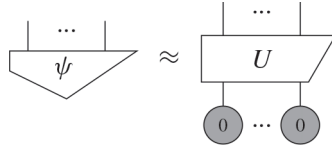
Раскрыв дублирование, мы увидим, что любое состояние в теории **линейных отображений** типа \mathbb{C}^2 можно выразить с точностью до числа (а именно глобальной фазы) в виде ZX-диаграммы. На самом деле это обобщается на состояния нескольких кубитов.

Предложение 9.101. Любое состояние в теории **линейных отображений** n копий \mathbb{C}^2 можно с точностью до числа выразить в виде ZX-диаграммы.

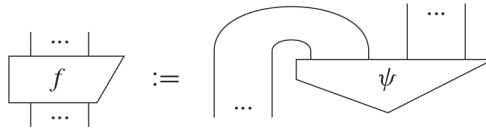
Мы отложим доказательство этой теоремы до раздела 12.1.3 главы о квантовых вычислениях, когда сможем заимствовать некоторые результаты из литературы по квантовым схемам. Точнее, в разделе 12.1.3 мы покажем, что с помощью ZX-диаграмм можно построить произвольное унитарное отображение \widehat{U} n кубитов, и, как и выше, сможем воспользоваться этим фактом для получения квантового состояния n -кубитов:



Раскрытие дублирования дает нам любое состояние с точностью до числа (см. следствие 6.18):

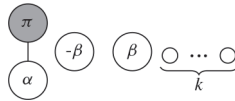


Затем, просто применив двойственность процессов и состояний к предложению 9.101, мы сможем также построить любое линейное отображение, для которого все входные и выходные провода имеют тип \mathbb{C}^2 :



Очевидно, что если ψ – ZX-диаграмма, то таковой является и f . Более того, мы можем получить все комплексные числа в виде ZX-диаграмм.

Предложение 9.102. Любое комплексное число можно выразить в виде ZX-диаграммы вида



для некоторых α, β и k .

Доказательство. Сначала заметим, что можно получить произведение любой комплексной фазы на $\sqrt{2}$ в виде:

$$\begin{array}{c} \pi \\ \circ \\ \alpha \end{array} \stackrel{(9.46)}{=} \sqrt{2} \begin{array}{c} 1 \\ \triangle \\ \alpha \end{array} \stackrel{(9.11)}{=} \sqrt{2} e^{i\alpha}$$

Поэтому достаточно показать, что можно выразить любое положительное вещественное число. Имеем:

$$\begin{array}{c} -\beta \\ \circ \end{array} \begin{array}{c} \beta \\ \circ \end{array} \stackrel{(9.100)}{=} (1 + e^{i\beta})(1 + e^{-i\beta}) = 1 + e^{i\beta} + e^{-i\beta} + 1.$$

Поскольку $e^{i\beta} = \cos \beta + i \sin \beta$ (см. раздел 5.3.1), это сводится к выражению

$$\begin{array}{c} -\beta \\ \circ \end{array} \begin{array}{c} \beta \\ \circ \end{array} = 2(1 + \cos \beta),$$

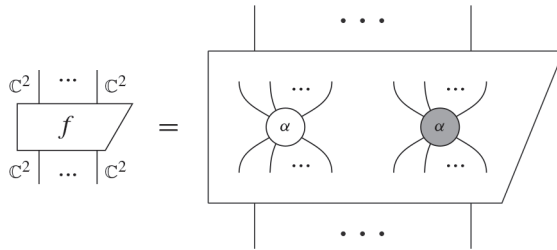
которое может принимать любое вещественное значение от 0 до 2. Для получения больших чисел просто увеличим количество кружочков:

$$\underbrace{(-\beta) \quad \beta \quad \underbrace{\circ \dots \circ}_k}_{k} = 2^{k+1}(1 + \cos \beta).$$

Таким образом, для любого вещественного положительного r можно сначала найти такое k , что $2^{k+1} \geq r$, а затем выбрать β . □

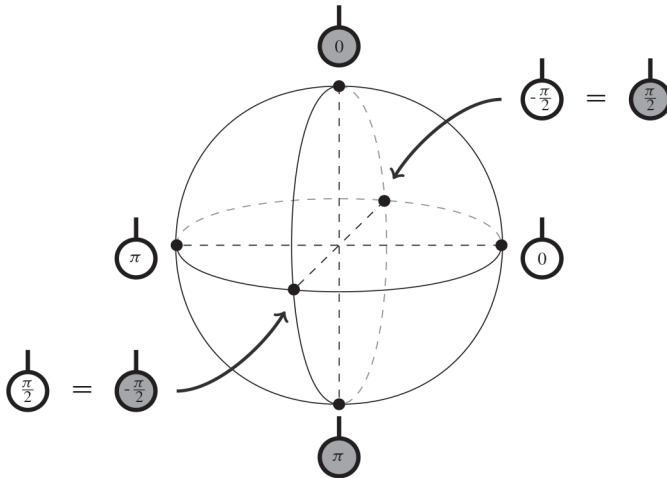
Отсюда вытекает следующая

Теорема 9.103. Любое линейное отображение, для которого все входные и выходные провода имеют тип \mathbb{C}^2 , можно выразить в виде ZX-диаграммы:



9.4.2. ZX-исчисление для диаграмм Клиффорда

Вместо того чтобы рассматривать весь кубит, мы можем сконструировать немало интересных состояний и процессов (на самом деле почти все встречавшиеся до сих пор), ограничившись только шестью репрезентативными состояниями на сфере Блоха, а именно состояниями, образующими Z-, X- и Y-базисы, которым соответствуют следующие фазовые состояния:



Поэтому фазовые группы тоже сводятся к четырехэлементной подгруппе \mathbb{Z}_4 группы $U(1)$:



Заметим, что каждое из этих состояний представимо как Z - или X -фазовое состояние с фазой, кратной $\pi/2$. Конечно, мы можем рассмотреть все такие ZX -диаграммы.

Определение 9.104. *Диаграммой Клиффорда* называется ZX -диаграмма, в которой фазы ограничены целыми кратными $\pi/2$.

Эти диаграммы определяют новую процессную теорию.

Определение 9.105. Теорией **отображений Клиффорда** называется подтеория теории **чистых квантовых отображений**, получаемая путем дублирования тех линейных отображений, которые можно выразить в виде диаграмм Клиффорда.

Как уже отмечалось, диаграммы Клиффорда допускают графическое исчисление, относительно которого теория **отображений Клиффорда** полна, т. е. существует такое множество равенств графического исчисления, что для любых двух равных (с точностью до числа) отображений Клиффорда одно из них можно преобразовать в другое, применяя только эти равенства.

На самом деле правил слияния пауков и сильной дополнителности уже почти достаточно. Почти, но не совсем, поскольку это общие правила, относящиеся ко всем квантовым системам, а не только к кубитам. Поэтому должно быть, по крайней мере, еще одно правило, которое четко дает понять, что мы имеем дело с кубитами. Этот недостающий ингредиент проистекает из того факта, что хотя в ZX -диаграмме присутствуют только Z -пауки и X -пауки, где-то там – благодаря фазам – скрывается также Y -базис, а значит, и Y -пауки. Существует ли какой-нибудь способ вытащить их наружу?

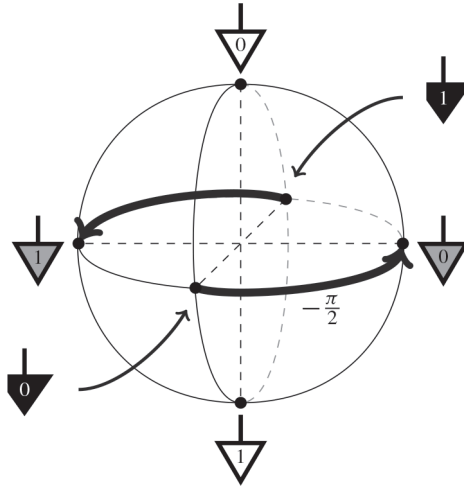
Как выясняется, достаточно придумать, как построить Y -копирующего паука, чтобы предоставить всю мощь ZX -исчисления в распоряжение диаграмм Клиффорда. В недублированной форме Y -базис можно записать в виде:

$$\left\{ \begin{array}{l} \sqrt{2} \begin{array}{c} \downarrow \\ 0 \end{array} = \begin{array}{c} \circ \\ \pi/2 \end{array} = e^{i\pi/4} \begin{array}{c} \circ \\ -\pi/2 \end{array} \\ \sqrt{2} \begin{array}{c} \downarrow \\ 1 \end{array} = \begin{array}{c} \circ \\ -\pi/2 \end{array} = e^{-i\pi/4} \begin{array}{c} \circ \\ \pi/2 \end{array} \end{array} \right. \quad (9.102)$$

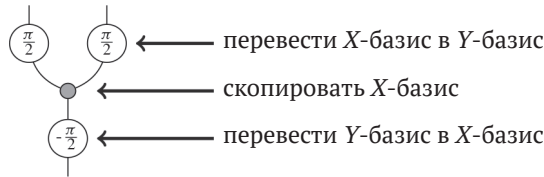
(Мы включили комплексные фазы явно, потому что им предстоит сыграть свою роль.)

Упражнение 9.106. Пользуясь конкретными определениями Y -базиса и фазовых Z - и X -пауков, докажите равенства (9.102) и, в частности, что комплексные фазы имеют именно такой вид.

Два способа выражения Y -базиса подсказывают два способа его копирования. Во-первых, поворот на угол $-\pi/2$ вокруг оси Z переводит Y -базис в X -базис:



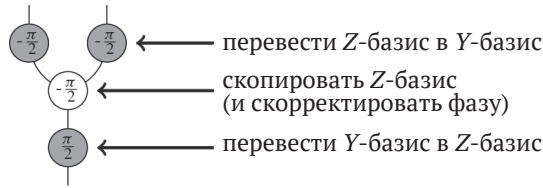
А поворот на угол $\pi/2$, конечно, переводит X -базис обратно в Y -базис. Поэтому один из способов скопировать Y -базис выглядит так:



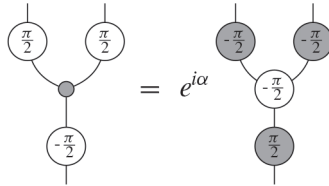
Увидеть это копирование в действии можно, подключив два состояния Y -базиса, записанных в виде \circ -фазовых состояний в соответствии с (9.102):

$$\begin{array}{l}
 \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \bullet \\ \circlearrowleft{-\frac{\pi}{2}} \\ \circlearrowleft{\frac{\pi}{2}} \end{array} = \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \bullet \\ \circ \end{array} \quad (9.68) = \frac{1}{\sqrt{2}} \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \circ \quad \circ \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \end{array} \\
 \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \bullet \\ \circlearrowleft{-\frac{\pi}{2}} \\ \circlearrowleft{-\frac{\pi}{2}} \end{array} = \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \bullet \\ \circlearrowleft{\pi} \end{array} \quad (9.85) = \frac{1}{\sqrt{2}} \begin{array}{c} \circlearrowleft{\frac{\pi}{2}} \quad \circlearrowleft{\frac{\pi}{2}} \\ \circlearrowleft{\pi} \quad \circlearrowleft{\pi} \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} \circlearrowleft{-\frac{\pi}{2}} \quad \circlearrowleft{-\frac{\pi}{2}} \end{array}
 \end{array}$$

Почти то же самое можно сделать с инвертированными цветами для \bullet -фаз, только надо исправить разность фаз между двумя ОНБ-состояниями. Из (9.102) мы видим, что эти фазы равны $e^{i\pi/4}$ и $e^{-i\pi/4}$ соответственно, поэтому разность составляет $\pi/2$. Мы можем учесть это, включив фазу $-\pi/2$ в \circ -паука:

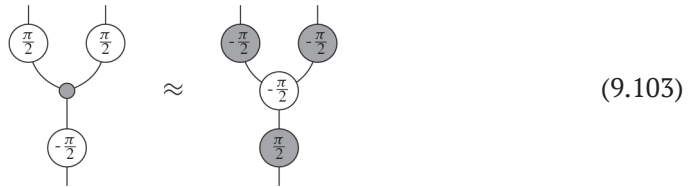


Упражнение 9.107. Путем вычислений на состояниях Y -базиса докажите, что

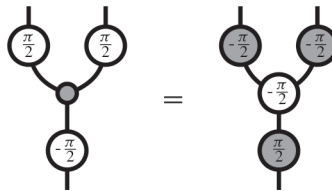


для некоторой фиксированной глобальной фазы $e^{i\alpha}$.

Отсюда следует, что

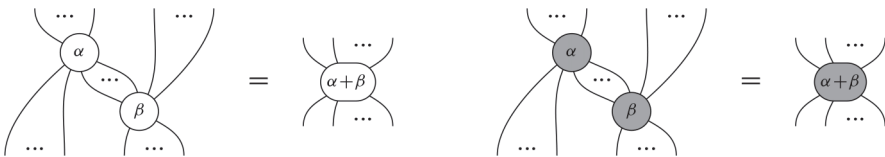


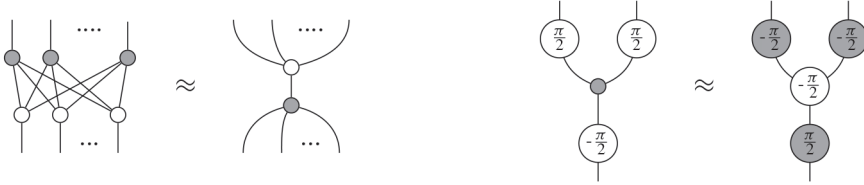
или, точнее (поскольку левая и правая части отличаются только глобальной фазой):



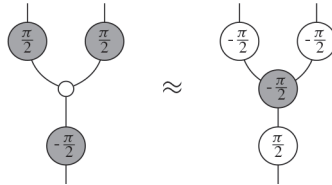
Добавив это Y -правило к тому, что мы уже знаем о сильно дополнительных парах пауков, получаем следующее определение.

Определение 9.108. ZX-исчисление для диаграмм Клиффорда состоит из следующих четырех правил:





Первое, что может вызвать удивление у части читателей, – тот факт, что четвертое правило, в отличие от встречавшихся ранее, несимметрично относительно \circ и \bullet . Эта асимметрия – всего лишь следствие стремления ограничиться минимальным набором правил, и в следующем разделе мы покажем, что в действительности ZX-исчисление симметрично относительно цветов, т. е. любое правило, которое в принципе можно доказать, доказуемо и с инвертированными цветами. Понятно, что для первых трех правил инверсия цветов ничего не меняет, поэтому нужно будет лишь доказать, что правило, получающееся цветовой инверсией Y-правила:



имеет место в ZX-исчислении.

Конечно, из предыдущих разделов мы уже многое знаем о ZX-исчислении. Например, поскольку, по теореме 9.71, третье правило эквивалентно сильной дополнителности, мы знаем, что можно доказать исходные уравнения сильной дополнителности:

(9.104)

(9.105)

а также уравнение дополнителности:

(9.106)

Эти частные случаи также явно показывают, что ZX-исчисление содержит равенства, позволяющие разъединять диаграммы. И это самые важные равенства, т. к. в основе своей ZX-диаграммы, как и все более простые виды диаграмм, встречавшиеся нам ранее, по-прежнему призваны отвечать на вопрос «что с чем соединено».

Как и в случае сильной дополнителности, есть несколько эквивалентных способов определить ZX-исчисление. В разделе 9.4.4 ниже мы построим вариант ZX-исчисления с существенно отличающимся четвертым правилом. На самом деле представленная выше версия в литературе никогда ранее не встречалась. Но, насколько мы знаем, это наименьший возможный набор правил. К тому же их очень легко запомнить, поскольку каждое правило сообщает ровно одну вещь о пауках, а именно:

- как комбинируются пауки одного цвета;
- как коммутируют пауки разных цветов;
- как преобразовать пауков одного цвета в пауков другого цвета.

В разделе 9.3.4 мы вывели ряд правил, относящихся к фазам в классической подгруппе, которая в случае кубитов состоит только из 0 и π . Когда мы выводили эти правила, мы, просто глядя на сферу Блоха, считали само собой разумеющимся, что состояния с фазой π для одного цвета являются базисными состояниями для другого цвета (с точностью до числа). Но, сохраняя верность нашему обету использовать для доказательства всего на свете только графическое исчисление, мы должны вывести этот факт, применяя лишь четыре правила, определяющих ZX-исчисление. Это возможно и будет продемонстрировано в следующем разделе.

Помимо «большой четверки» правил ZX-исчисления, нам еще понадобится несколько мелких правил для исключения ненулевых чисел:

$$\circ = \bullet = \text{шарик } \alpha \text{ с линией сверху} = \text{шарик } \alpha \text{ с линией снизу} \approx \square \text{ (9.107)}$$

Применяя такую же технику, как в упражнении 9.62, мы можем показать, что эти числа могут быть равны нулю, только когда все пауки уже нулевые.

9.4.3. ZX-исчисление для додо: только диаграммы и ничего более

Теперь, когда мы определили ZX-исчисление, наша цель – доказать все остальное в этой главе, используя только эти правила и ничего более. Это позволит составить полное представление о том, как ZX-исчисление выглядит «в действии». Начнем с легкой разминки.

Предложение 9.109. ZX-исчисление подчиняется следующим правилам:

$$\begin{matrix} \text{шарик } \alpha \text{ с линией сверху} \\ \approx \\ \text{шарик } \alpha \text{ с линией снизу} \end{matrix} \quad \begin{matrix} \text{шарик } \alpha \text{ с линией сверху} \\ \approx \\ \text{шарик } \alpha \text{ с линией снизу} \end{matrix} \quad \text{(9.108)}$$

Доказательство проводится в основном так же, как для (9.91), с применением правила «не нуля» в конце:

(9.105)

Для варианта с инвертированными цветами все аналогично. Поскольку использование слияния фазовых пауков обычно очевидно, мы не будем явно указывать этот шаг. \square

Далее мы покажем, как появляются на свет равенства (9.102), которые были у нас отправной точкой для конструирования четвертого правила.

Предложение 9.110. ZX-исчисление подчиняется следующим правилам:

(9.109)

Доказательство. Если взять частичный след обеих частей Y-правила:

(9.110)

то левая часть сводится к

(9.106), (9.107, 9.108)

а правая часть – к

(9.106), (9.107)

Затем применение \bullet -фазы $\pi/2$ к обеим частям дает первое из равенств (9.109):

(9.110)

Второе равенство можно получить, применив сопряжение к обеим частям, в результате чего знаки меняются на противоположные. \square

Теперь покажем, что в ZX-исчислении можно вывести все правила с участием фаз π из раздела 9.3.4 (при условии что мы ограничиваемся фазами, кратными $\pi/2$). Главное – мы должны показать, что π -фазовые состояния действительно являются базисными. Начнем с правила π -коммутирования.

Предложение 9.111. ZX-исчисление подчиняется правилу π -коммутирования:

$$\begin{array}{c} \bullet \\ \alpha \\ \bullet \\ \pi \end{array} \approx \begin{array}{c} \bullet \\ \pi \\ \bullet \\ -\alpha \end{array} \tag{9.111}$$

для $\alpha \in \{0, \pi/2, \pi, -\pi/2\}$.

Доказательство. Вычислив левую часть Y-правила на \bullet -состоянии, получаем:

$$\begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \approx \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \end{array} \approx \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \tag{9.108}$$

а проделав то же самое с правой частью, получаем:

$$\begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \approx \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \approx \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \approx \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ \pi \end{array} \tag{9.109}$$

откуда заключаем, что

$$\begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \approx \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ \pi \end{array} \tag{9.112}$$

Разгибание провода дает

$$\begin{array}{c} \bullet \\ \pi \end{array} \approx \begin{array}{c} \bullet \\ \pi/2 \end{array} \begin{array}{c} \bullet \\ \pi/2 \end{array} \approx \begin{array}{c} \bullet \\ -\pi/2 \end{array} \begin{array}{c} \bullet \\ \pi \end{array} \begin{array}{c} \bullet \\ -\pi/2 \end{array} \tag{9.112}$$

Затем применяем $\pi/2$ -фазовый \bullet -вентиль к выходу:

(9.113)

т. е. (9.111) для $\alpha := \pi/2$. Вентили с другими фазами можно просто разложить в последовательность $\pi/2$ -фазовых вентилей, например для $\alpha := \pi$ имеем:

□

Упражнение 9.112. Покажите, что если в начале приведенного выше доказательства проводить вычисление на \circ -состоянии, а не на \bullet -состоянии, то получится равенство

(9.114)

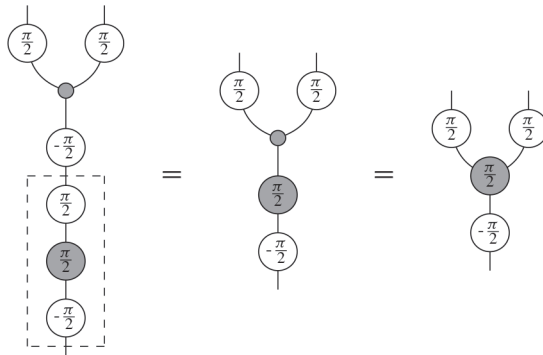
Этих равенств достаточно, чтобы доказать цветовую симметрию ZX-исчисления.

Теорема 9.113. ZX-исчисление подчиняется следующему правилу:

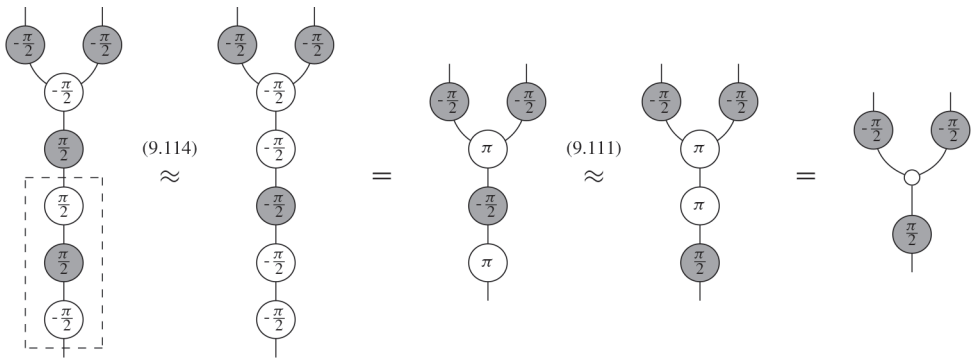
(9.115)

Поэтому любое равенство, доказуемое в ZX-исчислении, справедливо и после инверсии цветов.

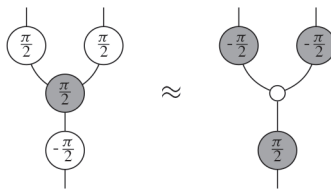
Доказательство. Применение последовательности фазовых вентилей к левой части Y-правила дает:



Применение тех же фазовых вентилей к правой части дает:



где на первом шаге мы применили сопряжение к обеим частям (9.114), чтобы изменить знаки. Таким образом, получаем:



и применение сопряжения к обеим частям завершает доказательство. □

Упражнение 9.114. Воспользуйтесь правилом π -коммутирования, чтобы доказать правило π -исключения:



для $\alpha \in \{0, \pi/2, \pi, -\pi/2\}$. Затем докажите вариант этого правила с инверсией цветов:

(9.117)

Следующее важное правило, касающееся разъединения диаграмм, нам еще не встречалось.

Предложение 9.115. ZX-исчисление подчиняется следующему правилу $\pi/2$ -дополнительности:

(9.118)

Доказательство. Прежде всего имеем:

Затем применение $\pi/2$ -фазовых вентиляй дает:

□

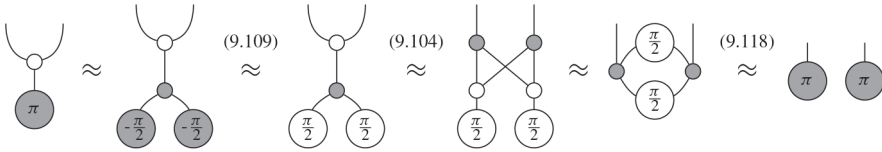
Замечание 9.116. Употребление термина «дополнительность» выше относится к тому факту, что $(\pi/2, \pi/2)$ – пара *дополнительных* углов, т. е. углов, в сумме составляющих π (или 180°). В разделе 9.4.6 мы встретимся с обобщением этого правила.

Наконец, мы достигли поставленной цели: пользуясь только ZX-исчислением, показать, что \bullet -состояние с фазой π является базисным состоянием для \circ (и наоборот – посредством инверсии цветов)

Предложение 9.117. ZX-исчисление подчиняется правилу π -копирования:

(9.119)

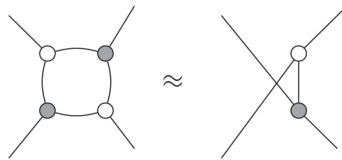
Доказательство. Имеем:



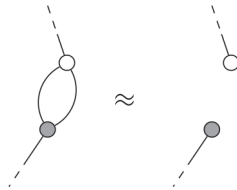
Здесь четвертый шаг может показаться неочевидным, но на самом деле это просто применение правила слияния \circ -фазовых пауков. \square

9.4.4. ZX для профессионалов: строим собственное исчисление

Вскоре мы увидим, что четырех правил из определения 9.108 достаточно для доказательства всех фактов, касающихся диаграмм Клиффорда. Однако это не обязательно означает, что это самый удобный из возможных наборов правил. Например, человеку, привыкшему к традиционным алгебраическим структурам, правила с большим количеством входов и выходов могут показаться очень громоздкими, а правила алгебры Фробениуса, которые мы обсуждали в разделе* 8.6.1, – куда более привлекательными, чем слияние пауков. (Читатель: вы, наверное, шутите? Мы: ничуть.) И тот же человек сочтет три определяющих правила сильной дополнителности более удобными, чем одно правило, в которое мы их упаковали. И дело не только в испорченности традиционной алгеброй, просто кому-то может показаться более симпатичным иметь примитивное правило удаления 4-циклов:

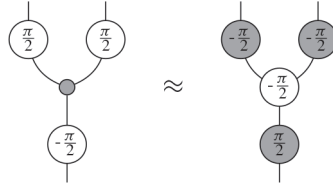


которое мы использовали с самого начала для обоснования сильной дополнителности. Из тех же соображений кому-то, возможно, больше нравится использовать в качестве примитива дополнителность, а не сильную дополнителность:



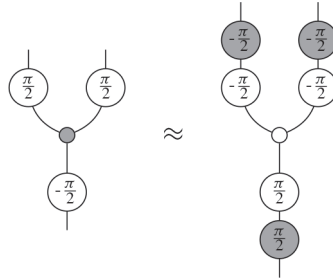
и составить новую комбинацию правил, из которой будет следовать сильная дополнителность. Почему бы и нет? Все мы разные.

В этом разделе мы выведем эквивалентную версию ZX-исчисления, в которой Y -правило

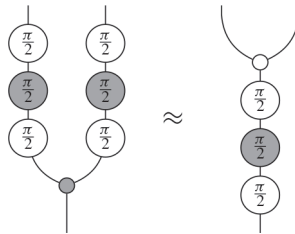


будет заменено правилом, симметричным относительно двух цветов. В предыдущем разделе мы уже проделали кое-какую работу, чтобы показать, что если некое правило имеет место в ZX-исчислении, то имеет место и правило с инвертированными цветами. Наше новое правило будет явно отражать эту цветовую симметрию посредством «переключателя цветов», который мы сконструируем из фазовых вентиляей.

Сначала, применив толику слияния фазовых пауков, получаем:



Затем, применив $\pi/2$ -фазовые вентили к обеим частям, избавимся от всех знаков «минус»:



На первый взгляд кажется, что стало только хуже. Но если положить

$$\square := \begin{array}{c} \circlearrowleft \frac{\pi}{2} \\ \circlearrowright \frac{\pi}{2} \\ \circlearrowleft \frac{\pi}{2} \end{array} \tag{9.120}$$

то получим

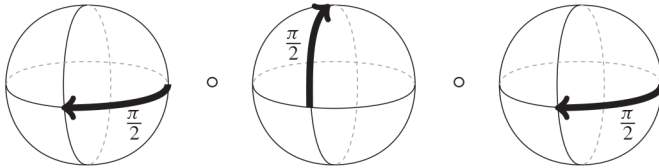
(9.121)

Таким образом, мы получили простое правило, которое говорит, что маленький белый квадратик проходит через копирующих пауков и изменяет их цвет. Ага! Похоже, мы нашли кандидата на роль переключателя цветов!

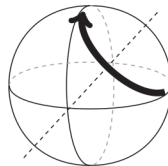
Но что это за таинственный квадратик? Понять это поможет геометрия. Взгляните на соответствующее квантовое отображение:



Будучи интерпретировано как вращения сферы Блоха, оно дает:



Читатели с развитым пространственным воображением увидят, что это сводится к повороту на 180° :

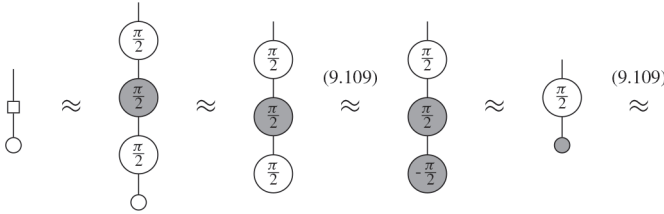


Ну а тем, кто пространственным воображением обделен, советуем найти какой-нибудь шарик и попробовать, или, если у вас, как у додо, нет противопоставленных больших пальцев, то можете воспользоваться ZX-исчислением и показать, что маленький белый квадратик переводит состояния X-базиса в состояния Z-базиса.

Предложение 9.118. ZX-исчисление подчиняется следующим правилам:

(9.122)

Доказательство. Имеем:



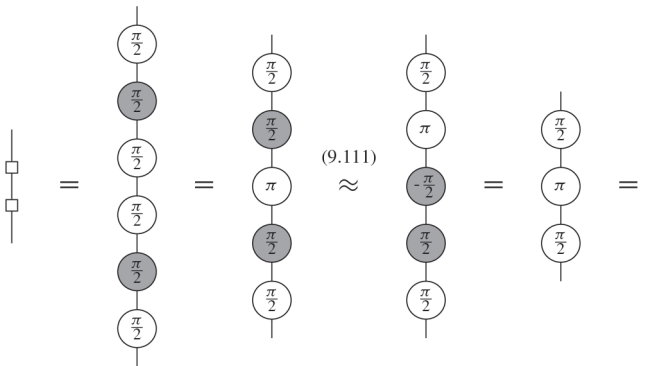
и аналогично для другого базисного состояния. □

Белый квадратик дает поворот на 180° , поэтому если мы проделаем это дважды, то вернемся туда, откуда начали, т. е. это отображение обратно самому себе. Читатели, подобные додо, снова могут убедиться в этом с помощью ZX-исчисления.

Предложение 9.119. ZX-исчисление подчиняется следующему правилу:

(9.123)

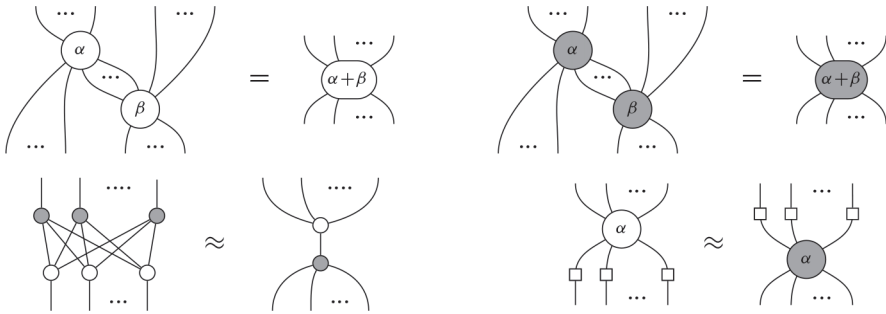
Доказательство. Одно применение правила π -коммутирования и несколько слияний пауков дают:



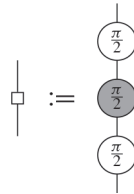
Итак, белый квадратик меняет местами состояния Z - и X -базиса и является самообратным. Ничего не напоминает? В самом деле:

Наш белый квадратик и линейное отображение Адамара, с которым мы впервые встретились в разделе 5.3.5, отличаются только глобальной фазой. Поэтому то и другое обычно называют вентиляем Адамара, или H -вентилем. Итак, мы подошли к кульминации.

Теорема 9.120. ZX-исчисление можно эквивалентно представить в виде:



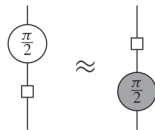
где



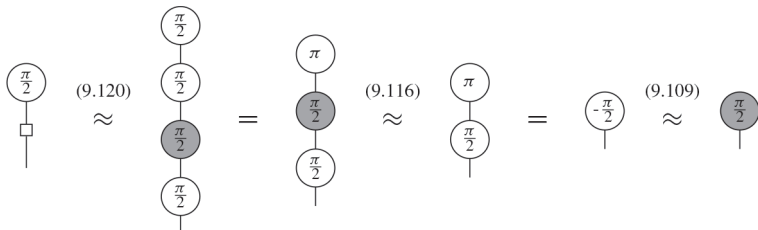
Доказательство. Поскольку любого \circ -фазового паука в диаграмме Клиффорда можно построить из следующих кусочков:



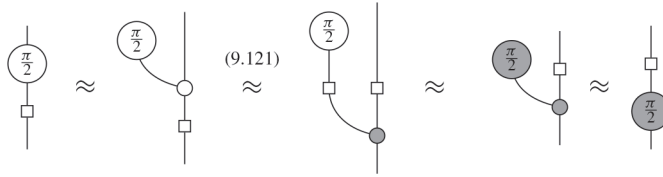
то, чтобы заменить целого \circ -фазового паука \bullet -фазовым пауком, нам нужны только правила проталкивания H -вентилей сквозь каждый из этих кусочков. Правила (9.121) и (9.122) вместе с их цветоинвертированными вариантами дают все необходимое, кроме



Чтобы доказать это, сначала заметим, что

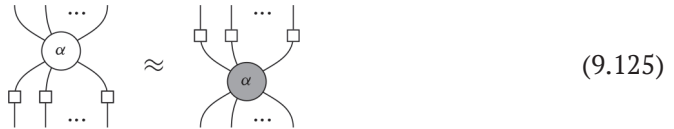


а затем используем приведенное выше на третьем шаге:



Обратно, равенство (9.121) является частным случаем правила изменения цвета. Раскрывая определение переключателя цветов и выполняя манипуляции с фазами, описанные в начале этого раздела, в обратном порядке, мы видим, что из (9.121) вытекает Y-правило. □

Новое правило



будем называть *правилом изменения цвета*.

9.4.5. ZX для богов: полнота

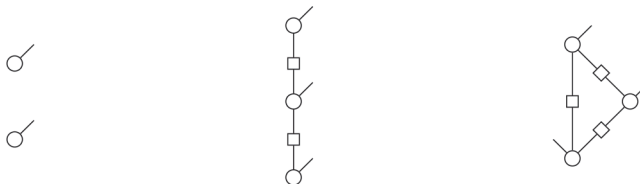
Конечная цель жизни, Вселенной и вообще всего на свете, конечно, состоит в том, чтобы заменить отвратительные символичные манипуляции диаграммами. И насколько ZX-диаграммы приблизили нас к *последнему рубежу*? Как уже было сказано, мы пока не знаем. Но вот что мы знаем точно, так это то, что в ограниченном случае ZX-исчисления для диаграмм Клиффорда эта цель фактически достигнута. Иначе говоря, пока речь идет о выводе равенств между диаграммами Клиффорда, мы можем вообще забыть о том, что эти диаграммы когда-то имели что-то общее с линейными отображениями, и просто пользоваться графическим исчислением. И доставит нас в эту точку следующая концепция, которая послужит нам флагманом «Энтерпрайз».

Определение 9.121. *Графовым состоянием* называется состояние, ZX-диаграмма которого состоит только из (неукрашенных) \circ -пауков и H -вентилей, где:

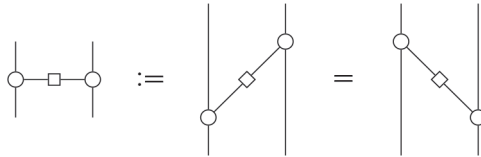
- 1) у каждого \circ -паука имеется ровно один выход;
- 2) все провода, кроме выходных, соединяют двух \circ -пауков с одним H -вентилем.

Поскольку у любого \circ -паука ровно один выход, мы можем точно описать квантовые системы с \circ -пауками. Тогда ребра представляют способ запутывания систем друг с другом в ассоциированном квантовом состоянии. В главе 12 мы увидим, что *квантовые графовые состояния*, полученные дублированием графовых состояний, образуют базис *основанной на измерениях* модели квантового вычисления.

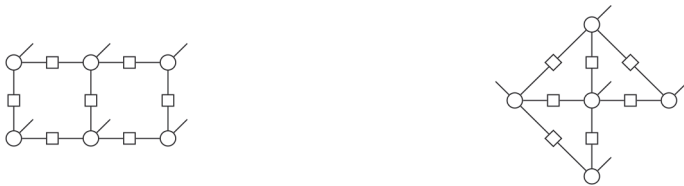
Вот несколько примеров квантовых состояний:



Отметим, что для большей ясности мы обычно не продолжаем выходные провода до верха и не всегда рисуем их вертикально. Кроме того, поскольку H -вентиль самотранспонированный, нет нужды различать его вход и выход. Поэтому мы можем рисовать H -вентили на горизонтальных или наклонных проводах, не опасаясь неоднозначности:



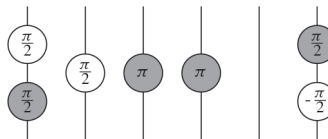
Это удобно, когда приходится рисовать более сложные графовые состояния:



Описанные состояния называются «графовыми», потому что они однозначно определяются базовым (неориентированным) графом, т. е. множеством вершин, соединенных ребрами, который говорит, куда помещать \circ -пауков и провода с H -вентиллями:



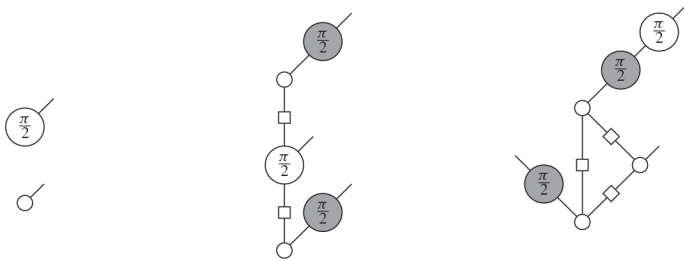
Нам графовые состояния полезны, потому что они лежат в основе хорошо ведущей себя канонической формы диаграмм Клиффорда. В этой канонической форме также принимают участие *локальные унитарные отображения Клиффорда*, т. е. унитарные отображения, которые можно выразить в виде параллельной композиции односистемных диаграмм Клиффорда, например:



Замечание 9.122. Поскольку локальные унитарные отображения Клиффорда воздействуют на системы по отдельности, они не влияют на запутывание систем. Поэтому когда мы рассматриваем графовое состояние как *ресурс запутывания*, локальные унитарные отображения Клиффорда не изменяют его сколько-нибудь существенным способом. Подробно мы обсудим эту концепцию в разделе 13.3.

Чтобы получить каноническую форму, мы сначала воспользуемся двойственностью процессов и состояний для преобразования произвольной диаграммы Клиффорда в состояние. А к этим состояниям Клиффорда мы затем применим следующий результат.

Предложение 9.123. Любое состояние Клиффорда можно с помощью ZX-исчисления преобразовать в графовое состояние, за которым следуют локальные унитарные отображения Клиффорда, например:



Это называется *графовой формой* диаграммы Клиффорда.

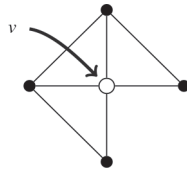
Мы не станем приводить полное доказательство этой теоремы, но опишем основные его этапы. Сначала с помощью правила слияния пауков входящие в диаграмму Клиффорда пауки разлагаются в конечное множество «паучат» – таких, как изображены в (9.124), и их \bullet -аналогов. Затем доказательство проводится индукцией по «паучатам». После добавления нового типа «паучонка» в диаграмму Клиффорда в графовой форме результат снова можно преобразовать в графовую форму.

Поскольку мы можем преобразовать любую диаграмму Клиффорда в графовую форму, нужно только показать, что ZX-исчисления достаточно для доказательства равенства между диаграммами в графовой форме. Давайте загрузим немного антиматерии в варп-двигатель.

Определение 9.124. Для неориентированного графа G и его вершины v *локальным дополнением* G в v (обозначается $G \star v$) называется граф, полученный путем дополнения всех пар w, w' вершин, смежных с v , где под дополнением понимаются следующие действия:

- если существует ребро, соединяющее w с w' , удалить его, а
- если не существует ребра, соединяющего w с w' , добавить его.

Определение довольно хитрое, поэтому рассмотрим пример. Возьмем граф и его вершину v , изображенную в виде белого кружочка:



Смежными с v являются вершины, соединенные с v ребром, они изображены белым цветом на рисунке ниже:

где

$$\alpha_i = \begin{cases} \pi/2 & \text{если } v_i \text{ смежна с } v_j \\ 0 & \text{в противном случае} \end{cases}$$

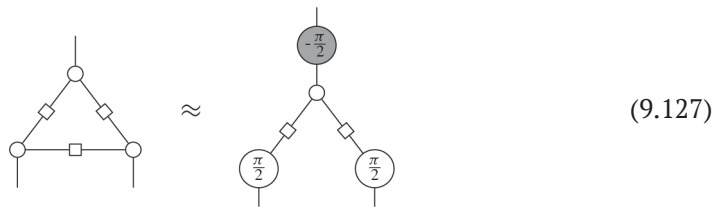
В частности, применение правила локального дополнения (9.126) переводит диаграмму Клиффорда в графовой форме в другую диаграмму Клиффорда в графовой форме, представляющую то же состояние. Удивительно, что таким образом можно получить любую графовую форму, представляющую данное состояние.

Предложение 9.126. Две диаграммы Клиффорда в графовой форме представляют одно и то же состояние тогда и только тогда, когда одну можно преобразовать в другую, применяя правило локального дополнения (9.126) и правила ZX-исчисления к локальным унитарным отображениям Клиффорда.

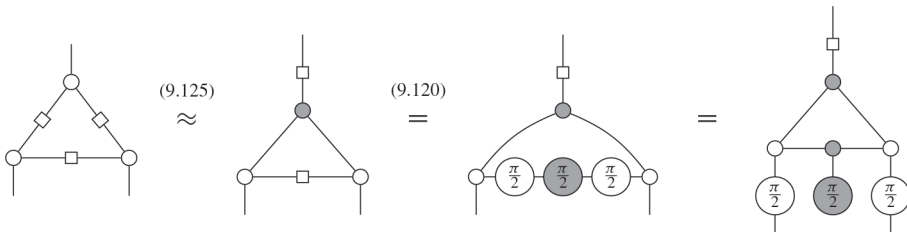
Доказательство этой, весьма содержательной теоремы мы снова опустим. Но запомните на будущее: применяя правило локального дополнения, мы можем решить, равны ли две графовые формы, с помощью преобразования диаграмм. В сочетании с предложением 9.123 это означает, что если мы сможем вывести правило локального дополнения в ZX-исчислении, то сможем и доказать любое равенство между отображениями Клиффорда.

И в качестве грандиозного графического финала мы таки выведем правило локального дополнения, пользуясь ZX-исчислением. Начнем с простенькой леммы.

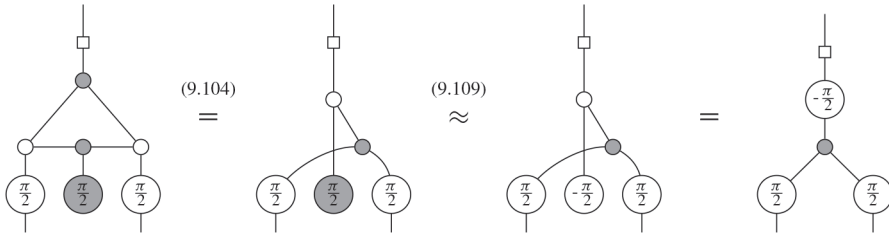
Лемма 9.127. ZX-исчисление подчиняется следующему правилу:



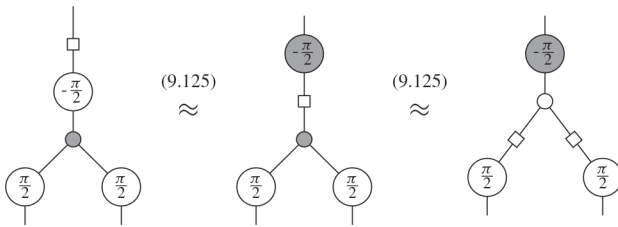
Доказательство. Сначала поднимем вверх H -вентиль:



затем воспользуемся сильной дополнительностью:

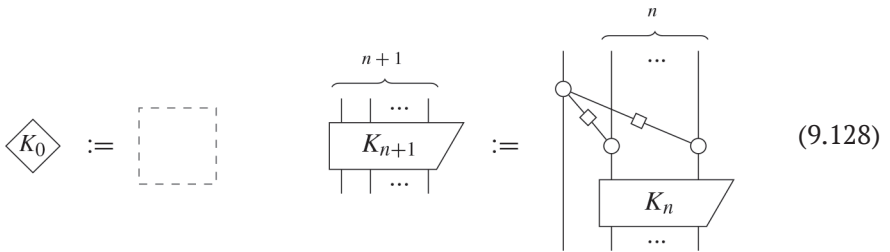


и, наконец, опустим H -вентиль:

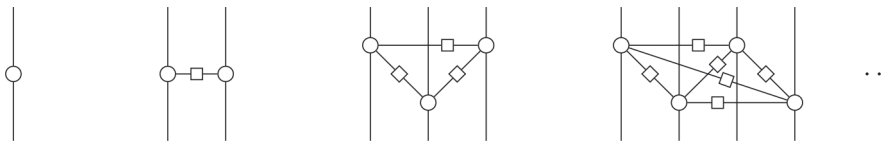


□

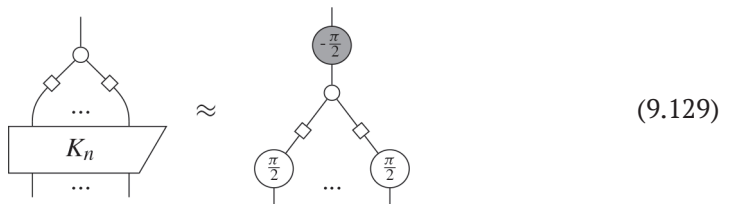
Следующая лемма обобщает предыдущую. Обозначим K_n ZX-диаграмму, рекурсивно определенную следующим образом:



Благодаря слиянию пауков это определение дает ряд вертикальных проводов, присоединенных к локально связным графам с H -ребрами:



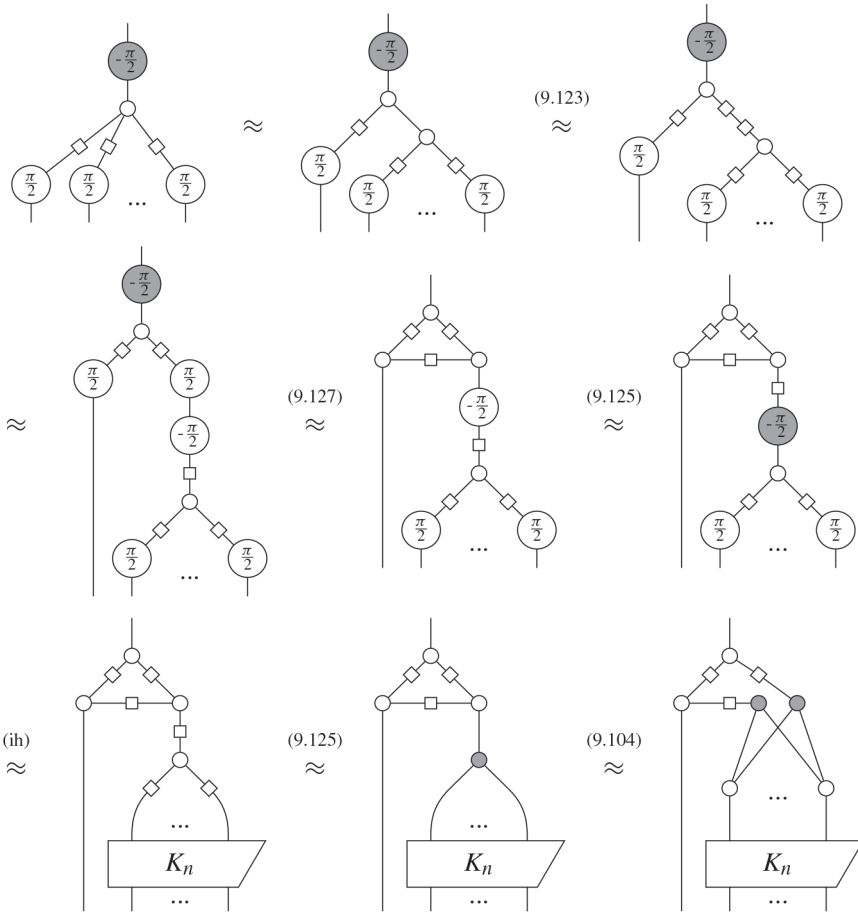
Лемма 9.128. ZX-исчисление подчиняется следующему правилу:

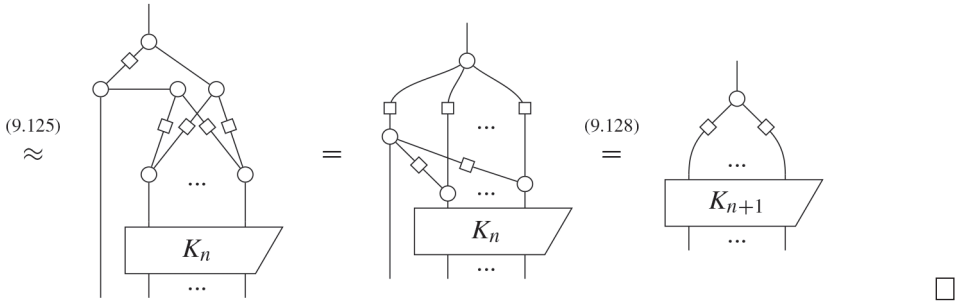


Доказательство проведем индукцией по n . Для $n = 0$ утверждение принимает вид:

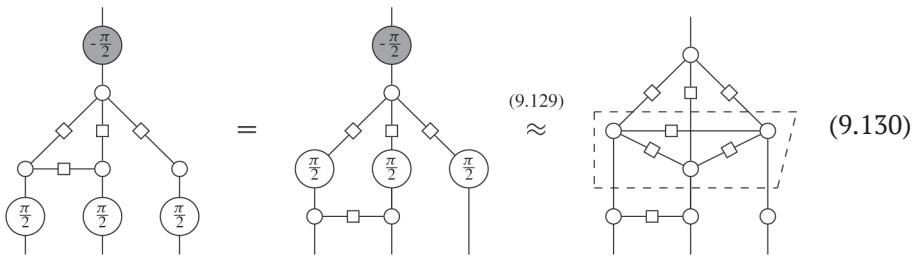
$$\begin{array}{c} | \\ \circ \end{array} \stackrel{(9.108)}{\approx} \begin{array}{c} | \\ \textcircled{-\frac{\pi}{2}} \\ | \\ \circ \end{array}$$

Предположим далее, что (9.129) справедливо для некоторого n , и ниже будем обозначать соответствующее равенство (ih). Тогда – соберитесь с духом! – в силу следующей цепочки равенств оно справедливо и для $n + 1$:

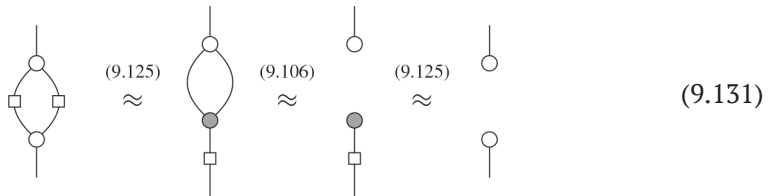




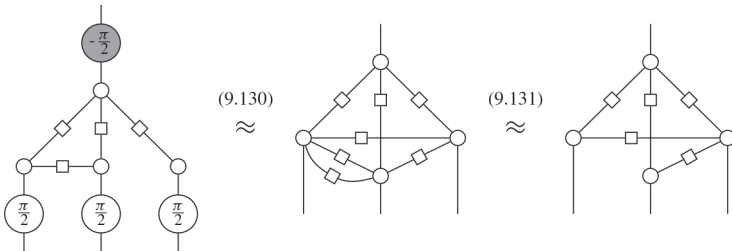
И что же говорит нам эта лемма? А говорит она, что путем применения \bullet -фазового вентиля с фазой $-\pi/2$ к вершине v_i графового состояния и \circ -фазового вентиля с фазой $\pi/2$ ко всем ее соседям, как в правой части правило локального дополнения (9.126), мы вводим новое H -ребро между каждой парой соседей v_j :



Но тогда, как и в случае дополнительных пауков, пары H -ребер в графовых состояниях взаимно уничтожаются:



и в итоге получается локальное дополнение в вершине v_j :



Готово! Мы вывели правило локального дополнения, не пользуясь ничем, кроме четырех скромных правил из определения 9.108. Собирая все вместе, мы приходим к следующему выводу.

Теорема 9.129. ZX-исчисление полно относительно **отображений Клиффорда**, т. е. для любых двух диаграмм Клиффорда D, E следующие утверждения эквивалентны:

- равенство $D = E$ выводимо в ZX-исчислении и
- ассоциированные отображения Клиффорда $\llbracket D \rrbracket$ и $\llbracket E \rrbracket$ равны с точностью до числа.

Мы также можем сформулировать утверждение, аналогичное имеющему место для струнных диаграмм и диаграмм с кружочками, при условии что две диаграммы Клиффорда считаются «одинаковыми», если одну можно преобразовать в другую средствами ZX-исчисления:

между отображениями Клиффорда имеет место равенство тогда и только тогда, когда диаграммы Клиффорда одинаковы.

9.4.6. Что нам дало полное ZX-исчисление

Хотя отображения Клиффорда уже демонстрируют много квантовых особенностей, есть, по меньшей мере, одна причина для рассмотрения более общих ZX-диаграмм. Хорошо известно, что диаграммы Клиффорда (или, точнее, их унитарные родственники – квантовые схемы Клиффорда) допускают эффективное классическое моделирование. То есть если подать на вход отображения Клиффорда некоторое фиксированное состояние и измерить выходы, то можно написать программу для классического компьютера, которая эффективно вычислит вероятности по правилу Борна. Поэтому если мы хотим построить квантовый компьютер, то отображения Клиффорда не дадут нам ничего нового. Мы еще вернемся к обсуждению этого вопроса в главе 12.

С другой стороны, добавив в диаграммы Клиффорда всего одну фазу, мы получим не в пример больше.

Определение 9.130. *Диаграммой Клиффорда+T* называется ZX-диаграмма, в которой фазы ограничены целыми кратными $\pi/4$, теорией **отображений Клиффорда+T** – соответствующая подтеория теории **чистых квантовых отображений**.

Странное название связано с тем, что в литературе по квантовым вычислениям \circ -фазовый вентиль с фазой $\pi/4$ часто называется *T-вентилем*. С практической точки зрения, добавление фазы $\pi/4$ дает нам все необходимое в том смысле, что позволяет подойти сколь угодно близко к желаемой цели.

Теорема 9.131. *Диаграммы Клиффорда+T приблизительно универсальны.* Это значит, что любое линейное отображение можно со сколь угодно высокой точностью аппроксимировать диаграммой Клиффорда+T.

Мы уже знаем, что ZX-диаграммы позволяют построить любой квантовый процесс, а теперь узнали, что даже диаграммы Клиффорда+T дают возможность построить практически любой процесс. И что можно сказать об этих более функционально богатых диаграммах?

При переходе от диаграмм Клиффорда к произвольным ZX-диаграммам мы первым делом замечаем, что некоторые правила, доказанные для $\alpha \in \{0, \pi/2, \pi, -\pi/2\}$, обобщаются на произвольные фазы. Например, очевидно, что применение *H*-вентилей к каждой ноге фазового паука изменяет его цвет вне зависимости от значения α . Следовательно, равенство

(9.132)

справедливо для всех α . Аналогично равенство

(9.133)

тоже справедливо для всех α .

На самом деле если добавить эти два правила в ZX-исчисление, то мы получим несколько улучшенную полноту для всех ZX-диаграмм.

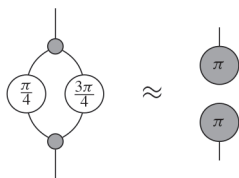
Теорема 9.132. ZX-исчисление, пополненное правилами (9.132) и (9.133), полно для **однокубитовых отображений Клиффорда+T**, т. е. отображений вида



На первый взгляд, не так уж много, но это только начало. А не получится ли так, что эта новая расширенная версия ZX-исчисления будет полна относительно всех диаграмм Клиффорда+T?

К сожалению, нет. Как и у двух вышеприведенных правил, у правила $\pi/2$ -дополнительности есть старший брат, имеющий место (почти) для всех фаз. Для любого угла α , не равного 0 или π , имеем:

Иначе говоря, для любой нетривиальной пары дополнительных углов $(\alpha, \pi - \alpha)$ приведенная выше диаграмма разделяется. Оказывается, что даже если ограничиться диаграммами Клиффорда+T, равенство



не доказуемо с помощью существующих правил. И это все, что мы знаем на данный момент! Быть может, существует какое-то одно волшебное правило, которое решает эту задачу, а быть может, и нет. И потому, увы, мы должны задать этот вопрос в «упражнении».

Упражнение* 9.133. Найдите полный набор правил для ZX-диаграмм (Клиффорда+T).

Как и с упражнением 7.39, если вам удастся найти решение, мы будем счастливы узнать об этом! Все имеющиеся публикации на эту тему обсуждаются в конце главы, но когда вы будете читать книгу, наверное, появятся новые.

9.5. Итоги: что следует запомнить

1. Несмещенными состояниями для пауков называются состояния, удовлетворяющие условиям:



Иначе говоря, несмещенные состояния для пауков дают равномерное распределение вероятностей для \circ -измерений. В терминах правила Борна это означает, что для всех i :

$$\begin{array}{c} \triangle \\ i \\ \downarrow \\ \psi \\ \triangle \end{array} = \frac{1}{D}$$

Опуская нормировку, мы получаем *фазовые состояния*:



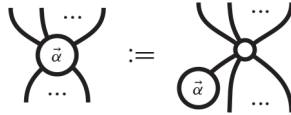
Фазы, украшающие эти состояния, интерпретируются как

данные, уничтожаемые классически-квантовым переходом.

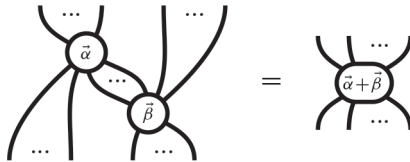
Иными словами, фазы – это истинно квантовый объект. В случае кубита они принимают вид:

$$\begin{array}{c} | \\ \circlearrowleft \\ \bar{\alpha} \end{array} \leftrightarrow \begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix}$$

2. Фазовые пауки возникают следующим образом:



а слияние фазовых пауков описывается равенством



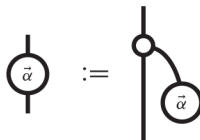
где

$$\begin{array}{c} | \\ \circlearrowleft \\ \overline{\alpha + \beta} \end{array} := \begin{array}{c} | \\ \circlearrowleft \\ \bar{\alpha} \end{array} \begin{array}{c} | \\ \circlearrowleft \\ \bar{\beta} \end{array} \quad (9.134)$$

Эта операция дает фазы со структурой коммутативной группы, которая называется *фазовой группой*. Единица и обратный элемент определяются в ней следующим образом:

$$\begin{array}{c} | \\ \circlearrowleft \\ \bar{0} \end{array} = \begin{array}{c} | \\ \circlearrowleft \end{array} \quad \begin{array}{c} | \\ \circlearrowleft \\ -\bar{\alpha} \end{array}$$

Важным примером фазовых пауков являются *фазовые вентили*:



3. Пауки \circ и \bullet называются *дополнительными*, если:

$$\begin{array}{c} \bullet \\ | \\ \circ \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

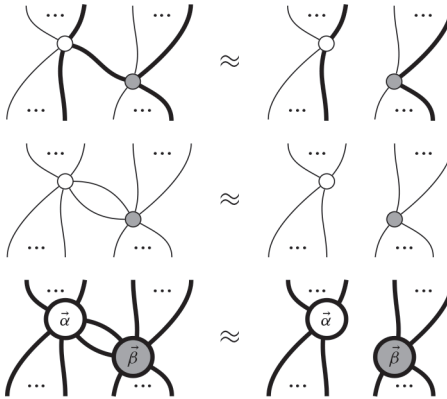
Дополнительность допускает следующую интерпретацию:

(кодировать в \circ) ЗАТЕМ (измерить в \bullet) = (нет потока данных).

Дополнительность эквивалентна тому, что все ОНБ-состояния \circ являются несмещенными для \bullet и наоборот, что можно выразить двумя способами:

$$\begin{array}{c} \bullet \\ | \\ \nabla_i \end{array} = \frac{1}{D} \begin{array}{c} | \\ \bullet \end{array} \qquad \begin{array}{c} \nabla_i \\ | \\ \bullet \end{array} = \frac{1}{D} \begin{array}{c} \bullet \\ | \\ \bar{\kappa} \end{array}$$

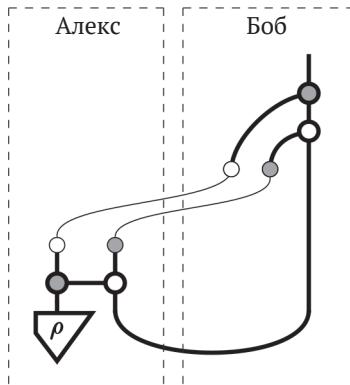
4. Дополнительность индуцирует правила разведения пауков:



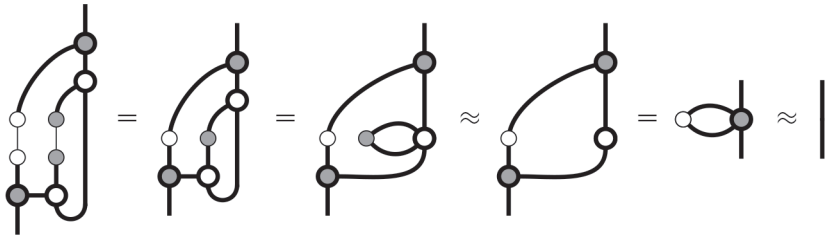
5. Дополнительная пара дает обобщенные вентили CNOT:



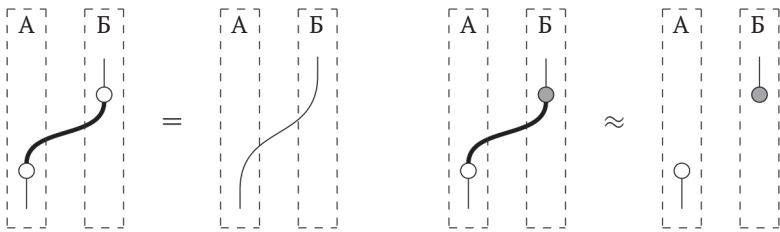
Она также дает все необходимое для телепортации:



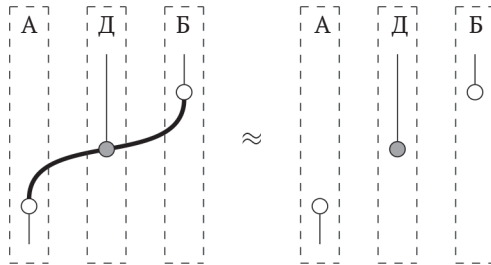
и для доказательства ее корректности:



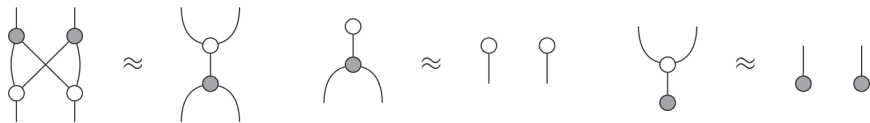
Мы можем также определить протокол *квантового распределения ключей*:



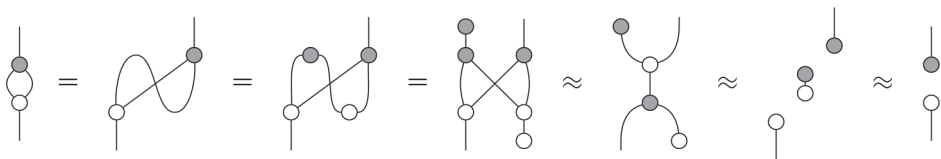
который позволяет обнаружить, что квантовый канал прослушивается:



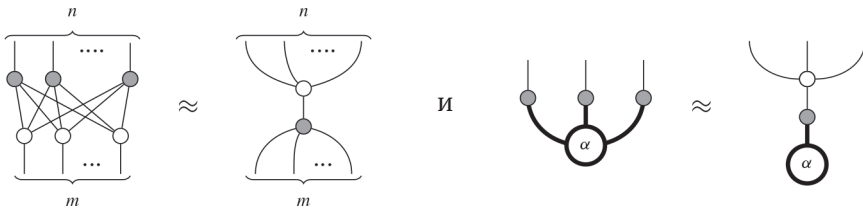
6. Из сильной дополнителности



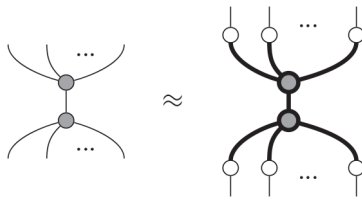
следует дополнителность (но эти понятия не совпадают):



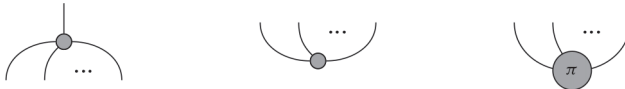
Она также дает новые средства преобразования диаграмм, например:



а еще



что показывает, что \bullet -пауки являются классическими отображениями для \circ . Примерами классических отображений для \circ в терминах \bullet -пауков являются *отображение четности, четное состояние и нечетное состояние*:



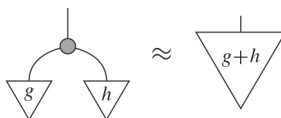
7. Сильная дополнительность эквивалентна тому, что базисные состояния \circ образуют *подгруппу* фазовой группы \bullet , и наоборот. То есть фазовые состояния, удовлетворяющие условиям



образуют следующие подгруппы:

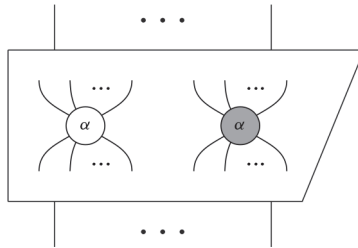
$$\left\{ \begin{array}{c} \circ \\ \vec{k} \end{array} \right\}_{\vec{k}} \subset \left\{ \begin{array}{c} \circ \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}} \quad \left\{ \begin{array}{c} \circ \\ \vec{k} \end{array} \right\}_{\vec{k}} \subset \left\{ \begin{array}{c} \circ \\ \vec{\alpha} \end{array} \right\}_{\vec{\alpha}}$$

8. Сильно дополнительные пары пауков *классифицируются* коммутативными группами. То есть для некоторого семейства \circ -пауков и любой конечной коммутативной группы G существует единственное семейство \bullet -пауков, такое что пара \circ/\bullet является сильно дополнительной и



Обратно, все сильно дополнительные пары возникают таким образом.

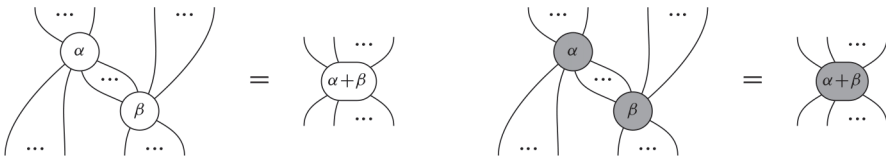
9. ZX-диаграммы, т. е. диаграммы, составленные из фазовых \circ - и \bullet -пауков:



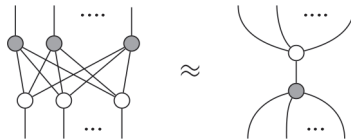
универсальны для кубитов, т. е. мы можем представить любое классически-квантовое отображение кубитов в виде ZX-диаграммы.

10. Диаграммами Клиффорда называются ZX-диаграммы, в которых фазы ограничены целыми кратными $\pi/2$. ZX-исчисление – графическое исчисление для диаграмм Клиффорда – состоит из следующих правил:

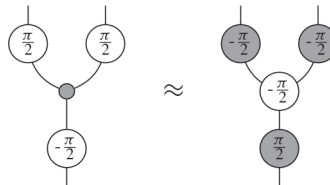
1. Два правила комбинирования пауков одного цвета:



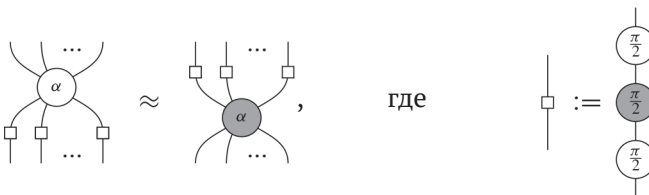
2. Правило коммутирования пауков разного цвета с изменением взаимного расположения:



3. Правило преобразования пауков одного цвета в другой:



Последнее правило можно заменить эквивалентным правилом изменения цвета:



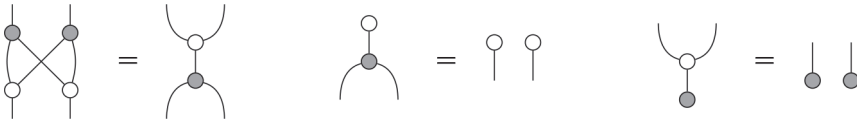
ZX-исчисление полно относительно **отображений Клиффорда**, т. е. чистых квантовых отображений, которые можно выразить в виде диаграмм Клиффорда. Поэтому любое равенство между отображениями Клиффорда можно доказать, пользуясь только правилами ZX-исчисления.

9.6. ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ*

9.6.1. Сильно дополнительные пауки как алгебра Хопфа*

В разделе* 8.6.1 мы видели, что пауки и ранее были широко известны как (ивольютивные специальные коммутативные) алгебры Фробениуса. Сильно дополнительные пары пауков тоже давно известны.

Определение 9.134. Биалгебра над векторным пространством V состоит из ассоциативной алгебры (\bullet, \circ) и коассоциативной коалгебры (\smile, \wp) , удовлетворяющих условиям:



Биалгебра называется *алгеброй Хопфа*, если она, кроме того, обладает линейным отображением

$$\begin{array}{c} | \\ \square \text{ / } \\ | \end{array} : V \rightarrow V$$

называемым *антиподом*, таким что

(9.135)

Выглядит знакомо. Если добавить коэффициенты $1/\sqrt{D}$ и в качестве антипода взять тривиальное отображение

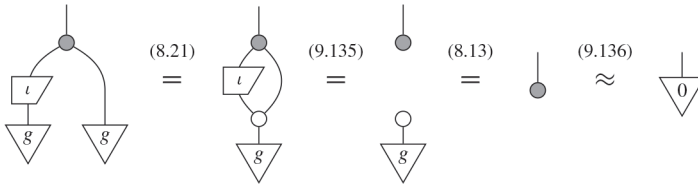
$$\begin{array}{c} | \\ \square \text{ / } \\ | \end{array} := |$$

то получатся в точности уравнения сильной дополнительности.

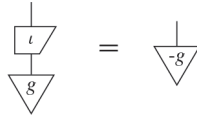
А для чего вообще нужны эти антиподы? Давайте еще раз взглянем на \bullet -пауков из раздела 9.3.6, определенных в терминах коммутативной группы G :

(9.136)

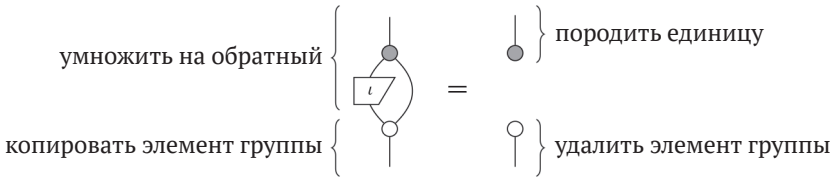
Подставляя ОНБ-состояние, соответствующее элементу группы $g \in G$, в равенство (9.135), получаем:



То есть если применить групповую операцию к g и результату применения ι к g , то получится 0. Это означает, что ι кодирует взятие обратного элемента:



Правило антиподов в алгебре Хопфа отражает тот факт, что $g - g = 0$:

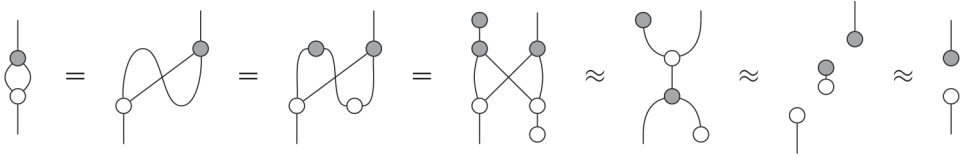


Алгебры Хопфа, получающиеся из группы описанным способом, называются *групповыми алгебрами*. Антипод в групповой алгебре тривиален в точности тогда, когда G состоит только из самообратных элементов $g = -g$, как, например, в группе \mathbb{Z}_2 .

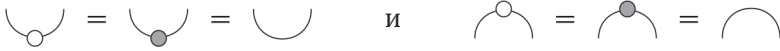
Замечание 9.135. Хотя мы обозначаем групповую операцию знаком $+$ (как обычно делают для коммутативных групп), эта конструкция работает и для некоммутативных групп. В таком случае алгебра \bullet оказывается некоммутативной, но \circ (которая по-прежнему является просто копированием) остается кокоммутативной. Существует обширная литература, посвященная изучению специальных алгебр Хопфа, которые не являются ни коммутативными, ни кокоммутативными и называются квантовыми группами.

Возможно, сейчас у вас возник вопрос: «Минуточку, а разве из сильной дополнителности (уравнений биалгебры) не следует дополнителность (дополнительное уравнение алгебры Хопфа)?» Да, конечно, следует, но \circ и \bullet должны быть пауками (т. е. инволютивными специальными коммутативными алгебрами Фробениуса), а не просто (ко)алгебрами.

Кроме того, внимательно изучив доказательство того, что сильная дополнителность влечет дополнителность:



мы увидим, что второй шаг существенно опирается на тот факт, что



справедливый только для семейств пауков, происходящих от самосопряженных ОНБ, – предположение, которого мы придерживаемся в этой книге.

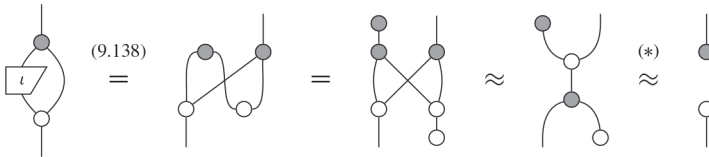
На самом деле мы могли бы опустить это предположение, при условии что модифицируем определение дополнительности:



где антипод выбирается следующим образом:



Тогда действительно получается:



Упражнение 9.136. Докажите последний шаг этого вывода, помеченный (*). Для этого, в частности, придется доказать равенства



Многое из сделанного в данной книге обобщается на эту более общую постановку, хотя диаграммы становятся чуть более сложными.

Упражнение 9.137. Адаптируйте описание квантовой телепортации, в котором используются дополнительные пауки (раздел 9.2.7), к этой более общей постановке. Бонусные очки: воспользуйтесь «волосатыми пауками» из раздела* 8.6.3 для выражения несамосопряженных пауков.

9.6.2. Сильная дополнителность и нормальные формы*

Мы уже видели такое следствие сильной дополнителности:

(9.139)

благодаря которому полный двудольный граф пауков можно заменить одним ●-пауком, за которым следует один ○-паук. Но на самом деле можно вывести гораздо больше равенств такого рода. Например, равенство

(9.140)

позволяет преобразовать циклы длины $2N$, состоящие из чередующихся ○- и ●-пауков, в последовательность связанных 6-циклов.

Упражнение* 9.138. Докажите равенство (9.140).

Равенства (9.139) и (9.140) – частные случаи следующего, гораздо более общего результата.

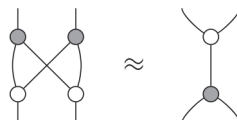
Теорема 9.139. Равенство

где Γ и Λ – схемы, состоящие только из пауков вида



доказуемо с применением слияния пауков и сильной дополнителности тогда и только тогда, когда количество по модулю 2 (прямых) путей, соединяющих каждый вход с каждым выходом, одинаково в Γ и Λ .

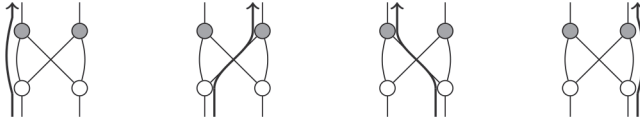
Иными словами, мы можем доказать любое равенство, вытекающее из сильной дополнителности, просто подсчитав пути. Посмотрим, как это выглядит в простейшем примере – первом уравнении сильной дополнителности:



Легко видеть, что существует всего один путь от первого входа к первому выходу:



На самом деле для любой комбинации входа и выхода существует всего один путь:



и то же верно для правой части:



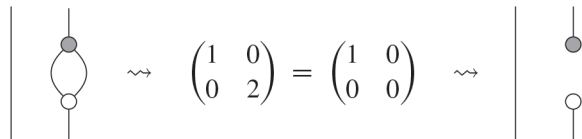
Отсюда можно сделать вывод, что левая и правая части равны. Проверка остальных двух уравнений сильной дополнителности показывает, что и они удовлетворяют правилу числа путей между входами и выходами (которое в этих случаях всегда равно 0).

Упражнение 9.140. Докажите равенство (9.140), пользуясь теоремой 9.139.

Удобно собрать всю информацию о подсчете путей в *матрицу путей* диаграммы. Это матрица \mathbf{m} , в которой элемент \mathbf{m}_i^j равен числу путей (по модулю 2) от входа i к выходу j . Например, у показанных выше диаграмм матрицы путей таковы:



Мы ведем подсчет по модулю 2, потому что пары путей можно исключать, пользуясь правилом дополнителности:



Это приводит к эквивалентной формулировке теоремы 9.139.

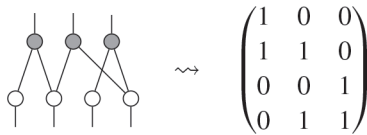
Следствие 9.141. Диаграммы Γ и Λ (см. теорему 9.139) равны тогда и только тогда, когда их матрицы путей одинаковы.

А как это доказать? Сначала заметим, что все правила сильной дополнителности и правило слияния пауков сохраняют матрицу путей. Поэтому достаточно показать, что с помощью этих правил мы можем привести любую диаграмму к *нормальной форме*, однозначно определяемой заданной матрицей путей. Эти нормальные формы описываются следующим образом:

- i) никакие два паука одного цвета не соприкасаются;
 - ii) любая пара пауков соединена не более чем одним ребром;
 - iii) все \circ -пауки встречаются раньше \bullet -пауков.
- Графически нормальные формы выглядят так:



Имея такую нормальную форму, мы можем построить матрицу путей, помещая в нее 1 всякий раз, как видим провод, соединяющий пауков. Например:

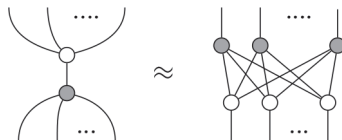


Обратно, для любой матрицы путей существует единственная нормальная форма, в которой от входов к выходам ведут правильные пути.

Таким образом, осталось только доказать, что любую диаграмму можно привести к нормальной форме. Если наша диаграмма не удовлетворяет условию (i) или (ii), то мы всегда можем применять правила слияния пауков или дополнителности, пока это условие не будет выполнено. Поэтому сложность представляет только условие (iii). Именно здесь играет роль разрешение использовать лишь пауков вида:

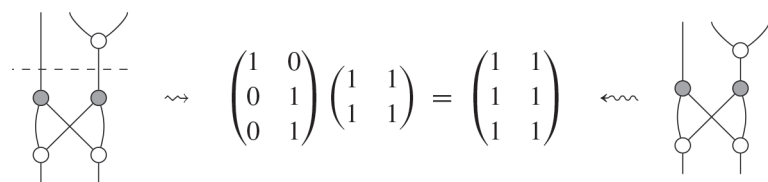


Диаграмма может не удовлетворять условию (iii), только если содержит правую часть вида (9.139). Но тогда, применив это же равенство в обратном направлении

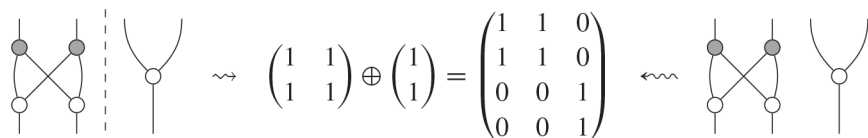


мы сможем протолкнуть \circ -паука за \bullet -паука. Поскольку мы ограничились схемными диаграммами, то, проделав этот трюк несколько раз, мы поднимем всех \bullet -пауков наверх, а всех \circ -пауков опустим вниз, что и даст нормальную форму.

Интересно, что сами матрицы путей образуют процессную теорию. Сначала отметим, что \circ -композиция двух матриц дает такой же результат, как подсчет путей в получающейся в результате композиции диаграмм:

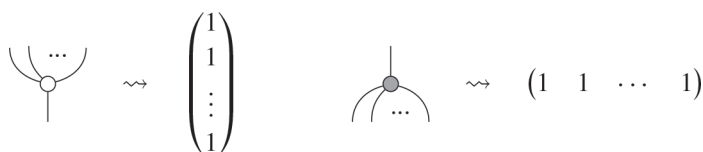


\otimes -композиция диаграмм дает не кронекеровское произведение матриц путей, а *прямую сумму*:



Это совершенно разумный способ параллельной композиции матриц, поэтому обозначим $\mathbf{matrices}_{\oplus}(\mathbb{Z}_2)$ процессную теорию матриц, определенную в разделе 5.2.5, с тем отличием, что параллельной композицией является \oplus , а не кронекеровское произведение.

Оба специальных вида пауков типа «один ко многим» из теоремы 9.139 обитают в этой процессной теории:



а единственные равенства, имеющие место между диаграммами этих пауков, – те, что вытекают из правил слияния пауков и сильной дополнителности (или, эквивалентно, из уравнений алгебры Хопфа). Эта процессная теория является «блуждающей алгеброй Хопфа» в том смысле, что содержит алгебру Хопфа и ничего более. Поэтому если мы хотим изучить существо алгебр Хопфа, то должны изучать эту процессную теорию. Специалистам по теории категорий это утверждение известно под названием *PROP для алгебр Хопфа*.

9.7. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Большая часть материала этой главы и, прежде всего, диаграммные понятия фазовых состояний, фазовых пауков, фазовой группы, дополнителности (т. е. взаимной несмещенности) и сильной дополнителности, а также все их эквивалентные характеристики, приведенные в разделе 9.3.4, взяты из работ Coecke and Duncan (2008, 2011). Однако в работе Coecke and Duncan (2008) имеется бессмысленное утверждение, а именно что при «слабом» предположении и замыкании классиче-

ской подгруппы дополнителность и сильная дополнителность эквивалентны. Только впоследствии авторы осознали, что замыкание классической подгруппы уже эквивалентно сильной дополнителности, так что это предположение совсем не слабое!

Обычное понятие взаимной несмещенности впервые появилось в работе Schwinger (1960). Подробный обзор всего, что известно по этому поводу, включая и проблемы классификации, содержится в работе Durt et al. (2010). С другой стороны, классификацией сильно дополнителных пар мы обязаны работе Kissinger (2012a).

ZX-исчисление также введено в работах Coecke and Duncan (2008, 2011). Однако представленной там версии оказалось недостаточно для теоремы полноты из раздела 9.4.5. Y-правило новое (если не считать его более сложного варианта, обсуждавшегося в беседах с Россом Данканом), но его эквивалентная версия в терминах разложения H -вентилей по углам Эйлера приведена в работе Duncan and Perdrix (2009). Большинство бытовавших вариантов ZX-исчисления содержало избыточность, но недавно в работе Backens et al. (2016) был предложен минимальный вариант (наше изложение заимствовано оттуда).

Теорема о полноте относительно отображений Клиффорда доказана в работе Backens (2014a), а теорема о полноте относительно однокубитовых отображений Клиффорда+T – в работе Backens (2014b). Родственная теорема о полной характеристике n -кубитовых схем Клиффорда в терминах генераторов и отношений доказана в работе Selinger (2015).

В работе Schröder de Witt and Zamdzhiev (2014) показано, что полноту невозможно обеспечить с помощью текущих правил для произвольных квантовых отображений кубитов, а в работе Perdrix and Wang (2015) – что так же обстоит дело для отображений Клиффорда+T. Уравнение дополнителности, использованное для этой цели, впервые появилось в работе Coecke and Edwards (2010).

Графовые состояния, сыгравшие важную роль в доказательстве полноты, введены в работе Hein et al. (2004). Предложение 9.125, принадлежащее Бэкенсу, основано на мощной теореме ван ден Неста, которая утверждает, что графовые состояния эквивалентны с точностью до локального унитарного отображения Клиффорда тогда и только тогда, когда их можно преобразовать друг в друга с помощью локального дополнения (Van den Nest et al., 2004).

Первым, кто осознал, что сильную дополнителность можно использовать для моделирования взаимодействий классических систем с квантовыми данными, как в примере 9.74, был Куан Лонг (Харни) Ванг (Quanlong (Harny) Wang), работавший в составе коллектива, подготовившего работу Coecke et al. (2012).

Квантовые схемы введены в работе Deutsch (1989). Идея квантового распределения ключей впервые высказана в работе Bennett and Brassard (1984), а вариант, полученный «сгибанием провода» (т. е. использование запутанного состояния вместо передачи квантовой системы), принадлежит Экерту (Ekert, 1991). Протокол, описанный в примере 9.61, предложен в работе Perdrix (2005).

Использование ZX-исчисления для моделирования квантовых схем взято из работы Coecke and Duncan (2008), а его применение для квантового распределения ключей, как описано в разделе 9.2.6, взято из работ Coecke and Perdrix (2010) и Coecke et al. (2011a). Построение управляемых операций в ZX-исчислении, как в разделе 9.2.7, заимствовано из работы Coecke and Duncan (2011). Аналогичная

конструкция в терминах только фазовых вентиляей и вентиля CNOT была представлена в работе Varenco et al. (1995).

Хорошим ресурсом для изучения алгебр Хопфа и квантовых групп является книга Street (2007). Из других стандартных учебников отметим Kassel (1995) и Majid (2000). Характеристика в терминах «подсчета путей», а также нормальная форма биалгебр, описанные в разделе* 9.6.2, предложены в работе Lack (2004) как пример систематической «композиции» двух диаграммных теорий (или *PROP*'ов), а именно алгебр и коалгебр. Та же техника использовалась в работе Bonchi et al. (2014b) для композиции пары биалгебр с целью получить свободный от фаз фрагмент ZX-исчисления. Интересно, что характеристика этой теории практически совпадает с характеристикой биалгебр, приведенной в разделе* 9.6.2, только вместо матриц используется более общее понятие «линейных отношений». Поучительный и не лишенный юмора рассказ об этом результате, включающий ссылки на футбол, конструктор LEGO и деление на ноль, имеется в блоге (Sobocinski, 2015).

Фраза «фантастическая эффективность диаграммных рассуждений с привлечением пауков» украдена из работы Wigner (1995b), где автор рассуждает о «фантастической эффективности математики в естественных науках».

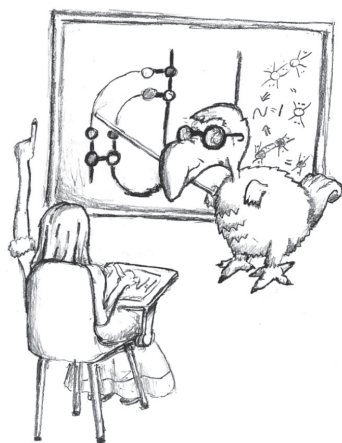
Глава 10

Квантовая теория: полная картина

Философия написана в той величественной Книге (я имею в виду Вселенную), которая всегда открыта нашему взору, но читать ее может лишь тот, кто сначала освоит язык и научится понимать знаки, которыми она начертана. Написана же она на языке математики, и знаки ее – треугольники, окружности и другие геометрические фигуры, без которых нельзя понять ни единого из стоящих в ней слов и остается лишь блуждать в темном лабиринте.

– Галилео Галилей «Пробирных дел мастер»¹

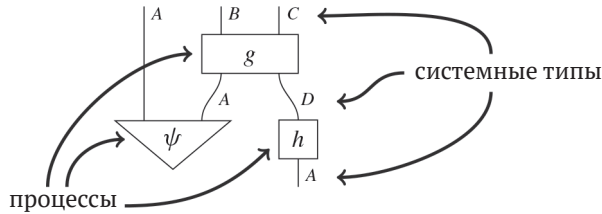
В предыдущих главах мы построили диаграммные представления основных составных частей квантовой теории и соотнесли их с обычным квантовым формализмом в терминах гильбертовых пространств и линейных отображений. А теперь пришло время забыть о последнем и перейти к чистому квантовому пикторализму! Поскольку, чтобы добраться до этой точки, требуется немало времени, мы в этой главе расскажем всю квантовую историю на языке диаграмм и только диаграмм.



¹ Галилео Галилей. Пробирных дел мастер / пер. Ю. А. Данилова. М.: Наука, 1987.

10.1. ДИАГРАММЫ

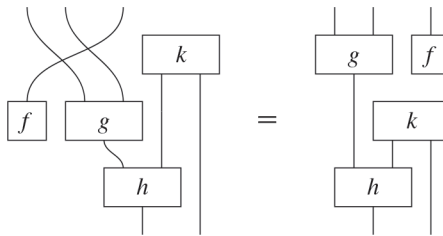
Диаграммы состоят из блоков и проводов, которые представляют соответственно процессы и системы:



Золотое правило диаграмм:

важны только соединения!

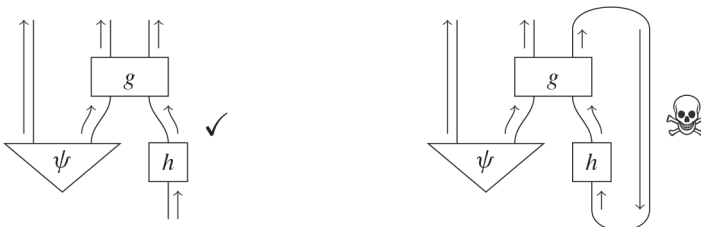
Это означает, что две диаграммы равны, если они содержат одинаковые блоки, одинаково соединенные, и не важно, как именно они расположены на странице:



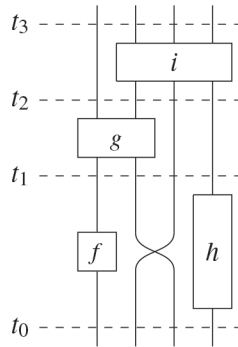
Вся эта книга – история об эволюции диаграммного языка. В разделе 2.2.1 мы выделили несколько этапов этой эволюции в порядке возрастания выразительности. Теперь мы знаем об этих этапах все.

10.1.1. Схемные диаграммы

Схемные диаграммы – это диаграммы, не содержащие ориентированных циклов:



Их можно охарактеризовать как диаграммы, передающие идею прошлого и будущего. Их всегда можно организовать как последовательность временных шагов:



хотя, возможно, и не единственным способом.

Процессы, не имеющие входов, называются *состояниями*, а процессы, не имеющие выходов, – *эффектами*. Когда состояние встречается с эффектом, на свет рождается число:

$$\left. \begin{array}{l} \text{эффект} \left\{ \begin{array}{c} \triangle \pi \\ \downarrow \\ \nabla \psi \end{array} \right\} \\ \text{состояние} \left\{ \begin{array}{c} \triangle \pi \\ \downarrow \\ \nabla \psi \end{array} \right\} \end{array} \right\} \text{число} \quad (10.1)$$

которое можно интерпретировать как вероятность (а иногда только как возможность) возникновения эффекта π при условии заданного состояния ψ . Это называется *обобщенным правилом Борна*.

В общем случае число – это не что иное, как процесс, не имеющий ни входов, ни выходов



и обычно мы записываем его просто λ . Всегда существует одно специальное число – пустая диаграмма, или 1:



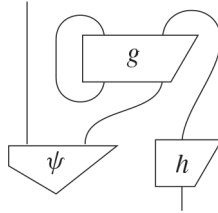
Иногда имеется также 0 – число, которое «пожирает все». Как и следовало ожидать, произведение чего-то на 1 равно этому «чему-то», а произведение чего-то на 0 равно 0:

$$\left[\text{dashed box} \right] \left[f \right] = \left[f \right] \quad \quad 0 \left[f \right] = 0 \quad (10.2)$$

См. также *схемы* в разделе 3.2; *состояния, эффекты и числа* в разделе 3.4.1; *ноль* в разделе 3.4.2.

10.1.2. Струнные диаграммы

Струнные диаграммы отменяют запрет на ориентированные циклы и даже разрешают соединять входы с входами, а выходы с выходами:



Можно также сказать, что они происходят из схемных диаграмм путем добавления специальных процессов:

$$\text{чашки} := \cup \quad \text{и} \quad \text{крышки} := \cap \quad (10.2)$$

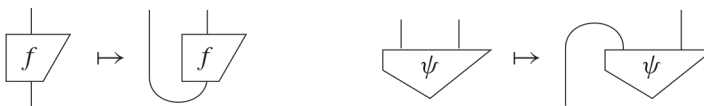
которые удовлетворяют уравнениям разгибания:

$$\cup = | \quad \cap = \cup \quad \text{loop} = \cap \quad (10.3)$$

Существование чашек и крышек явно свидетельствует о *неразделимости* в следующем смысле:

для любой (нетривиальной) системы чашка и крышка никогда не являются \otimes -разделимыми.

Однако чем рассуждать о том, чего нельзя сделать с чашками и крышками (разделить их), гораздо интереснее посмотреть, что сделать можно! Они позволяют закодировать процессы и двухкомпонентные состояния, а затем вернуться обратно, ничего не потеряв:



Эта двойственность процессов и состояний дает изоморфизм:

$$\left\{ \begin{array}{c} |B \\ \hline \text{f} \\ \hline |A \end{array} \right\}_f \cong \left\{ \begin{array}{c} |A \quad |B \\ \hline \psi \\ \hline \end{array} \right\}_\psi \quad (10.4)$$

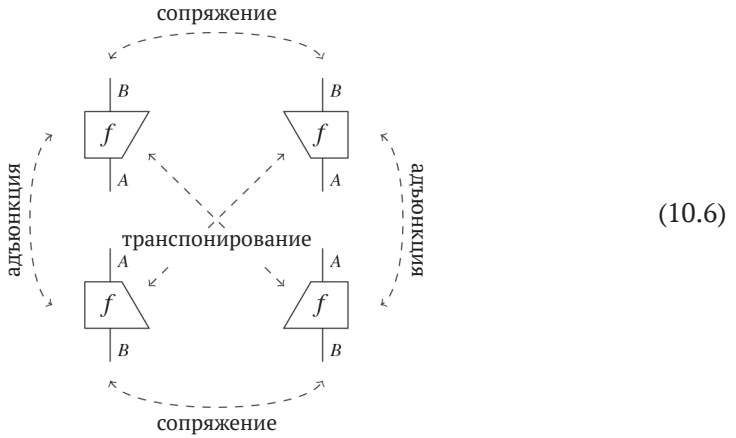
Чашки и крышки также индуцируют поворот блоков на 180°, называемый *транспонированием*:

$$\text{Block } f := \text{Block } f \text{ with loop} \quad (10.5)$$

С другой стороны, *адьюнкция* означает вертикальное отражение блоков:

$$f \mapsto f^\dagger$$

Комбинирование этих операций дает четыре воплощения любого блока:



В частности, адьюнктом состояния является эффект, проверяющий нахождение в этом состоянии:

$$\psi \mapsto \psi^\dagger$$

Мы ожидаем, что результат проверки на нахождение состояния в самом себе будет равен 1:

$$\psi \circ \psi^\dagger = 1 \quad (10.7)$$

т. е. по умолчанию мы ожидаем, что состояния *нормированные*. Однако ненормированные состояния естественно возникают, когда нужно выразить недетерминированность. Например,

$$\psi' := p \psi$$

можно интерпретировать как « ψ происходит с вероятностью p ».

Адьюнкты допускают определения специальных процессов, например *изометрий*:

$$\begin{array}{c} | \\ \text{A} \\ \text{U} \\ | \\ \text{B} \\ \text{U} \\ | \\ \text{A} \end{array} = \begin{array}{c} | \\ \text{A} \end{array} \quad (10.8)$$

унитарных процессов, представляющих собой двусторонние изометрии, и *положительных процессов* f , т. е. таких, для которых существует процесс g такой, что

$$\begin{array}{c} | \\ \text{A} \\ f \\ | \\ \text{A} \end{array} = \begin{array}{c} | \\ \text{A} \\ g \\ | \\ \text{B} \\ g \\ | \\ \text{A} \end{array} \quad (10.9)$$

См. также (не)разделимость в разделе 4.1.1; двойственность процессов и состояний в разделе 4.1.2; транспонирование в разделе 4.2.1; адьюнкты в разделе 4.3.1; сопряжение в разделе 4.3.2; изометрические и унитарные процессы в разделе 4.3.4; положительные процессы в разделе 4.3.5.

10.1.3. Дублированные диаграммы

Дублированными называются диаграммы вида:

$$\begin{array}{c} | \\ \Phi \\ | \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ | \\ \hat{f} \\ | \end{array} := \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ | \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ | \end{array} \quad (10.10)$$

где эффект

$$\text{---} = \begin{array}{c} \text{---} \\ \text{---} \\ | \end{array} \quad (10.11)$$

интерпретируется как *отбрасывание* выходов процесса.

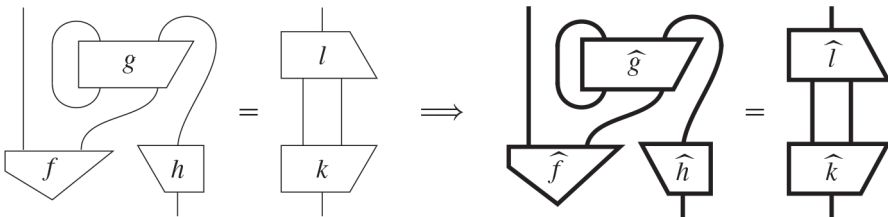
Они получаются в результате двухшаговой конструкции. Сначала мы дублируем системы:

$$\text{double} \left(\begin{array}{|c} \hline \\ \hline \end{array} \right) = \begin{array}{|c} \hline \\ \hline \end{array} := \begin{array}{|c} \hline \\ \hline \end{array}$$

и процессы

$$\text{double} \left(\begin{array}{|c} \hline \\ \hline \end{array} \right) = \begin{array}{|c} \hline \\ \hline \end{array} := \begin{array}{|c} \hline \\ \hline \end{array}$$

Эта операция сохраняет диаграммы, а потому и равенства между диаграммами:



Поэтому все, что можно доказать с использованием диаграмм одиночных процессов, имеет место и для дублированных. Обратное утверждение – что любое равенство между дублированными процессами справедливо и для недублированных, почти верно. Единственное, что не сохраняется при таком переходе, – некоторые числа, называемые *глобальными фазами*:

$$\bar{\lambda} \lambda = \begin{array}{|c} \hline \\ \hline \end{array} \Rightarrow \text{double} \left(\lambda \begin{array}{|c} \hline \\ \hline \end{array} \right) = \text{double} \left(\begin{array}{|c} \hline \\ \hline \end{array} \right)$$

но поскольку они никак не влияют на вероятности, то и скатертью дорога!

Однако если работа с дублированными процессами ничем не отличается от работы с одиночными (с точностью до глобальной фазы), то в чем смысл дублирования? Главная «фишка» дублирования в том, что открывается место для кое-чего нового. Второй шаг конструкции дублирования – присоединение отбрасывания, представляющего акт буквального устранения системы (или просто ее игнорирования). Для этого мы соединяем вместе две копии нормированного состояния, давая им возможность аннигилировать:

$$\begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline \\ \hline \end{array} = \begin{array}{|c} \hline \\ \hline \end{array} \quad (10.12)$$

Поскольку отбрасывание не является результатом дублирования чего-то, оно называется *нечистым*. Вообще, отбрасывая выходы *чистых* (т. е. дублированных) процессов, мы получаем множество других, нечистых процессов вида (10.10).

Посредством дублирования всех проводов мы также открыли вакансию для систем другого типа, которые можно представить в виде до боли знакомых одиночных проводов:

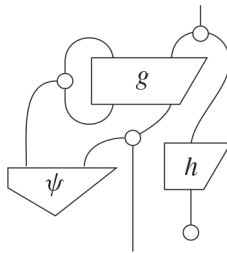
$$\left(\begin{array}{l} \text{дублированные} \\ \text{системы} \end{array} := \left| \right) \neq \left(\begin{array}{l} \text{одиночные} \\ \text{системы} \end{array} := \left| \right) \right.$$

А как взаимодействуют системы двух типов? С помощью *пауков*.

См. также *дублирование* в разделе 6.1; *глобальные фазы* в разделе 6.1.2; *отбрасывание* в разделе 6.2.1; *дублированная процессная теория* в разделе 6.2.4; *классические провода* в разделе 8.1.

10.1.4. Паучьи диаграммы

Паучьи диаграммы состоят из блоков и «обобщенных проводов», которым разрешено соединять произвольное число входов с произвольным числом выходов:



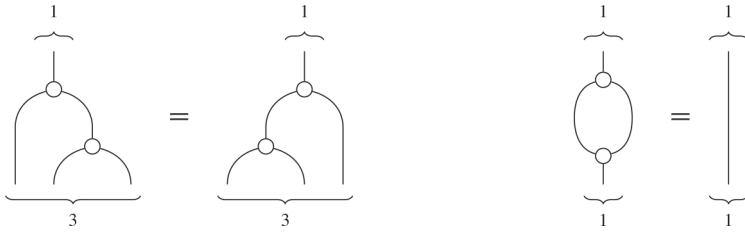
Их тоже можно эквивалентно представить в виде схемных диаграмм, добавив специальные процессы, называемые *пауками*:

$$\text{пауки} := \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \\ \diagdown \quad \diagup \\ \dots \end{array} \quad (10.13)$$

Они подчиняются всего одному правилу – смежные пауки сливаются:

$$\begin{array}{c} \dots \quad \dots \\ \diagup \quad \diagdown \\ \circ \quad \circ \\ \diagdown \quad \diagup \\ \dots \quad \dots \end{array} = \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \\ \diagdown \quad \diagup \\ \dots \end{array} \quad (10.14)$$

Отсюда, в частности, следует, что любые две связные диаграммы, составленные из пауков с одинаковым количеством входов и выходов, равны:



Учитывая, что двуногие пауки – это просто «старые добрые» провода:

(10.15)

паучьи диаграммы включают струнные диаграммы, а слияние пауков обобщает уравнения разгибания, например:

(10.16)

Дублирование дает нам еще два вида пауков совершенно бесплатно. Мы получаем новые чистые процессы, дублируя паука целиком:

(10.17)

Мы также получаем *гибридных пауков*, интерпретируя некоторые пары ног как дублированные системы (*сворачивание*), но оставляя другие одиночными:

(10.18)

дублированные системы
одиночные системы

Они подчиняются собственным правилам слияния:

$$(10.19)$$

и, кроме того, гибридные пауки могут сливаться с остальными двумя видами пауков:

$$(10.20)$$

Отбрасывание само является гибридным пауком:

$$(10.21)$$

откуда

$$(10.22)$$

С каждым семейством пауков мы можем ассоциировать *допускающие копирование состояния*:

$$(10.23)$$

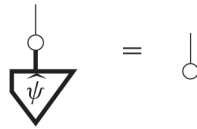
которые к тому же ортонормированны:

$$(10.24)$$

Отсюда и из правила слияния пауков получаем *обобщенное правило копирования*:

$$(10.25)$$

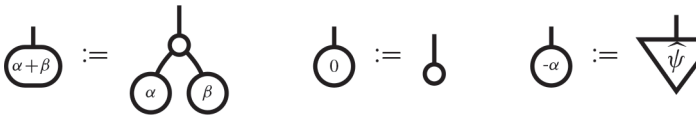
Это свойство – погнать при переходе из дублированного мира в одиночный – полностью характеризует фазы. Чтобы убедиться в этом, рассмотрим все состояния, где



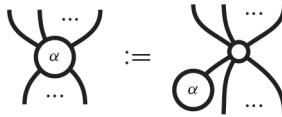
Тогда, как по мановению волшебной палочки, возникает коммутативная *фазовая группа*. Полагая



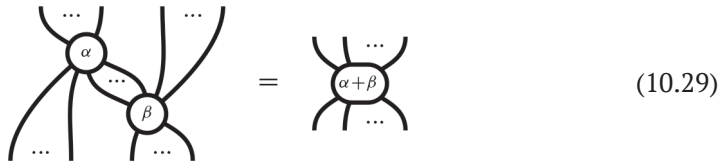
получаем



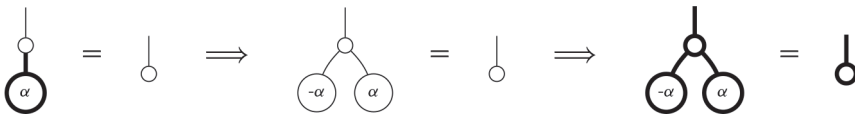
Затем, полагая



мы восстанавливаем всех фазовых пауков и ассоциированное с ними правило слияния:



На самом деле никакого волшебства тут нет. Свойство «погнать при переходе из дублированного мира в одиночный» – именно то, что отвечает за нетривиальную часть работы, а именно за наличие обратных элементов в этой группе:



В случае ZX-диаграмм возникающая таким образом группа совпадает с группой круга $U(1)$:



а в случае *ZX-диаграмм Клиффорда* мы ограничиваемся только четырехэлементной подгруппой \mathbb{Z}_4 группы $U(1)$:



В обоих случаях группы можно рассматривать как определенного вида вращения сферы. Но не будем забегать вперед.

См. также *фазовые пауки* в разделе 9.1.2; *фазовая группа* в разделе 9.1.4; *ZX-диаграммы* в разделе 9.4.1; *диаграммы Клиффорда* в разделе 9.4.2.

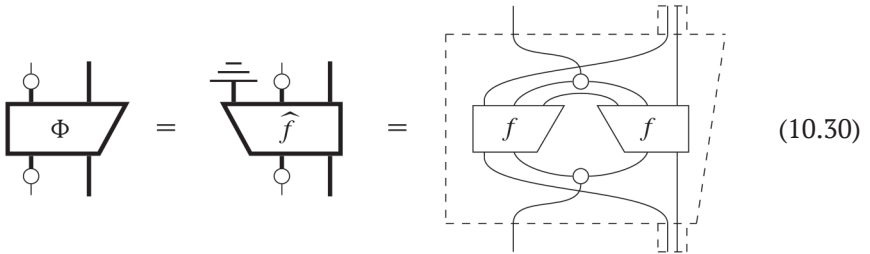
10.2. ПРОЦЕССЫ

Процессной теорией называется совокупность процессов, которые имеет смысл соединять между собой. Иными словами, она замкнута относительно образования диаграмм. Вот как выглядит процессная теория, которую все мы любим: *квантовая теория*.

Существует два вида систем: квантовые и классические:



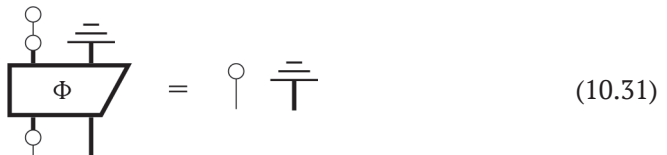
Процессы, которые могут быть реализованы (не обязательно со стопроцентной вероятностью), – это:



где блок, помеченный буквой f , состоит из фазовых пауков:



Процессы, которые могут быть реализованы со стопроцентной вероятностью, дополнительно подчиняются правилу причинности (каузальности):

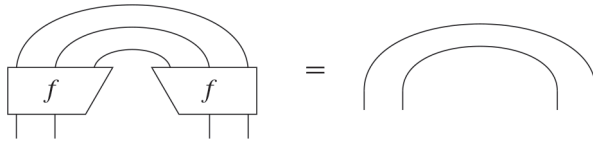


10.2.1. Причинность

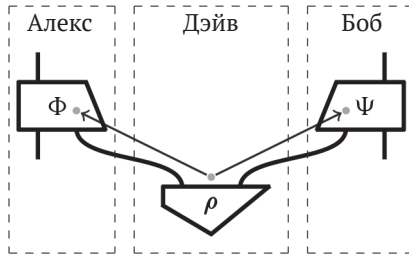
Причинность – чрезвычайно важный принцип квантовой теории, который тем не менее имеет удивительно простую интерпретацию:

если выход процесса отбрасывается,
то это все равно, что его никогда и не существовало.

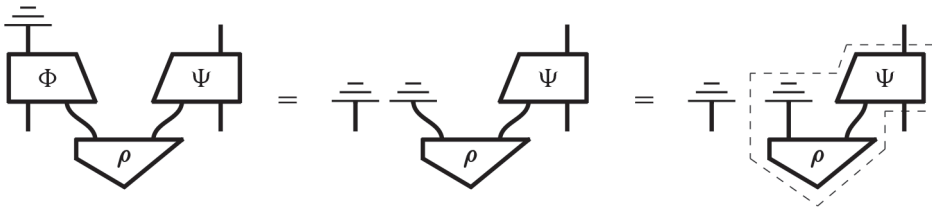
Для квантового процесса (10.30) причинность эквивалентна тому, что f – изометрия:



Этот принцип гарантирует, что квантовая теория совместима со специальной теорией относительности, т. е. является *несигнальной*. Несигнальность означает, что поток информации не должен нарушать *причинную структуру*. Так, если Алекс и Боб находятся очень далеко друг от друга, но, возможно, разделяют какую-то общую корреляцию из прошлого:



то Алекс не может напрямую общаться с Бобом. В пользу этого свидетельствует тот факт, что если Боб не знает выхода процесса Алекса:



то он не может знать и его входа.

См. также *причинность* в разделе 6.2.5; *причинная структура* в разделе 6.3.1; *несигнальность* в разделе 6.3.2.

10.2.2. Разложение процессов и невозможность распространения

Процессная теория допускает *спектральную декомпозицию*, если любой положительный процесс можно представить в виде:

(10.35)

для (каузальных) состояний ρ и p .

Из этих результатов о разделении сразу вытекает *невозможность распространения*, т. е. не существует квантового процесса такого, что:

(10.36)

Тождественный процесс чистый, поэтому если бы такой процесс существовал, то он разделялся бы как

(10.37)

что приводит к противоречию:

(10.36r) (10.37)

См. также *спектральная теорема* в разделе 5.3.3.1; спектральное и сингулярное разложение в разделе 8.2.5; невозможность распространения в разделе 6.2.8.

10.2.3. Примеры

В квантовой теории процессы, которые могут протекать недетерминированно, называются **КК-отображениями**, а каузальные КК-отображения называются просто **квантовыми процессами**. В этом разделе мы приведем несколько важных примеров.

10.2.3.1. Классические отображения

Классические отображения – это КК-отображения, не имеющие квантовых входов и выходов:

(10.38)

а классические процессы – это каузальные классические отображения:

$$\begin{array}{c} \circ \\ \diagdown \\ \boxed{f} \\ \diagup \\ | \end{array} = \begin{array}{c} \circ \\ | \end{array} \quad (10.39)$$

Следовательно, классические отображения автоматически являются самосопряженными:

$$\begin{array}{c} | \\ \diagdown \\ \boxed{f} \\ \diagup \\ | \end{array} = \begin{array}{c} | \\ \diagup \\ \boxed{f} \\ \diagdown \\ | \end{array} \quad (10.40)$$

Простейшие примеры классических отображений – \circ -копируемые состояния и эффекты, которые представляют:

$$\text{классические значения} := \begin{array}{c} | \\ \diagdown \\ \boxed{i} \\ \diagup \\ | \end{array} \quad \text{классические испытания} := \begin{array}{c} \triangle \\ \diagup \\ \boxed{i} \\ \diagdown \\ | \end{array}$$

Система, допускающая только два таких значения/испытания, 0 и 1, называется битом.

Приведем примеры классических процессов:

- классические значения, потому что:

$$\begin{array}{c} \circ \\ | \\ \diagdown \\ \boxed{i} \\ \diagup \\ | \end{array} = \boxed{} \quad (10.41)$$

- функциональные отображения, т. е. процессы, кодирующие функцию

$$f : \{1, \dots, m\} \mapsto \{1, \dots, n\}$$

посредством

$$\begin{array}{c} | \\ \diagdown \\ \boxed{f} \\ \diagup \\ | \\ \diagdown \\ \boxed{i} \\ \diagup \\ | \end{array} := \begin{array}{c} | \\ \diagdown \\ \boxed{f(i)} \\ \diagup \\ | \end{array} \quad (10.42)$$

которые характеризуются равенством

$$\begin{array}{c} \circ \\ \diagup \\ \diagdown \\ | \\ \diagdown \\ \boxed{f} \\ \diagup \\ | \end{array} = \begin{array}{c} | \\ \diagdown \\ \boxed{f} \\ \diagup \\ \circ \\ \diagdown \\ \boxed{f} \\ \diagup \\ | \end{array} \quad (10.43)$$

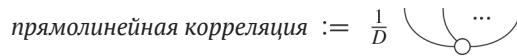
и, следовательно, удовлетворяют условию

$$\begin{array}{c} \circ \\ | \\ \boxed{\hat{f}} \\ | \\ \circ \end{array} = \begin{array}{c} | \\ \boxed{f} \\ | \end{array} \quad (10.44)$$

- ○-пауки ровно с одним входом:



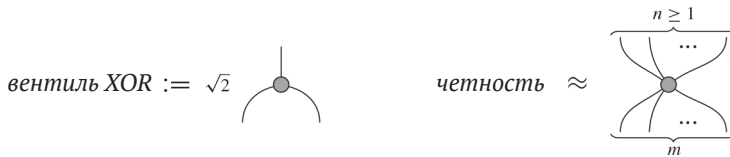
- ○-пауки, не имеющие входов (после перенормировки):



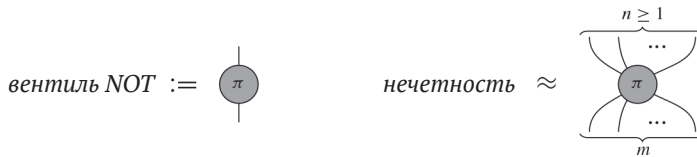
и как частный случай:



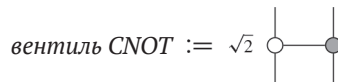
- ●-пауки, имеющие более одного выхода (после перенормировки):



- то же самое, но с фазой π :



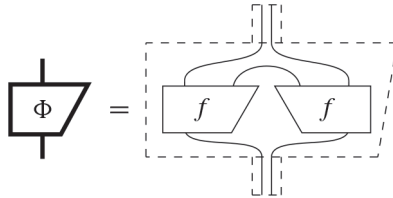
- и комбинации вышеперечисленного:



Последние три примера приведены для частного случая битов, но обобщаются и на другие классические системы.

10.2.3.2. Квантовые отображения

Квантовыми отображениями называются КК-отображения, не имеющие классических входов и выходов:



Ниже приведены примеры квантовых состояний:

максимально смешанное состояние := $\frac{1}{D} \underline{\underline{\mathbb{1}}}$

состояние Белла := $\frac{1}{D}$

ГХЦ-состояние := $\frac{1}{D}$

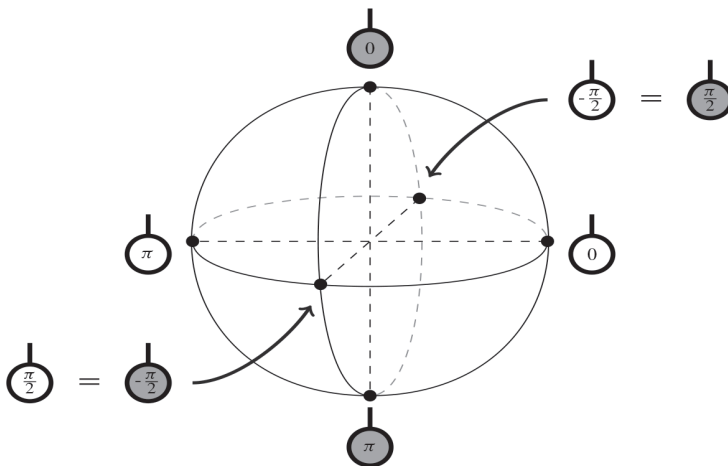
Ограничившись кубитами, т. е. двумерными квантовыми системами, имеем:

состояния Z-базиса := $\left\{ \begin{matrix} \text{0} \\ \text{1} \end{matrix} \right\}$

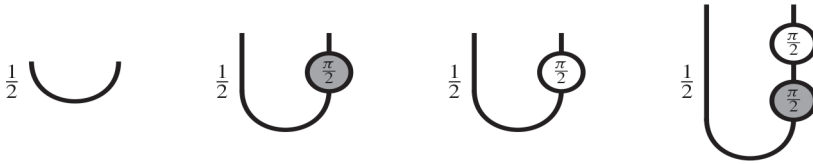
состояния X-базиса := $\left\{ \begin{matrix} \text{0} \\ \text{1} \end{matrix} \right\}$

состояния Y-базиса := $\left\{ \begin{matrix} \frac{\pi}{2} \\ -\frac{\pi}{2} \end{matrix} \right\}$

что можно изобразить на сфере Блоха:



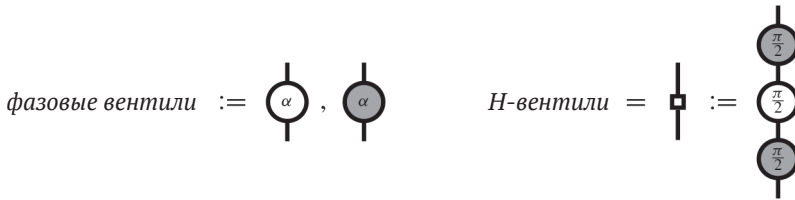
На паре кубитов состояние Белла расширяется до базиса Белла:



который выражается в терминах состояния Белла и четырех *отображений Белла*:



Все это унитарные квантовые процессы, или *квантовые вентили*. Перечислим другие важные однокубитовые квантовые вентили:



и два двухкубитовых квантовых вентилей:



10.2.3.3. Классически-квантовые взаимодействия

Многие классически-квантовые взаимодействия возникают как частные случаи гибридных пауков:

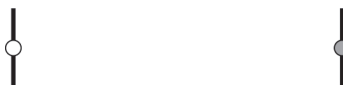
- кодировщик и измеритель для всех цветов:



- соответствующие *невозмущающие измерения*:



- и *декогеренция*:



Более общие *возмущающие* и *невозмущающие измерения ОНБ* получаются в результате комбинирования гибридных пауков с унитарным процессом \hat{U} :



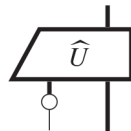
Важными примерами являются *Y-измерения*:



и неразделимое измерение Белла:



Если измерения извлекают классические данные из квантовой системы, то *управляемые унитарные процессы*



применяют классические данные для изменения квантовой системы. Они характеризуются следующими уравнениями:

(10.45)

Примером может служить *коррекция*, используемая в квантовой телепортации:

$$\text{[Trapezoidal gate } \hat{U} \text{]} := \text{[CNOT circuit]} \quad (10.46)$$

которую можно разложить следующим образом:

$$:= \text{[CNOT 1]} := \text{[CNOT 2]} \quad (10.47)$$

Ну, что ж, мы получили неплохой набор деталей. Теперь соединим их вместе и запустим эту штуку!

См. также классические отображения и функциональные отображения в разделе 8.2.1; классические логические вентили в разделе 5.3.4; отображения четности в разделе 9.3.5; максимально смешанное состояние в разделе 6.2.2; сфера Блоха в разделе 6.1.2; отображения и базис Белла в разделе 5.3.6; фазовые вентили в разделе 9.1.5; *H*-вентиль в разделе 5.3.5; измеритель и кодировщик в разделе 8.1.3; декогеренция в разделе 8.3.2; измерения ОНБ в разделе 8.4.1; управляемые унитарные процессы в разделе 8.4.2; измерение и коррекция Белла в разделе 9.2.7.

10.3. Законы

Обратимся теперь к важнейшим законам, управляющим квантовыми процессами. Кое-что можно уже извлечь из того факта, что пауки одного цвета сливаются. Однако по-настоящему интересно становится, когда вступают в борьбу пауки разных цветов.

10.3.1. Дополнительность

Пауки называются *дополнительными*, если выполняется условие

$$\text{[CNOT (grey control, white target)]} = \frac{1}{D} \text{[CNOT (white control, grey target)]} \quad (10.48)$$

или, эквивалентно,

$$\text{[CNOT (white control, grey target)]} = \frac{1}{D} \text{[CNOT (grey control, white target)]} \quad (10.49)$$

Словами это можно выразить так:

(кодирование в ○) ЗАТЕМ (измерение в ●) = (нет потока данных).

Из простого условия (10.48) можно вывести много других равенств. Прежде всего отметим версию для гибридных пауков:

$$\text{Diagram (10.50)} = \frac{1}{D} \text{Diagram (10.50)}$$
(10.50)

что после раскрытия дает

$$\text{Diagram (10.51)} = \frac{1}{D} \text{Diagram (10.51)}$$
(10.51)

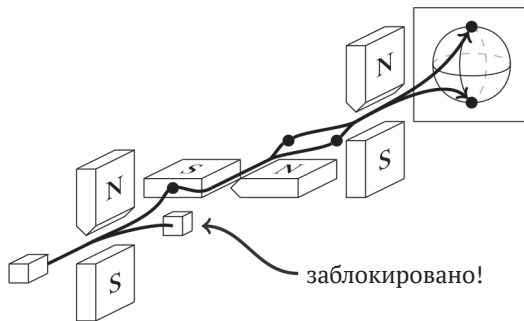
а после дублирования:

$$\text{Diagram (10.52)} = \frac{1}{D^2} \text{Diagram (10.52)}$$
(10.52)

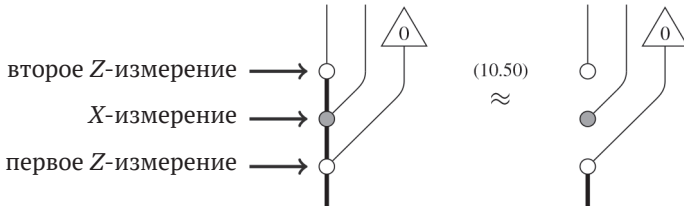
а в сочетании с правилом слияния гибридных и квантовых пауков (10.20) дает еще одно равенство:

$$\text{Diagram (10.53)} = \frac{1}{D^2} \text{Diagram (10.53)}$$
(10.53)

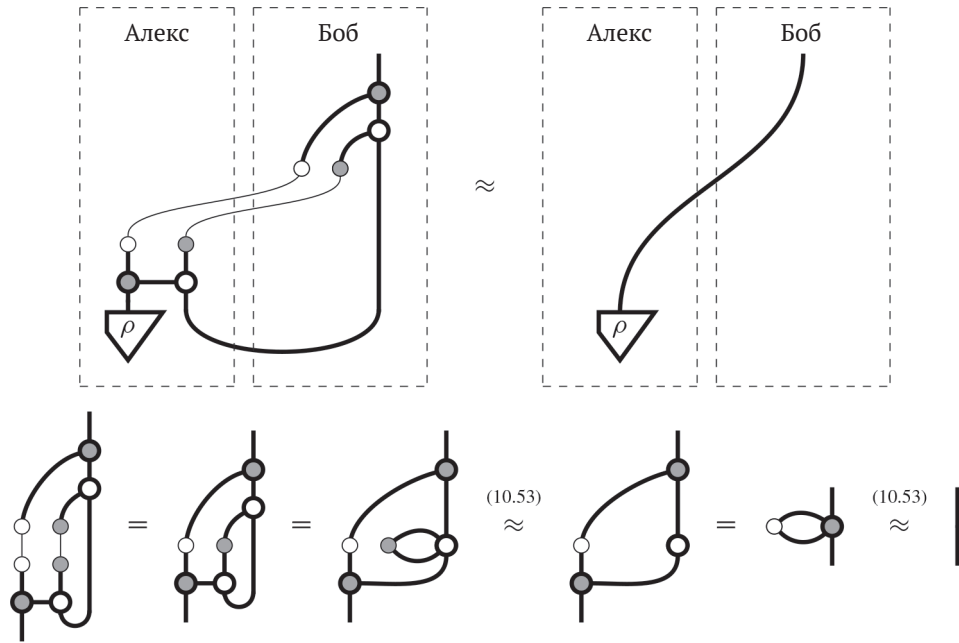
Дополнительность – великое дело. Например, она объясняет поведение прибора Штерна–Герлаха



следующим образом:



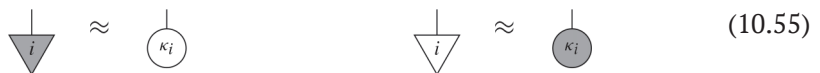
Она обеспечивает магию диаграмм для квантовой телепортации:



и она же лежит в основе базовых свойств классических и квантовых вентилях:



Для дополнительных пауков допускающие копирование состояния одного цвета с точностью до числа совпадают с фазовыми состояниями другого цвета:



Поэтому дополнительность дает несколько новых равенств, правил *к-копирования*:

$$\begin{array}{c} \text{white circle with grey dot} \\ \text{---} \\ \text{white circle with grey dot} \end{array} \approx \begin{array}{c} \text{white circle with grey dot} \\ \text{---} \\ \text{white circle with grey dot} \end{array} \quad \begin{array}{c} \text{white circle with grey dot} \\ \text{---} \\ \text{grey circle with grey dot} \end{array} \approx \begin{array}{c} \text{grey circle with grey dot} \\ \text{---} \\ \text{grey circle with grey dot} \end{array} \quad (10.56)$$

С точностью до глобальной фазы эти допускающие копирование фазовые состояния проходят прямо через фазовые вентили другого цвета:

$$\begin{array}{c} \text{grey circle with grey dot} \\ \text{---} \\ \text{white circle with grey dot} \end{array} = \begin{array}{c} \text{white circle with grey dot} \\ \text{---} \\ \text{white circle with grey dot} \end{array} \quad \begin{array}{c} \text{white circle with grey dot} \\ \text{---} \\ \text{grey circle with grey dot} \end{array} = \begin{array}{c} \text{grey circle with grey dot} \\ \text{---} \\ \text{grey circle with grey dot} \end{array} \quad (10.57)$$

См. также *дополнительность* в разделе 9.2.1; *прибор Штерна–Герлаха* в разделе 9.2.5; *телепортация посредством дополнительнойности* в разделе 9.2.7.

10.3.2. Сильная дополнительность

Пауки называются *сильно дополнительными*, если выполняется условие

$$\begin{array}{c} n \\ \text{---} \\ \text{complete bipartite graph} \\ \text{---} \\ m \end{array} \approx \begin{array}{c} n \\ \text{---} \\ \text{spider diagram} \\ \text{---} \\ m \end{array} \quad (10.58)$$

Сильную дополнительность можно эквивалентно выразить в виде трех правил:

$$\begin{array}{c} \text{spider with 2 legs top, 2 bottom} \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \text{spider with 2 legs top, 2 bottom} \end{array} \quad (10.59)$$

$$\begin{array}{c} \text{spider with 1 leg top, 1 bottom} \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \text{leg} \\ \text{---} \\ \text{leg} \end{array} \quad \begin{array}{c} \text{spider with 1 leg top, 1 bottom} \end{array} = \frac{1}{\sqrt{D}} \begin{array}{c} \text{leg} \\ \text{---} \\ \text{leg} \end{array} \quad (10.60)$$

Хотя у этих правил нет (единственной) естественной интерпретации, как в случае дополнительнойности, тем не менее дополнительность из них следует:

$$\begin{array}{c} \text{spider} \end{array} = \begin{array}{c} \text{spider with crossing} \end{array} = \begin{array}{c} \text{spider with crossing} \end{array} = \begin{array}{c} \text{spider with crossing} \end{array} \approx \begin{array}{c} \text{spider} \end{array} \approx \begin{array}{c} \text{spider} \end{array} \approx \begin{array}{c} \text{spider} \end{array} \quad (10.59) \quad (10.60)$$

Один из способов интерпретировать равенство (10.58) – рассматривать некоторые его части как дублированные, например:

(10.61)

Это следствие сильной дополнителности используется, для того чтобы показать, что корреляции для ГХЦ-состояния принимают определенную форму:

(10.61)

которая будет играть определяющую роль в установлении *квантовой нелокальности*.

Оно дает также целый ряд новых равенств, касающихся копируемых фаз и протекающих из того факта, что для сильно дополнителных пауков результат групповой операции над двумя копируемыми фазами снова является копируемой фазой. Таким образом, копируемые фазы образуют подгруппу фазовой группы, которая называется *классической подгруппой*:

$$\left\{ \begin{array}{c} | \\ \circ \\ \kappa \end{array} \right\}_{\kappa} \subset \left\{ \begin{array}{c} | \\ \circ \\ \alpha \end{array} \right\}_{\alpha} \qquad \left\{ \begin{array}{c} | \\ \bullet \\ \kappa \end{array} \right\}_{\kappa} \subset \left\{ \begin{array}{c} | \\ \bullet \\ \alpha \end{array} \right\}_{\alpha}$$

Итак, помимо правил κ -копирования (10.56), сильная дополнителность влечет также следующие факты:

- единица – копируемое состояние:

(10.62)

- копируемость соответствующих фазовых вентилей:

(10.63)

- коммутирование классических фазовых вентилей с точностью до глобальной фазы:

(10.64)

Для ZX-диаграмм классическая подгруппа имеет вид:

$$\left\{ \begin{array}{c} \text{circle with dot at } 0 \\ \text{circle with arrow at } \pi \end{array} \right\} \subseteq \left\{ \text{circle with arrow at } \alpha \right\}$$

потому что

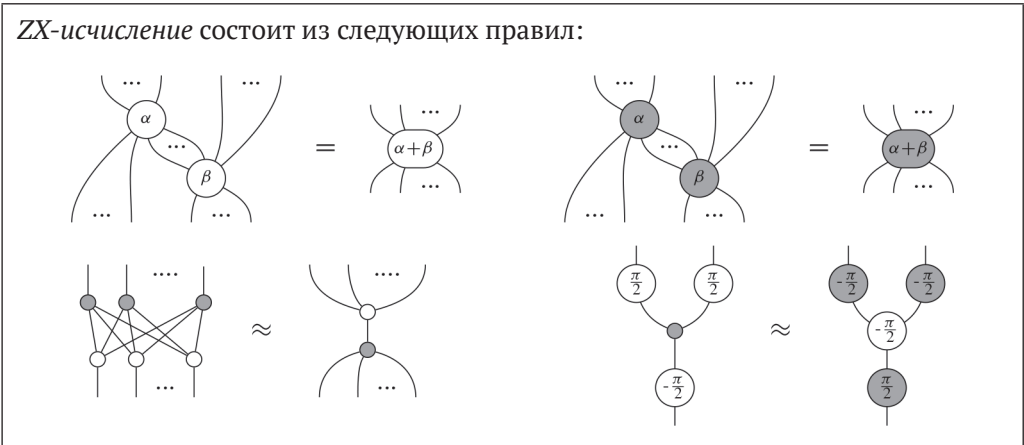
$$\begin{array}{c} \downarrow \\ 0 \end{array} \approx \text{circle with dot at } 0 \qquad \begin{array}{c} \downarrow \\ 1 \end{array} \approx \text{circle with dot at } \pi \qquad (10.65)$$

и аналогично для инвертированных цветов. Но вовсе необязательно верить нам на слово, это можно доказать, применив ZX-исчисление!

См. также сильная дополнительность в разделе 9.3; обобщенная форма и дублирование в разделе 9.3.3; классическая подгруппа в разделе 9.3.4.

10.3.3. ZX-исчисление

ZX-исчисление состоит из следующих правил:



ZX-исчисление является полным графическим исчислением для ZX-диаграмм Клиффорда. То есть любое равенство между двумя ZX-диаграммами доказуемо в ZX-исчислении. Оно состоит из правил трех видов, которые описывают:

- 1) как комбинируются пауки одного цвета;
- 2) как коммутируют пауки разных цветов, меняясь местами;
- 3) как пауки одного цвета преобразуются в пауков другого цвета.

Первое правило – это слияние пауков, а второе проистекает из сильной дополнительности. Поэтому правила первых двух видов справедливы для любых сильно дополнительных пауков. С другой стороны, третье правило, Y-правило, сообщает некую информацию конкретно о кубитах и сфере Блоха, а именно что состояния Y-базиса можно скопировать двумя эквивалентными способами.

Приведенные выше правила – самый краткий известный нам способ описать это исчисление. Но существует удобная альтернативная система, в которой Y-правило заменено *правилом изменения цвета*:

где $\square :=$ (10.66)

Из ZX-исчисления можно также вывести:

○ правило 0-копирования:

(10.67)

и правило π -копирования:

(10.68)

которые подтверждают, что множество $\{0, \pi\}$ действительно образует классическую подгруппу:

(10.69)

○ правило π -коммутирования:

(10.70)

○ правило исключения фазы:

(10.71)

а также правило π -исключения, специализирующее (10.57):

(10.72)

- в совокупности (10.70) и (10.71) дают:

$$(10.73)$$

- правило $\pi/2$ -дополнительности:

$$(10.74)$$

- два эквивалентных выражения Y-базиса:

$$(10.75)$$

- равенства между гибридными пауками, полученные в результате сворачивания и раскрытия:

$$(10.76)$$

$$(10.77)$$

$$(10.78)$$

$$(10.79)$$

- самообратимость H-вентиля:

$$(10.80)$$

Многие из приведенных выше \approx -равенств справедливы с точностью до глобальной фазы, поэтому дублирование дает:

$$(10.81)$$

$$(10.82)$$

$$(10.83)$$

$$(10.84)$$

$$(10.85)$$

$$(10.86)$$

$$(10.87)$$

Таким образом, из четырех скромных уравнений ZX-исчисления мы можем вывести уйму полезного. Но, конечно, мы занимались этим не просто для развлечения (хотя это и правда весело). В следующих четырех главах мы увидим, как эти равенства в сочетании с графическим представлением квантовой теории в целом можно использовать в таких разных областях, как основания квантовой теории, квантовые вычисления, теории квантовых ресурсов и автоматизация доказательств во всех этих дисциплинах.

См. также ZX-исчисление в разделе 9.4 и правило изменения цвета в разделе 9.4.4.

10.4. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

В предыдущих главах мы уже привели все библиографические ссылки, относящиеся к разработке квантового пикторализма, а здесь дадим (несколько своеобразную) временную цепочку событий, приведших в эту точку. Применение диаграмм для обсуждения квантовой телепортации началось с работы Соеске (2003, 2014а).

Данная работы была опубликована только в 2014 году. С этого момента дальнейшее уточнение диаграммного языка было тесно переплетено с разработкой соответствующей теоретико-категорной аксиоматики. Отчасти это было вызвано тем, что диаграммы выглядят как-то несерьезно, а если в статье нет трудной математики, то шансы опубликовать ее в серьезном журнале близки к нулю. Категорная аксиоматика для вышеупомянутой статьи содержится в работе Abramsky and Coecke (2004). Практически все имеющееся в ней сводилось к струнным диаграммам. Разумеется, Пенроуз рисовал струнные диаграммы, начиная с 1970-х годов (Penrose, 1971). Но они не использовались для описания квантовых особенностей, например квантовой телепортации, по той простой причине, что про них тогда никто не знал. Сам Пенроуз даже говорил, что «эта нотация, похожа, пригодна только для личных вычислений, поскольку ее и напечатать-то толком нельзя» в книге, которая, по стечению обстоятельств, тоже выпущена издательством Cambridge University Press (Penrose, 1984).

Дублирование появилось вскоре после статьи 2004 года, несмотря на то что относящиеся к этой теме работы пошли в печать чуть позже. В работе Coecke (2007) дублирование было предложено, чтобы получить корректное правило Борна, и независимо Сэлинджер (Selinger, 2007) применил адъюнкцию к нечистым процессам. В той же работе были введены асимметричные блоки, позволяющие четко различать адъюнкцию, транспонирование и сопряжение. Идея процесса отбрасывания была выдвинута в работе Coecke and Perdrix (2010).

Пауки потребовали эволюционного процесса, начавшегося в 2006 году и занявшего 6 лет (Coecke and Pavlovic, 2007; Coecke and Paquette, 2008; Coecke et al., 2010a, 2012), ушедших на то, чтобы адекватно учесть классические системы и процессы. Полнота паучьих диаграмм доказана в работе Kissinger (2014b). Напротив, фазы и (сильная) дополнительность в терминах пауков появились одновременно (Coecke and Duncan, 2008, 2011). Полнота все еще не доказана, а самые сильные из текущих результатов для ZX-диаграмм приведены в работах Backens (2014a, b).

Причинность, хотя она играет центральную роль в этой книге, стала последним фрагментом картины. Ее важность была осознана с появлением теоретико-информационной аксиоматики в работе Chiribella et al. (2010, 2011).

Глава 11

Основания квантовой теории

Мермин когда-то выразил широко распространенное отношение к квантовой теории фразой «Заткнись и считай». Мы предлагаем другой лозунг: «Заткнись и думай!»

– Люсьен Харди и Роб Спеккенс, 2010

Эта глава посвящена основаниям квантовой теории. Используя все, что вы узнали к этому моменту, мы попытаемся ответить на некоторые очень глубокие вопросы:

- 1) какие особенности природы отражает квантовая теория?
- 2) наоборот, какие особенности физической теории обусловлены природой (точнее, нашим текущим ее пониманием)?
- 3) какие из этих особенностей являются «чисто квантовыми» в том смысле, что не имеют аналогов ни в какой классической физической теории?

Наш подход к этим вопросам будет основан на рассмотрении одного из самых знаменитых (и исторически противоречивых) свойств квантовой теории: *квантовой нелокальности*. Сначала мы дадим точное определение нелокальности и докажем, что она существует в рамках теории **квантовых процессов** и даже в рамках сравнительно небольшой подтеории **каузальных отображений Клиффорда**. Затем мы представим новую процессную теорию, называемую **спек-теорией** (спек), в которую встроена локальность. Удивительно, что теория **отображений Клиффорда** и **спек-теория** совпадают во всем, кроме одного аспекта: фазовой группы одиночной системы. И (еще одно предварительное уведомление!) именно это различие сводит на нет доказательство, работающее для квантовой теории.

11.1. КВАНТОВАЯ НЕЛОКАЛЬНОСТЬ

Квантовая нелокальность – пожалуй, самая плохо понимаемая из новых квантовых особенностей, – как в философском, так и в структурном отношении. Будучи воспитаны в мире, который кажется «классическим», и – главное – получив наконец испортившее нас «классическое» научное образование, мы привыкли ожидать от физической теории двух свойств:

- 1) *реализм*: у физических систем изначально имеются какие-то свойства, а потому исход «измерения» такого свойства в некотором смысле предопределен еще до самого измерения;

2) *локальность*: одна система не может оказать мгновенного воздействия на другую удаленную систему.

Еще на самых ранних этапах кое-что в квантовой теории вызвало глубокое недовольство Эйнштейна, основоположника теории относительности. Он понял, что происходит нечто очень странное:

квантовая теория не является локально-реалистичной теорией.

Первой реакцией многих ученых (включая Эйнштейна) была уверенность в том, что все объясняется просто «неполнотой» квантовой теории. Поскольку любая теория, безусловно, должна быть локальной и реалистичной, проблема квантовой теории заключается в какой-то ошибке, которую нужно исправить.

Но, как вскоре станет ясно, нам придется научиться жить в отсутствие локального реализма. Неспособность какой бы то ни было локально-реалистичной теории повторить предсказания квантовой теории – это и есть то, что мы называем *квантовой нелокальностью*.

11.1.1. Уточнения квантовой теории

Обычно мы считаем, что физическая система обладает некоторыми свойствами, даже когда их никто не наблюдает, а когда мы наблюдаем систему, эти свойства проявляются. Например, цвет карандаша не изменится, если мы на него не смотрим. Реализм стоит за предположением о том, что нечто подобное справедливо и для квантовой теории, т. е. то, что мы видим в результате квантовых измерений, не возникло из ничего в процессе измерения, а имеет некоторые причины в прошлом.

Конечно, в самом начале этой книги, заставляя Дэйва путешествовать с Северного полюса на Южный, мы ясно дали понять, что измерения изменяют состояние системы недетерминированно и что исход измерения не говорит определенно, в каком состоянии находилась система. Теперь мы знаем, что это именно то, что сообщает нам стандартный квантовый формализм.

Однако априори нет никаких причин, мешающих усовершенствовать квантовую теорию таким образом, чтобы исход каждого измерения можно было проследить до чего-то, существовавшего ранее. Быть может, кто-то уже посадил Дэйва в ракету, нацеленную на Южный полюс, и только и ждал, когда мы спросим, где он находится. То есть существуют некоторые *скрытые параметры*, и кажущаяся недетерминированность объясняется тем, что мы о них ничего не знаем. Поэтому если уточнить теорию, включив в нее эти дополнительные параметры, то раз! – и не будет никакой недетерминированности.

Такое уточнение иногда называют *моделью со скрытыми параметрами*, или – в последнее время – *онтологической моделью*. Чтобы избежать философской нагрузки, обременяющей оба этих термина, мы будем говорить просто *уточнение*.

Важнейшая особенность уточнения состоит в том, что как бы хорошо добавление параметров ни объясняло исходы измерения, оно должно сохранять предсказания квантовой теории. Знаменитый пример такого уточнения – теория де Бройля–Бома, в которой постулируется существование неких вездесущих частиц, в любой момент обладающих точными положением и импульсом. Подвох в том, что на них воздействует нечто, распределенное в пространстве и называемое *вол-*

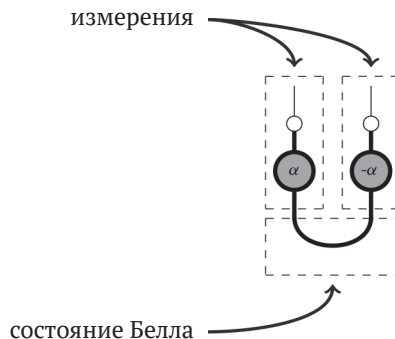
ной-пилотом, что объясняет характерное квантовое поведение, которое, как мы видели в разделе 7.1.4, имеет место при любой попытке произвести измерение этих частиц. Таким образом, эта теория сохраняет реализм ценой отказа от локальности.

С другой стороны, в разделе 6.3 мы видели, что в основе теории относительности лежит положение, согласно которому ничто в природе не может перемещаться быстрее света. Поэтому многие считают отказ от локальности слишком высокой ценой за реализм.

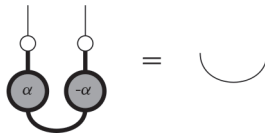
В таком случае мы должны потребовать, чтобы любое уточнение квантовой теории, наделяющее ее детерминированными исходами измерений, было совместимо с теорией относительности. Квантовая теория, конечно, уже удовлетворяет этому условию – благодаря принципу причинности (см. раздел 6.3.2). Чтобы сохранить эту совместимость, все вновь вводимые параметры не должны перемещаться быстрее света.

Так, в частности, любая корреляция, которая может иметь место для пространственно разделенных систем, должна иметь общую причину в прошлом. Иными словами, должен выполняться принцип *общей причины Рейхенбаха*. Этот принцип гласит, что любая корреляция – либо следствие прямой причинной связи, либо вызвана общей причиной. Пример первого – тот факт, что выстрел из ружья причиняет боль (или смерть). Пример второго – сильная корреляция, наблюдавшаяся в прошлом веке между распространением телевизоров в домохозяйствах и гибелью ежей. Общая причина заключается в повсеместном повышении благосостояния, вследствие чего люди покупали не только телевизоры, но и автомобили, под колесами которых гибли ежи. Печально.

Чтобы продемонстрировать противоречие между квантовой теорией и локальным реализмом, мы поступим следующим образом. Рассмотрим тщательно подобранные *сценарии измерения*, т. е. зафиксируем определенное квантовое состояние и измерим каждую из находящихся в нем систем несколькими разными способами. Вычислим вероятности в каждом сценарии, а значит, и *корреляции* между исходами измерений и изучим свойства этих корреляций. Например, если бы мы рассматривали две системы в соединении Белла и подвергли каждую таким измерениям:



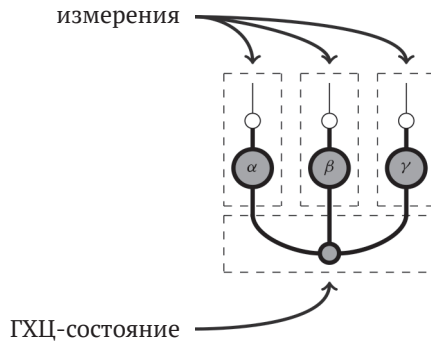
просто воспользовавшись слиянием фазовых пауков, то увидели бы, что исходы измерений обеих систем всегда одинаковы, т. е. между ними существует прямая корреляция:



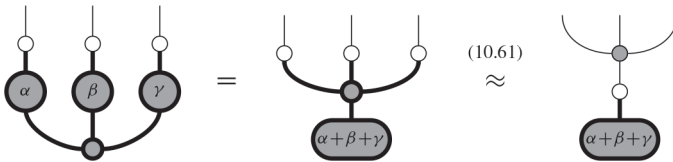
В этом сценарии участвуют квантовые процессы, но, конечно, мы могли бы породить такие же корреляции с помощью какого-нибудь вполне классического (и потому локального) процесса. Чтобы установить противоречие с локальным реализмом, нам потребовалось бы рассмотреть сценарий, в котором имеется несколько разных способов измерения одного и того же квантового состояния.

11.1.2. Сценарии ГХЦ–Мермина

Снова рассмотрим следующие измерения в ГХЦ-состоянии:



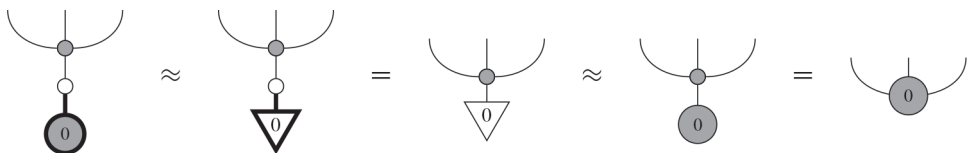
Каждое измерение, по видимости, локально зависит от фазы, но, воспользовавшись слиянием фазовых пауков и сильной дополнителностью, получаем:

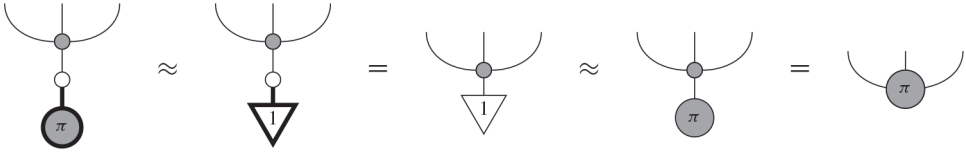


В частных случаях, когда $\alpha + \beta + \gamma$ равно 0 или π , фазовое состояние



принадлежит классической подгруппе для \odot , поэтому в силу (10.69) и (10.26) имеем:



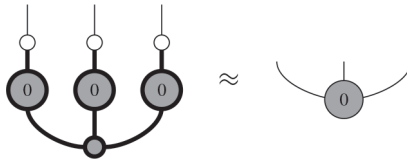


Таким образом, мы получаем четное и нечетное состояния соответственно (см. раздел 9.3.5).

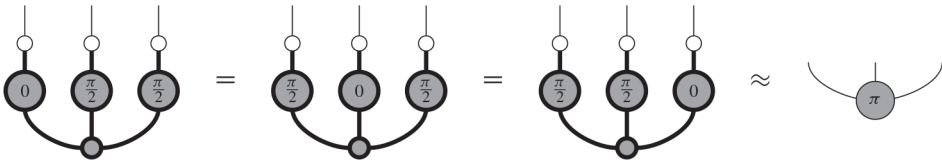
Теперь рассмотрим некоторые конкретные значения фаз α, β и γ . Если положить фазу равной 0, то получается обычное Z-измерение, а если фаза равна $\pi/2$, то получается Y-измерение:



Чтобы получить противоречие с локальным реализмом, нужно рассмотреть конкретный выбор измерений, дающий четное состояние, а именно:



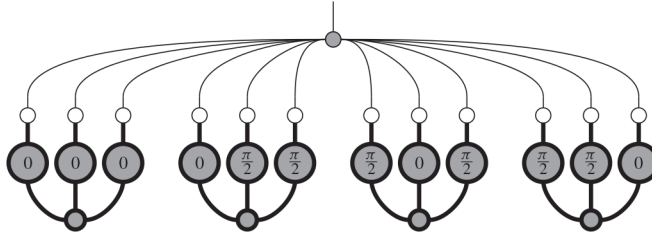
а также три варианта выбора, дающих нечетное состояние:



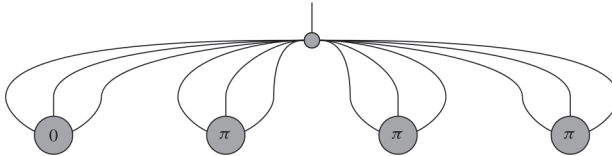
Иными словами, мы рассматриваем следующие измерения:

| | Система A | Система B | Система C |
|-------------|-----------|-----------|-----------|
| Сценарий 1 | Z | Z | Z |
| Сценарий 2a | Z | Y | Y |
| Сценарий 2b | Y | Z | Y |
| Сценарий 2c | Y | Y | Z |

Мы воспользуемся одним свойством совокупности этих сценариев, чтобы продемонстрировать противоречие с локальным реализмом. Это свойство называется «полной четностью»:



Подставляя четности отдельных сценариев:



мы в силу правила слияния фазовых пауков получаем:

$$\begin{array}{c} | \\ \circ \\ \pi \end{array} = \begin{array}{c} | \\ \nabla \\ 1 \end{array}$$

так что полная четность нечетная.

11.1.3. Получение противоречия

Локальный реализм предполагает, что у всех исходов измерений имеется общая причина в прошлом. Поэтому мы построим уточненную модель, в которой классические значения «заранее знают», каким будет для них исход любого измерения:

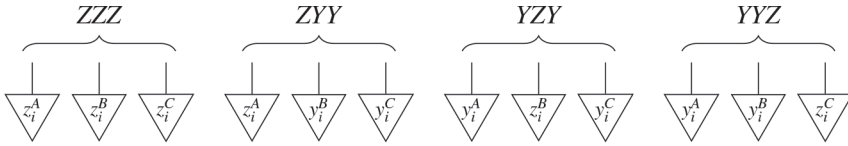
$$\begin{array}{c} \underbrace{\quad\quad\quad}_{\text{1-я система}} \quad \underbrace{\quad\quad\quad}_{\text{2-я система}} \quad \underbrace{\quad\quad\quad}_{\text{3-я система}} \\ \begin{array}{c} \downarrow \\ \nabla \\ z^A \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \\ y^A \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \\ z^B \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \\ y^B \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \\ z^C \end{array} \quad \begin{array}{c} \downarrow \\ \nabla \\ y^C \end{array} \end{array} \quad (11.1)$$

Так, например, если измерить Z в первой системе, то получится исход $z_A \in \{0, 1\}$; если измерить Y в третьей системе, то получится y_C , и т. д. Стало быть, общее состояние системы в этой модели – это распределение вероятностей классических значений:

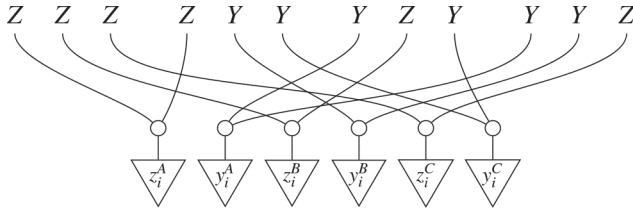
$$\sum_i p^i \begin{array}{c} \downarrow \\ \nabla \\ z_i^A \end{array} \begin{array}{c} \downarrow \\ \nabla \\ y_i^A \end{array} \begin{array}{c} \downarrow \\ \nabla \\ z_i^B \end{array} \begin{array}{c} \downarrow \\ \nabla \\ y_i^B \end{array} \begin{array}{c} \downarrow \\ \nabla \\ z_i^C \end{array} \begin{array}{c} \downarrow \\ \nabla \\ y_i^C \end{array} \quad (11.2)$$

Но мы знаем, что, согласно предсказанию квантовой теории, полная четность для всех четырех измерений всегда нечетна. Следовательно, для совместимости с квантовой теорией любое возможное значение в приведенном выше распределении вероятностей должно давать нечетную полную четность. Однако, как мы сейчас увидим, это неверно ни для какого значения!

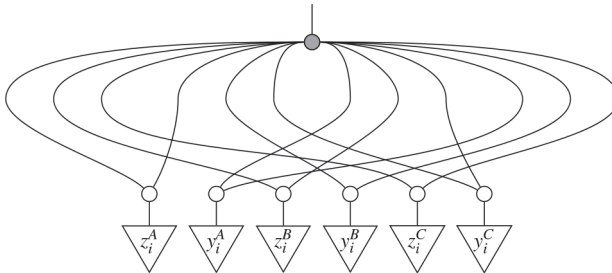
По определению, любое значение в (11.2) дает следующие исходы в каждом из четырех выбранных измерений:



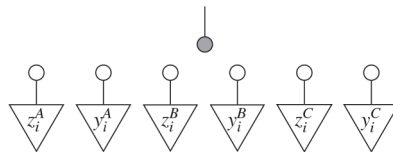
Объединяя дубликаты состояний посредством копирующих пауков, получаем:



Тогда полная четность определяется диаграммой



Внимательно приглядевшись к этому «чудовищному спагетти локальности», мы увидим, что каждого ○-паука соединяют с ●-пауком ровно две ноги. Поэтому, применив уравнение дополненности (10.49), получаем:



что равно

$$\begin{array}{c} \downarrow \\ \bullet \\ 0 \end{array} \approx \begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array}$$

Таким образом, для любого состояния полная четность четна. Поскольку четное не равно нечетному:

$$\begin{array}{c} \downarrow \\ \triangle \\ 0 \end{array} \neq \begin{array}{c} \downarrow \\ \triangle \\ 1 \end{array}$$

квантовая теория нелокальна.

11.2. КВАНТОВОПОДОБНЫЕ ПРОЦЕССНЫЕ ТЕОРИИ

Один из способов понять некоторый объект – разобраться, как он соотносится с похожими объектами. Предположим, к примеру, что мы хотим составить список самых примечательных особенностей додо. Если бы мы сравнивали додо с людьми, то нашли бы массу неинтересных различий, например «додо не имеют пальцев». Но если сравнивать додо с другими птицами, то обнаружится ряд уникальных характеристик. Например, мы сразу отметим их неумение летать и легендарные вкусовые качества (что дает ключ к пониманию того, почему они вымерли!).

Нечто подобное было проделано для квантовой теории путем рассмотрения ее как части более широкого класса теорий. Это можно сделать разными способами в зависимости от того, какие аспекты теории мы хотим изучить и сравнить с другими. Например, много усилий было направлено на то, чтобы интерпретировать квантовую теорию как *пример обобщенной теории вероятностей*. В такой постановке система всегда имеет выпуклое множество состояний (например, шар Блоха в случае кубитов), но многие другие характерные черты квантовой теории начинают «сыпаться».

Можно обратить взгляд в другом направлении: на процессные теории, демонстрирующие похожее диаграммное (т. е. композиционное) поведение, и именно это и будет нас интересовать (естественно!). В главе 9 мы видели, что многие квантовые особенности можно выразить в терминах пауков – чисто диаграммных созданий. Поэтому, просто дав паучьим диаграммам интерпретацию в других процессных теориях, мы сможем увидеть, как выглядят измерения, дополнительность и даже аргументы, касающиеся нелокальности, в «квантовоподобных» процессных теориях.

11.2.1. Дополнительность в теории отношений

В главе 5 мы узнали, что теория **отношений** невыносимо скучна, когда дело доходит до ОНБ. А именно любая система имеет ровно один ОНБ (см. пример 5.6), определяемый набором одноэлементных множеств. Но, добравшись до главы 8, мы, руководствуясь своими целями, заменили ОНБ пауками, и действительно в теории **линейных отображений** фиксирование ОНБ – в точности то же самое, что фиксирование семейства пауков. Конечно, если бы это было верно для **отношений**, то пауки оказались бы такими же скучными, как ОНБ, поскольку существовали бы пауки только одного цвета.

Однако, как выясняется, теория **отношений** гораздо интереснее, чем может показаться на первый взгляд, и существует немало объектов, которые ведут себя как пауки, хотя и происходят не от ОНБ. Например, даже для системы \mathbb{B} существуют пауки двух цветов. Среди прочего это означает, что диаграмма



вполне осмысленна в теории **отношений** (или, точнее, в теории «КК-отношений», которая строится по аналогии с теорией **КК-отображений**), и мы можем производить вычисления с этими пауками так же, как делали все это время.

Пауки первого цвета – это те, что происходят от уникального ОНБ для \mathbb{B} :

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \circ \\ \diagdown \quad \diagup \\ \dots \end{array} \quad :: \quad \left\{ \begin{array}{l} (0, \dots, 0) \mapsto (0, \dots, 0) \\ (1, \dots, 1) \mapsto (1, \dots, 1) \end{array} \right.$$

и легко видеть, что эти создания действительно сливаются, как положено. Но как насчет пауков второго цвета?

Напомним, что в разделе 9.3.5 мы охарактеризовали \bullet -пауков в терминах четности состояний \circ -базиса. Хотя X -базис не переносится в теорию **отношений** (из-за досадного знака минуса во втором базисном состоянии), \bullet -пауки переносятся! А именно положим

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} \quad :: \quad (b_1, \dots, b_m) \mapsto (b'_1, \dots, b'_n)$$

тогда и только тогда, когда количество единиц среди $b_1, \dots, b_m, b'_1, \dots, b'_n$ четно. Частными случаями этих пауков четности являются реляционные версии примеров, которые мы видели в разделе 9.3.5, например реляционное XOR:

$$\begin{array}{c} | \\ \bullet \\ \diagdown \quad \diagup \end{array} \quad :: \quad (i, j) \mapsto i \oplus j$$

и реляционное трехсистемное состояние четности:

$$\begin{array}{c} | \\ \bullet \\ \diagdown \quad \diagup \end{array} \quad :: \quad * \mapsto \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$$

Упражнение 11.1. Покажите, что определенные выше пауки действительно ведут себя как пауки, т. е.

$$\begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array} = \begin{array}{c} \dots \\ \diagup \quad \diagdown \\ \bullet \\ \diagdown \quad \diagup \\ \dots \end{array}$$

а также что имеет место инвариантность относительно перекоммутации ног и сопряжения и что пара \circ/\bullet является сильно дополнительной:

$$\begin{array}{c} \bullet \\ | \\ \circ \\ | \\ \bullet \end{array} = \begin{array}{c} \circ \\ | \\ \bullet \end{array} \quad \begin{array}{c} \circ \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \end{array} \quad \begin{array}{c} \circ \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \end{array} \quad \begin{array}{c} \circ \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \circ \end{array}$$

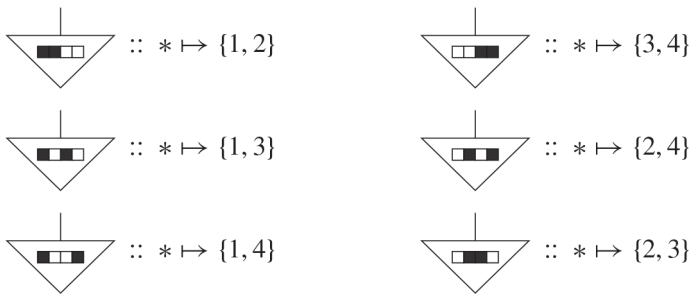
11.2.2. Модельная квантовая теория Спеккенса

Хотя в теории **отношений** есть неразделимые состояния и даже сильно дополнительные пауки, она все же мало напоминает квантовую теорию. Но, как это ни удивительно, существует подтеория теории **отношений**, которая так и обладает многими квантовыми особенностями. Например, состояния наименьшей нетривиальной системы организованы в виде сферы, что очень напоминает ограничение шести состояний для сферы Блоха, с которым мы столкнулись в разделе 9.4.2 при изучении **отображений Клиффорда**. Сначала мы определим эту теорию конкретно (т. е. пойдём «трудным путем»), а затем покажем, что ее можно также получить путем небольшой модификации ZX-исчисления.

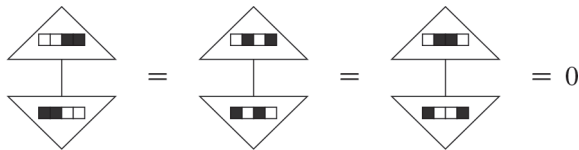
Базовая система в этой новой теории, называемой **спек-теорией**, представляет собой множество из четырех элементов:

$$IV := \{1, 2, 3, 4\}.$$

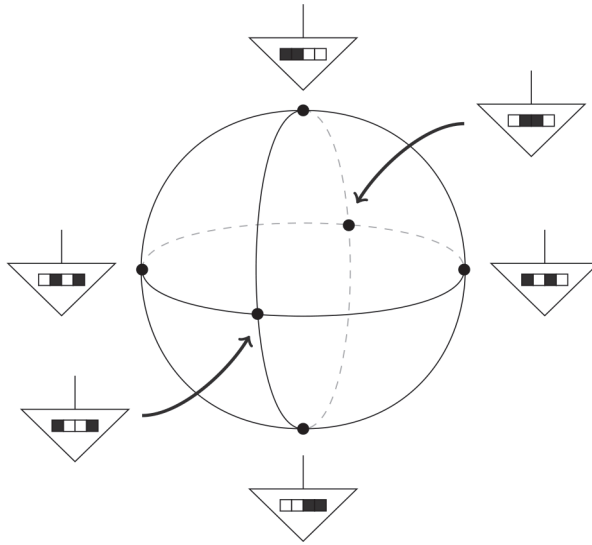
Поскольку это будет подтеория теории **отношений**, состояния IV определяются подмножествами. Но мы возьмем не все $2^4 = 16$ подмножеств IV, а только шесть двухэлементных подмножеств:



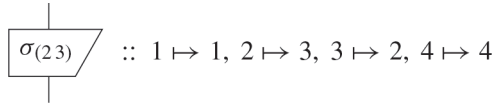
Очевидно, что из них можно составить три пары ортогональных состояний:



поэтому мы – с явным намеком – поместим их на «спек-сферу»:



По аналогии со сферой Блоха будем называть состояния на оси Z спек- Z -состояниями, состояния на оси X – спек- X -состояниями, а состояния на оси Y – спек- Y -состояниями. Это состояния нашей процессной теории, а какие в ней процессы? В одиночной системе мы допускаем произвольные перестановки множества $I\bar{V}$, например:



Поскольку перестановка не может изменить количество заполненных блоков, она переводит любое двухэлементное подмножество в какое-то двухэлементное подмножество, например:



Кроме того, ортогональные состояния переводятся в ортогональные, т. е. антиподы на «спек-сфере» сохраняются. Таким образом, эти перестановки, которые, как легко видеть, являются унитарными, аналогичны однокубитовым унитарным отображениям в теории **отображений Клиффорда**.

Это все, что касается процессов в одиночной системе. Чтобы получить все процессы в спек-теории, нужно добавить одно семейство пауков, а именно пауков, которые копируют спек- Z -состояния:

$$(11.3)$$

Мы называем их пауками $\{1, 2\}$ -четности. В явном виде паук $\{1, 2\}$ -четности определяется отношением:

$$\begin{matrix} n \\ \text{...} \\ \text{...} \\ m \end{matrix} \text{ spider} \quad :: \quad \begin{cases} (a_1, \dots, a_m) \mapsto (b_1, \dots, b_n) \\ (a_1 + 2, \dots, a_m + 2) \mapsto (b_1 + 2, \dots, b_n + 2) \end{cases}$$

для всех $a_i, b_i \in \{1, 2\}$ таких, что количество двоек среди $a_1, \dots, a_m, b_1, \dots, b_n$ четно. На самом деле это единственное семейство пауков, для которого отношение копирования

$$\text{Spider} \quad :: \quad \begin{cases} 1 \mapsto \{(1, 1), (2, 2)\} \\ 2 \mapsto \{(1, 2), (2, 1)\} \\ 3 \mapsto \{(3, 3), (4, 4)\} \\ 4 \mapsto \{(3, 4), (4, 3)\} \end{cases}$$

удовлетворяет условиям (11.3). Более того,

$$\text{Spider} \quad :: \quad * \mapsto \{1, 3\}$$

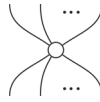
является одним из шести состояний на «спек-сфере», поэтому мы можем достичь любого другого состояния посредством перестановок, например:

Поскольку мы можем восстановить «спек-сферу», используя только пауков и перестановки, то можно определить полную процессную спек-теорию следующим образом.

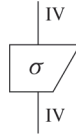
Определение 11.2. Спек-теорией называется следующая подтеория теории отношений:

- системы состоят из n экземпляров множества IV ;
- процессами являются струнные диаграммы, состоящие из:

– пауков $\{1, 2\}$ -четности:



– всех перестановок одной системы:

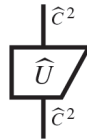


Теперь сравним это со следующей характеристикой **отображений Клиффорда**.
Предложение 11.3. Теорию **отображений Клиффорда** можно эквивалентно определить как следующую подтеорию теории **чистых квантовых отображений**:

- системы состоят из n экземпляров множества $\widehat{\mathbb{C}}^2$;
- процессами являются струнные диаграммы, состоящие из:
 - квантовых Z -пауков:



– всех унитарных отображений Клиффорда одиночной системы:



Доказательство. Очевидно, что любая струнная диаграмма, состоящая из \circ -пауков и унитарных отображений Клиффорда, является диаграммой Клиффорда (см. определение 9.104) и, следовательно, дает отображение Клиффорда. Обратно, следующие диаграммы являются унитарными отображениями Клиффорда одиночной системы:



Из них и \circ -пауков мы можем получить:



=



=



что дает нам все необходимые части для построения произвольной диаграммы Клиффорда. □

Неплохо, правда?

Замечание 11.4. Одно кажущееся различие между **отображениями Клиффорда** и **спек-теорией** заключается в том, что числа в них различны: в теории **отображений Клиффорда** это положительные вещественные числа, а в **спек-теории** – булевы величины. Мы говорим «кажущееся», потому что это легко поправить. Простой способ – считать равенство в теории **отображений Клиффорда** «равенством с точностью до числа», тогда останется только два неравных числа (0 и 1). Чуть более трудоемко, но все же возможно пополнить числа в **спек-теории** положительными вещественными числами и немного подкорректировать определение «соединения процессов проводами», например:

$$\begin{array}{c} \triangle \\ \square \\ \triangle \end{array} = \frac{1}{2}$$

Аналогия между **отображениями Клиффорда** и **спек-теорией** на этом не заканчивается. Точно так же, как мы конструировали \circ -пауков (или спек- Z -пауков), можно сконструировать два других семейства пауков (спек- X -пауков и спек- Y -пауков), которые копируют две другие ортогональные пары состояний.

Упражнение 11.5. Используя \circ -пауков и перестановки, определите новых пауков:



так что



копируют состояния спек- X и спек- Y соответственно.

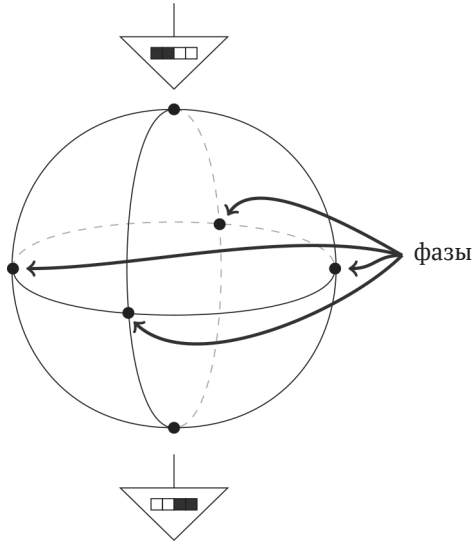
И конечно, они взаимодействуют так, как мы и надеялись.

Упражнение 11.6. Покажите, что спек- \circ -пауки и спек- \bullet -пауки являются сильно дополнительными.

Посмотрим, как далеко заведет нас эта аналогия.

11.2.3. Фазы в спек-теории

Поскольку мы расположили шесть состояний на сфере, возникает соблазн интерпретировать точки на экваторе как фазы:



и попытаться собрать из них (коммутативную) фазовую группу. Как мы вскоре увидим, это действительно возможно. И более того, начав украшать пару сильно дополнительных пауков этими фазами, мы получим универсальность для спек-теории, Y-правило (которое соотносит два разных способа копирования базиса спек-Y) и даже соответствующую теорему о полноте! Но тогда какая же разница может быть между спек-теорией и отображениями Клиффорда?

Читатели, немного знакомые с теорией групп (или почитавшие раздел* 9.3.6), наверное, догадались, каков ответ. Существует ровно две коммутативные группы с четырьмя элементами, и, как выясняется, одна из них – отображения Клиффорда, а другая – спек-теория! В случае отображений Клиффорда фазовая группа совпадает с \mathbb{Z}_4 , циклической группой из четырех элементов. Это множество $\{0, 1, 2, 3\}$, в котором групповой операцией является сложение по модулю 4.

«Постойте-ка! – слышим мы. – А я-то думал, что фазовая группа состоит из поворотов вокруг экватора сферы Блоха».



Да, вы правы! Но если присвоить элементам этой группы другие имена:

$$0 \leftrightarrow 0 \qquad 1 \leftrightarrow \frac{\pi}{2} \qquad 2 \leftrightarrow \pi \qquad 3 \leftrightarrow -\frac{\pi}{2}$$

то станет ясно, что на самом деле это одна и та же группа, например:

$$1 + 2 = 3 \quad \Leftrightarrow \quad \text{circle with } \frac{\pi}{2} \text{ rotation} + \text{circle with } \pi \text{ rotation} = \text{circle with } -\frac{\pi}{2} \text{ rotation}$$

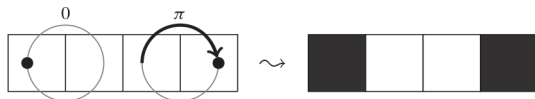
Для фазы спек-Z-состояний должно выполняться условие:

$$\begin{array}{c} \triangle \\ \blacksquare \blacksquare \square \\ \hline \psi \\ \nabla \end{array} = \begin{array}{c} \triangle \\ \square \blacksquare \blacksquare \\ \hline \psi \\ \nabla \end{array} = 1$$

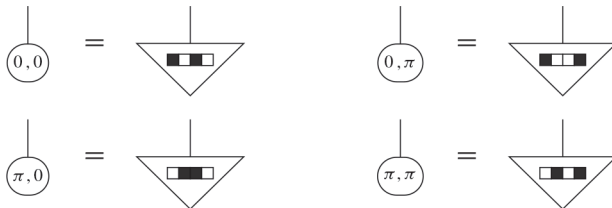
Таким образом, чтобы получить фазовое состояние, мы должны выбрать по одному элементу из множеств {1, 2} и {3, 4}, что дает остальные четыре спек-состояния. Как и в случае кубитов, мы можем составить из них группу, нарисовав колесики. Однако на этот раз рисовать придется два колесика, а не одно, и каждое может быть установлено в положение 0 или π :



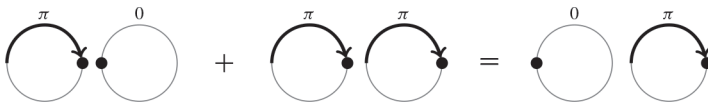
Чтобы понять, какому состоянию соответствует каждое колесико, нужно просто закрасить черным квадратики, в которые попадает черная точка:



Таким образом, получается четыре фазы:



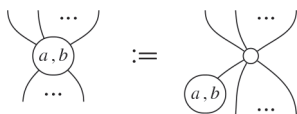
Групповая операция – это просто поэлементное сложение углов, например:



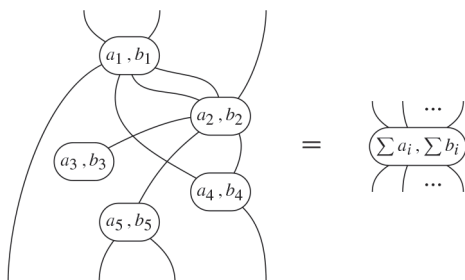
И действительно, можно проверить, что

$$\begin{array}{c} \circ \\ \swarrow \searrow \\ \circ \quad \circ \\ a, b \quad c, d \end{array} = \begin{array}{c} | \\ \text{---} \\ a+c, b+d \end{array}$$

Как и в квантовом случае, новые фазовые состояния можно использовать для украшения новой породы пауков:

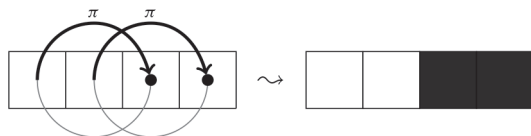


так что удовлетворяется «правило слияния спек-пауков»:

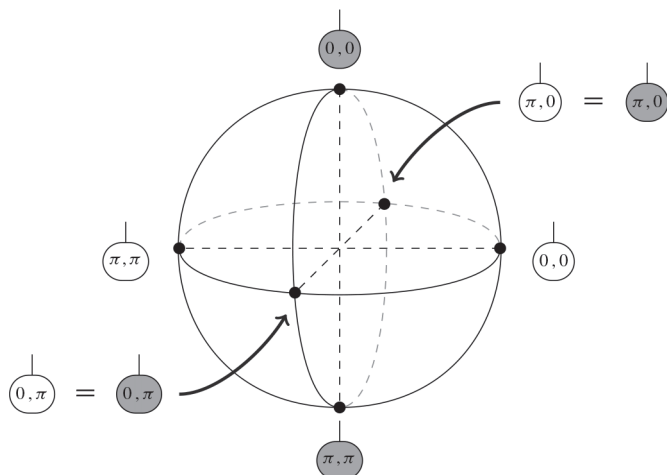


Если фазовая группа для **отображений Клиффорда** – \mathbb{Z}_4 , то эта новая фазовая группа называется $\mathbb{Z}_2 \times \mathbb{Z}_2$. Вместо множества из четырех элементов $\{0, 1, 2, 3\}$, в котором групповой операцией является сложение по модулю 4, тут мы имеем два одинаковых множества из двух элементов $\{0, 1\}$ и сложение по модулю 2.

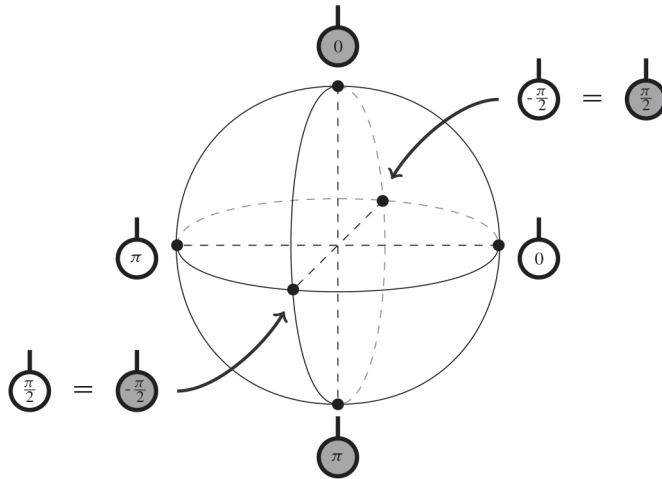
Чтобы образовать фазовые состояния для спек-Х-состояний, мы должны выбрать по одному элементу из множеств $\{1, 3\}$ и $\{2, 4\}$. Чтобы получить это из элемента фазовой группы, мы просто изменим положение колесиков:



что дает нам достаточно фазовых состояний для заполнения спек-сферы:



Давайте-ка еще раз взглянем на сферу Блоха.

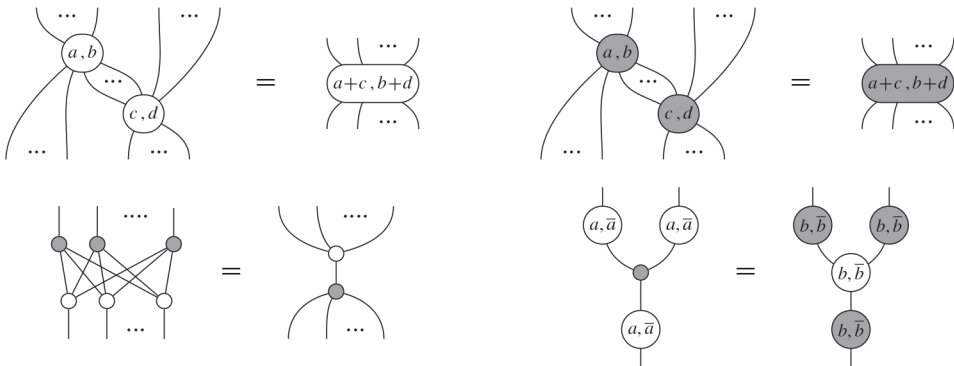


Ух ты! Ну просто близнецы-братья! И вправду начинает казаться, что единственное различие между этими теориями – фазовая группа. На самом деле так оно и есть. Но что означает «изменить фазовую группу» всей процессной теории? Мы можем придать этим словам точный смысл, воспользовавшись нашим старым другом – ZX-исчислением.

11.2.4. ZX-исчисление для спек-теории

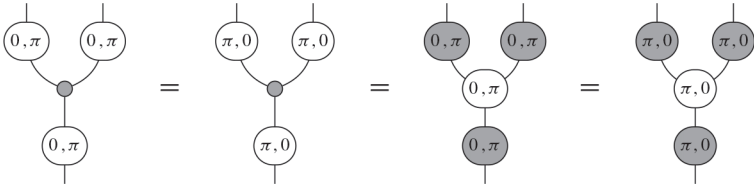
Мы уже знаем, что спек-теория допускает фазовую группу и вариант слияния фазовых пауков. Еще мы знаем, что \circ и \bullet сильно дополнительные. Поэтому мы почти построили полноценное ZX-исчисление для спек-теории. Недостаёт только Y-правила, которое мы сейчас и добавим.

Определение 11.7. ZX-исчисление для спек-теории состоит из следующих правил:

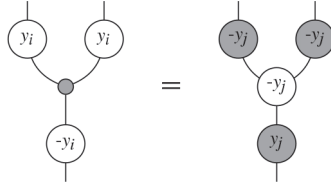


где $a, b, c, d \in \{0, \pi\}$ и a^- – сокращенное обозначение $\pi + a$.

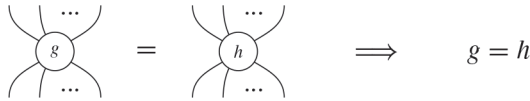
Это определение почти совпадает с определением ZX-исчисления для **отображений Клиффорда**. Даже «расширенное» Y-правило, которое в случае спек-теории соотносит не два, а четыре варианта Y-копирования:



полностью аналогично Y -правилу для **отображений Клиффорда**. То есть оба они для выбранных элементов y_1, y_2 фазовой группы имеют вид:



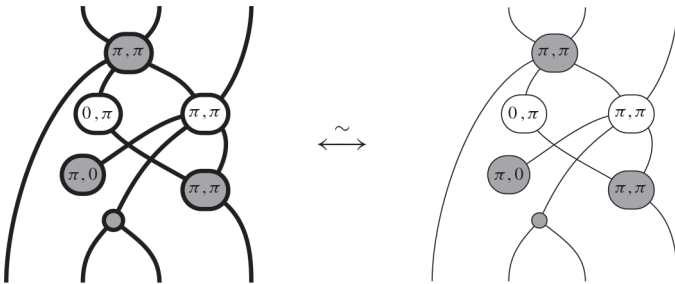
для всех $i, j \in \{1, 2\}$. Если предположить, что $y_1 \neq y_2$ и что украшения пауков определены однозначно, т. е.



то y_1 и y_2 однозначно определяются исчислением (с точностью до переименования некоторых элементов фазовой группы). Для **отображений Клиффорда** должно быть $y_1 := \pi/2$ и $y_2 := -\pi/2$, а для **спек-теории** $-y_1 := (0, \pi)$ и $y_2 := (\pi, 0)$.

Упражнение* 11.8. В теории **отображений Клиффорда** добавочные вариации Y -правила избыточны. Действительно ли они необходимы для **спек-теории**?

Пример 11.9. Поскольку дублирование процессов в любой процессной теории просто устраняет глобальные фазы (см. замечание 6.19), а единственной глобальной фазой в **спек-теории** является 1, то дублирование процессов в **спек-теории** просто дает ту же **спек-теорию**:



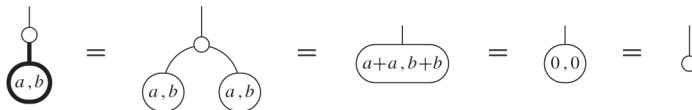
Однако дублирование позволяет нам кодировать измерения:



исходы которых мы можем вычислять с помощью фазовой группы. Например, если произвести \circ -измерение каждого из двух спец- Z состояний, то получится:



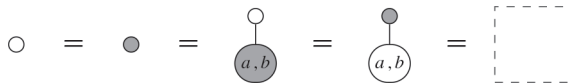
что означает соответственно «навверняка в $\{0, 1\}$ » и «навверняка в $\{2, 3\}$ ». Остальные состояния на спек-сфере являются \circ -фазовыми состояниями, поэтому \circ -измерение для них дает:



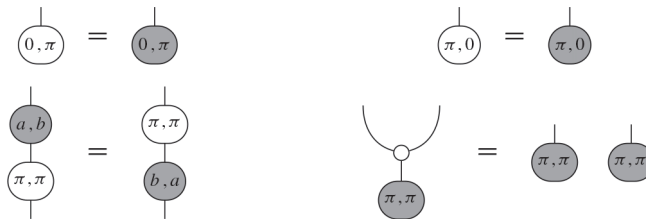
что означает «понятия не имею».

Как и в случае ZX-исчисления для **отображений Клиффорда**, первым делом мы хотим вывести удобные правила.

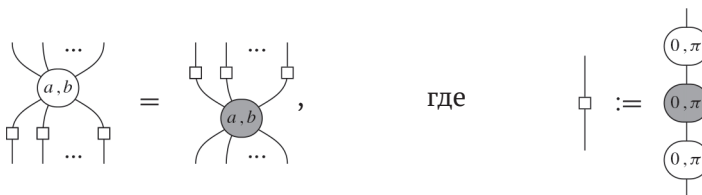
Упражнение 11.10. Предполагая «простые правила», аналогичные равенству (9.107):



покажите, что в ZX-исчислении для **спек-теории** действуют собственные варианты «правил додо», выведенных в разделе 9.4.3:



и правила изменения цвета



Как и в случае **отображений Клиффорда**, для ZX-исчисления для **спек-теории** справедлива следующая теорема.

Теорема 11.11. ZX-исчисление для **спек-теории** полно относительно **спек-теории**.

Доказательство (которое мы здесь не приводим) во многих отношениях повторяет доказательство для **отображений Клиффорда**. А именно для процессов в **спек**-теории можно естественно определить понятие *графовой формы*, к которой можно привести любой процесс. Затем, используя спек-версию правила локального дополнения (9.129), можно доказать, что две диаграммы графовой формы преобразуются друг в друга тогда и только тогда, когда они равны как процессы в **спек**-теории.

Это означает, что, как и в случае **отображений Клиффорда**, мы можем определить **спек**-теорию не конкретно, а как теорию, в которой процессами являются диаграммы фазовых пауков (по модулю равенств в определении 11.7). Таким образом, имеет место следующая теорема.

Теорема 11.12. Единственное различие между **отображениями Клиффорда** и **спек**-теорией заключается в выборе фазовой группы: \mathbb{Z}_4 или $\mathbb{Z}_2 \times \mathbb{Z}_2$.

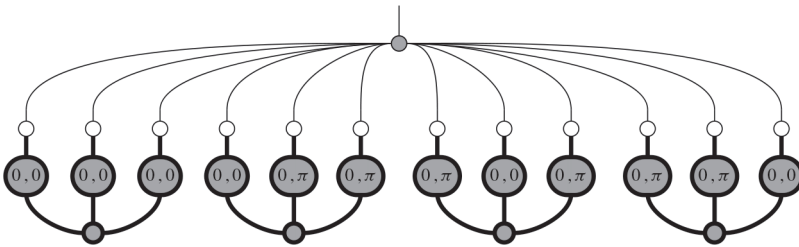
Интересно, а так ли важно это мелкое отличие?

11.2.5. Нелокальность в спек-теории?

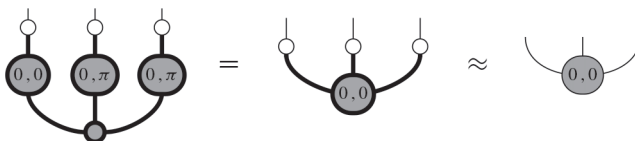
Неужели замена фазовой группы может оказать какое-то влияние? Да, и еще какое! Попробуем воспроизвести сценарий ГХЦ–Мермина из раздела 11.1.2 в **спек**-теории путем дублирования и фиксации некоторых измерений (см. пример 11.9):



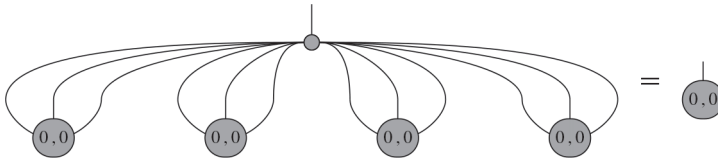
Ранее локально-реалистичная теория предсказывала, что полная четность



должна быть четной, т. е. иметь фазу 0, или в **спек**-теории – $(0, 0)$. Поскольку в теории **отображений Клиффорда** мы получали фазу π , квантовая теория нелокальна. Но т. к. в **спек**-теории фазовая группа совпадает с $\mathbb{Z}_2 \times \mathbb{Z}_2$, все пары $(0, \pi)$ -фаз взаимно уничтожаются, например:

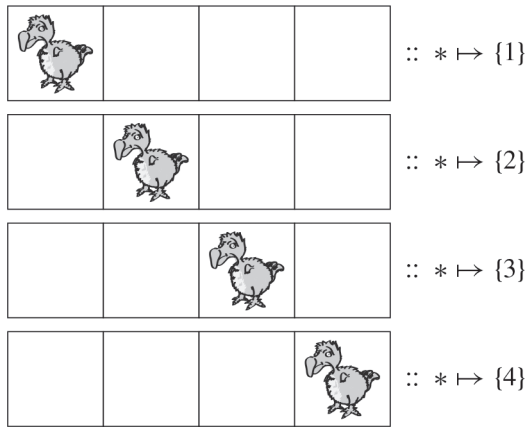


Следовательно, мы получаем:

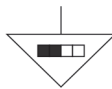


и противоречие исчезает! На самом деле попытка доказательства нелокальности **спек**-теории обречена на провал, какие бы измерения мы ни производили. Это объясняется тем, что **спек**-теория по построению локально-реалистична!

Чтобы убедиться в этом, нужно лишь понять, что на самом деле означают состояния в **спек**-теории. В разделе 3.4.1 мы видели, что в теории **отношений** состояния представляют недетерминированность. То есть множество IV можно рассматривать как (классическую) систему, находящуюся в одном из четырех возможных состояний. Например, это может быть набор четырех клеток, в одной из которых спрятался Дэйв:



Поскольку такие состояния представляют некоторое реальное положение вещей, они называются *онтическими* (объективными). С другой стороны, может случиться так, что мы не знаем точно, где находится Дэйв, но знаем, что он в одной из первых двух клеток:



Поскольку это состояние представляет не реальное состояние системы, а лишь наше знание о ней, оно называется *эпистемическим* (гносеологическим).

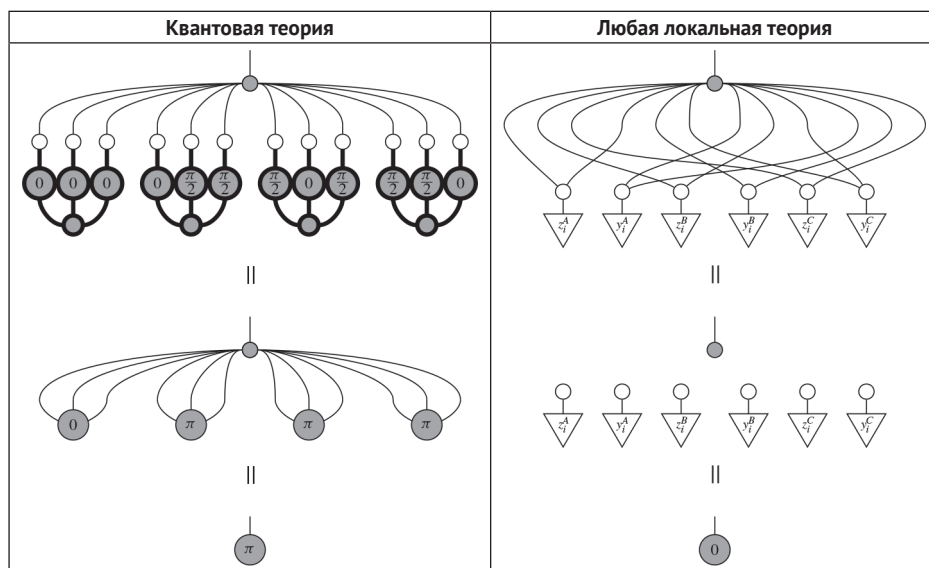
Принципиальный аспект **спек**-теории заключается в том, что налагаются ограничения на допустимые эпистемические состояния, так что мы никогда не знаем точно, в какой клетке находится Дэйв. Отсюда вытекает много, на первый взгляд, квантовых особенностей, таких как (сильная) дополнительность, неразделимость

систем и нечто, очень напоминающее сферу Блоха. Но в конечном итоге эта теория с самого начала разрабатывалась так, чтобы ее всегда можно было уточнить до локально-реалистической, просто введя некоторые онтические состояния в качестве скрытых параметров.

Упражнение* 11.13. Преобразуйте ZX-исчисление в графическое исчисление для квантовой системы, отличной от кубитов. Какие теории можно получить путем изменения фазовой группы?

11.3. Итоги: что следует запомнить

1. Квантовая теория не является *локально-реалистичной*, т. е. любое уточнение квантовой теории, в котором все исходы измерений имеют некоторую общую причину в прошлом, обязано нарушать локальность.
2. Этот факт можно установить, придя к противоречию с помощью диаграмм:



3. В теории **отношений** существуют дополнительные пауки даже на двухэлементном множестве \mathbb{B} .
4. Модельную теорию Спеккенса, близко напоминающую квантовую теорию для кубитов, можно сформулировать как процессную **спек**-теорию, являющуюся подтеорией теории **отношений**. Ее также можно сформулировать с помощью одних лишь диаграмм как модификацию ZX-исчисления; для этого достаточно заменить группу \mathbb{Z}_4 группой $\mathbb{Z}_2 \times \mathbb{Z}_2$.
5. Квантовая нелокальность, и сценарий ГХЦ–Мермина в частности, тесно связана с тем фактом, что фазовая группа для кубитов включает \mathbb{Z}_4 . Напротив, фазовая группа в модельной теории Спеккенса не содержит \mathbb{Z}_4 .
6. Вообще, изучение **квантовой теории** в более широком контексте процессных теорий позволяет понять, какие части теории являются причиной ее удивительных свойств.

11.4. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Рассуждение ГХЦ–Мермина первоначально было опубликовано в несколько более сложной форме в работе Greenberger et al. (1990), а в ее настоящем виде предложено в работе Mermin (1990). Первое, чрезмерно усложненное диаграммное доказательство дано в работе Coecke et al. (2012). Но довольно скоро авторы опомнились и предложили доказательство, представленное в этом разделе (Coecke et al., 2016). Обобщения данного рассуждения можно найти в работе Gogioso and Zeng (2015).

Первое доказательство нелокальности изложено Джоном Беллом (John Bell, 1964), а озабоченность Эйнштейна, которая послужила стимулом к дискуссиям, приведшим к теореме Белла, высказана в работах (Einstein et al., 1935; Einstein, 1936). Первая экспериментальная проверка описана в работе Aspect et al. (1981), но лишь недавно был поставлен эксперимент, который широко признан безупречным (Hensen et al., 2015). Модель со скрытыми переменными Дэвида Бома впервые опубликована в работе (Bohm, 1952a,b).

Тот факт, что дополнительность можно представить в теории **отношений**, замечен в работе Coecke and Edwards (2011), где также впервые представлена **спек**-теория как подтеория теории **отношений**. Павлович (Pavlovic, 2009) классифицировал всех пауков в теории отношений, а все пары сильно дополнительных пауков были классифицированы в работе Evans et al. (2009) и независимо Эдвардсом. Собрание фактов, касающихся множеств и отношений, см. в работе (2015a).

Спеккенс представил свою модельную теорию в работе Spekkens (2007). Раньше очень похожая, но не столь подробно разработанная модельная теория была предложена в работе Hardy (1999). Вместо полного изложения теории Спеккенс привел рецепт для порождения всех состояний и процессов, не показав, что таким образом можно получить непротиворечивую теорию. Ключом к этому рецепту был принцип баланса знаний, ограничивающий достижимый объем знаний о системе. То, что рецепт Спеккенса действительно дает непротиворечивую теорию, было установлено в работе Coecke and Edwards (2012) путем его соотнесения со **спек**-теорией. В этой же работе было помещено теоретико-процессное граффити под Оксфордским мостом:



Оба лагеря объединили силы для выяснения того, что именно в фазовой группе инкапсулированы истинные различия между квантовой и модельной теориями (Coecke et al., 2011b). Эта работа стала потом основой докторской диссертации Эд-

вардса (Edwards, 2009), содержащей дальнейшее развитие. Где сейчас находится Эдвардс, нам неизвестно.

В работе Backens and Nabi Duman (2015) пришло осознание того, что, немного подправив ZX-исчисление, можно получить **спек**-теорию, и там же была доказана соответствующая теорема о полноте, которая поставила точку в полностью диаграммном оформлении модельной теории Спеккенса.

Эпиграф в начале этой главы взят из работы Hardy and Spekkens (2010). См. также обсуждение цитаты Мермина в разделе 1.3.

Глава 12

Квантовые вычисления

Во имя Пасты, и Соуса, и Святых Фрикаделек...

– Бобби Хендерсон

«Евангелие от Летящего
Макаронного Монстра», 2006

За концептуальными основами следует практика. Если изучение оснований квантовой теории столь же старо, сколь и сама квантовая теория, то квантовые вычисления появились сравнительно недавно. Настолько недавно, что крупномасштабные практические квантовые вычисления пока еще не стали реальностью. На сборку и настройку типичного «квантового компьютера» нужно потратить много месяцев, прежде чем можно будет решить такие поражающие воображение задачи, как разложение числа 6 в произведение 3×2 . Тем не менее если бы такие машины существовали, то мы смогли бы многократно ускорить решение некоторых трудных (классических) вычислительных задач, в том числе имеющих отношение ко взлому огромного количества ныне работающих криптографических систем.

Прежде чем переходить к «квантовым вычислениям», нужно сказать несколько слов о «вычислениях» вообще. Что такое вычисление? К этому моменту наш ответ, наверное, не повергнет вас в ступор: это процессная теория! По существу, вычисление – не что иное, как соединение входов и выходов небольших процессов для получения более крупных процессов. Точнее, *вычисление* состоит из конечного множества базовых процессов, соединяемых между собой в соответствии с инструкциями (число которых также конечно), которые мы называем *алгоритмом*, или попросту *программой*.

Единственное существенное различие между классическим и квантовым вычислениями – содержание базовых процессов. В случае классического вычисления они включают такие вещи, как логические операции (например, XOR) или чтение-запись памяти. В случае квантовых вычислений мы можем добавить сюда квантовые процессы и классически-квантовые взаимодействия типа измерений. Поэтому смысл квантовых вычислений – понять, как следует писать новые виды программ, в которых эти новые строительные блоки задействованы для построения более быстрых алгоритмов или для решения задач, которые ранее считались неразрешимыми.

Первые квантовые алгоритмы были «доказательствами правильности концепции» в том смысле, что они решали некоторую задачу гораздо быстрее классического компьютера, но сами решаемые ими задачи были не особенно интересны. Однако все кардинально изменилось с изобретением алгоритмов *квантового по-*

иска Гровера и разложения на множители Шора. Второй из них продемонстрировал применение квантовых компьютеров для эффективного разложения больших чисел на множители. Он представляет огромный интерес по одной простой причине: подавляющее большинство современных криптографических систем основано на алгоритме RSA, который опирается на предположение о вычислительной неразрешимости задачи о факторизации больших чисел. Более того, практически все альтернативы RSA (кроме горстки так называемых постквантовых систем) зависят от тесно связанной задачи вычисления «дискретных логарифмов». И задачу разложения на множители, и эту задачу можно эффективно решить как частные случаи задачи о скрытой подгруппе, которую мы поставим в разделе 12.2.4. Итак, как только появятся квантовые компьютеры, замочек в адресной строке браузера, означающий, что данные вашего банковского счета зашифрованы, станет ничего не значащим украшением (хотя квантовому хакеру, наверное, более интересны вещи посерьезнее величины вашего овердрафта).

В этой главе мы объединим в вычисления уже знакомые нам классически-квантовые строительные блоки. Сделать это можно разными способами, т. е. существует много моделей квантовых вычислений. Мы сосредоточим внимание на двух таких моделях, первая из которых – модель квантовых схем – более-менее очевидным образом обобщает классическую концепцию вычислений с помощью схем на квантовые процессы. Но начнем мы не с битов и выполнения классических логических вентилях, а с кубитов, выполнения квантовых вентилях и измерения того, что получилось.

Вторая, куда более экстравагантная модель называется *основанным на измерениях квантовым вычислением* (measurement-based quantum computation – MBQC). Она вообще опирается не на логические вентиля или нечто подобное, а только на измерения. В основе MBQC лежит чисто квантовое свойство измерений вносить кардинальные изменения в состояние, требуемое для выполнения любого вычисления, и потому эта модель не похожа ни что известное по классическим вычислениям.

Обе модели можно выразить с помощью ZX-исчисления, которое позволяет рассуждать и доказывать утверждения о них, пользуясь только диаграммами, а также транслировать вычисления из одной модели в другую. На самом деле это улица с двусторонним движением. Две самые важные теоремы из главы 9 (универсальность и полнота ZX-исчисления) получаются кодированием ZX-диаграмм в схемной модели и в MBQC соответственно.

12.1. СХЕМНАЯ МОДЕЛЬ

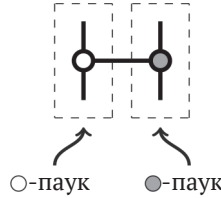
Модель квантовых схем – непосредственное обобщение вычислений с помощью схем, состоящих из классических логических вентилях (например, AND, OR, NOT), на квантовые процессы. Все вычисления в схемной модели выполняются в три этапа:

- 1) подготовить некоторые кубиты в определенном фиксированном состоянии;
- 2) выполнить схему, состоящую из базовых квантовых вентилях;
- 3) измерить некоторые получившиеся кубиты.

Как и в классических схемах, мы предполагаем, что набор базовых квантовых вентилях определен заранее. Типичные примеры – фазовые вентилях:



и вентиль CNOT

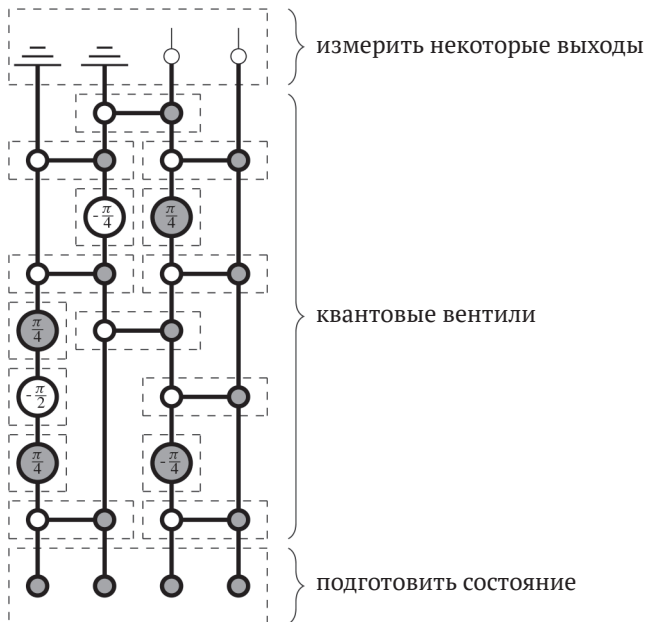


Таким образом, в общем случае пауков следует интерпретировать не как вентили, а как «фрагменты вентиляей». Например, ни один из квантовых пауков в вентиле CNOT сам по себе не является унитарным, но в совокупности они составляют унитарный квантовый вентиль. Затем правила ZX-исчисления, управляющие этими пауками, дают результирующие вентили. На самом деле можно даже сделать следующее (хотя мы и не рекомендуем это).

Упражнение* 12.1. Постройте эквивалентное представление ZX-исчисления, пользуясь только равенствами, включающими фазовые вентили и вентиль CNOT.

12.1.1. Квантовые вычисления как ZX-диаграммы

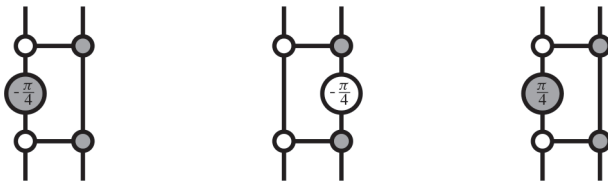
В совокупности три этапа квантового вычисления в схемной модели дают ZX-диаграмму вида:



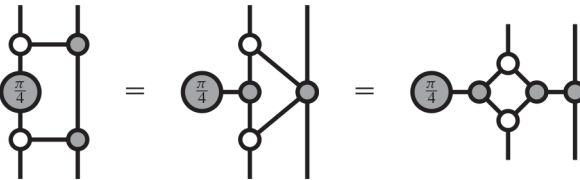
Теперь мы можем воспользоваться ZX-исчислением для выписывания равенств между вычислениями. Если такая диаграмма включает только фазы, кратные $\pi/2$, или только однокубитовые вентили с фазами, кратными $\pi/4$, то из теорем 9.129 и 9.132 соответственно мы знаем, что любое равенство, справедливое для схем, состоящих из таких вентилей, выводимо в ZX-исчислении. Однако ZX-исчисление очень полезно и для более общих схем.

Посмотрим, к примеру, что ZX-исчисление может сказать нам о довольно сложной схеме, изображенной выше. Если попытаться оставить квантовые вентили в покое, то мы окажемся в тупике, но что, если на время забыть о том, что средняя часть состоит из квантовых вентилей, и обращаться с ней, как с любой ZX-диаграммой? Вот тогда-то и случится сеанс ZX-магии!

Для начала рассмотрим следующие фрагменты диаграммы:



Забыв, что мы имеем дело с вентилями, можно выделить 4-цикл:



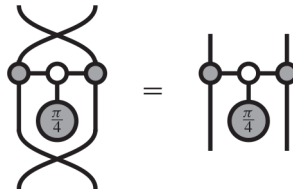
и воспользоваться правилами сильной дополнителности:



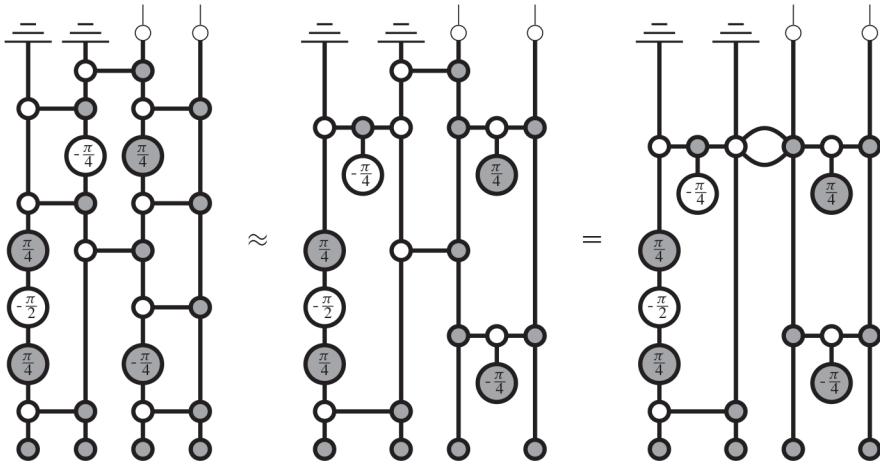
Аналогично имеем:



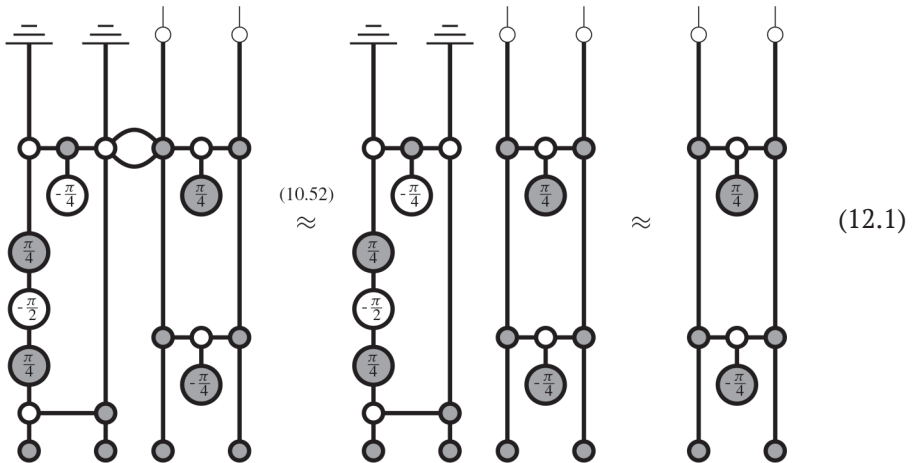
Одним из следствий является факт, который раньше был незаметен: эти фрагменты симметричны относительно двух своих входов:



А после подстановки в большую схему получаем еще более удивительный результат:



В силу дополнителности левая часть схемы отделяется от правой части, поэтому (отброшенная) левая часть вообще не дает никакого эффекта:



Поскольку далее мы имеем

(12.2)

(что легко показать, если преобразовать диаграммы обратно в вентиляную форму), то наша сложная схема на проверку оказывается совсем не такой сложной:

(12.1) (12.2) (10.77)

Упражнение 12.2. Вместо того чтобы возвращаться к вентиляной форме, докажите равенство (12.2) непосредственно, пользуясь сильной дополнительностью.

12.1.2. Построение квантовых вентилях в виде ZX-диаграмм

Квантовые вентилях – это простые унитарные квантовые процессы, которые можно использовать для построения более сложных. Мы уже видели несколько кандидатов на роль квантовых вентилях, например фазовые вентилях и вентиль CNOT. Теперь построим более сложные вентилях, используя фазовых пауков в качестве «фрагментов вентилях».

Напомним (см. пример 9.80), что можно использовать равенства

$$\begin{array}{cc}
 \begin{array}{c} \text{---} \\ \text{---} \\ \nabla \\ 0 \end{array} & \stackrel{(10.65)}{\approx} & \begin{array}{c} \text{---} \\ \bigcirc \\ 0 \end{array} & &
 \begin{array}{c} \text{---} \\ \text{---} \\ \nabla \\ 1 \end{array} & \stackrel{(10.65)}{\approx} & \begin{array}{c} \text{---} \\ \bigcirc \\ \pi \end{array}
 \end{array}$$

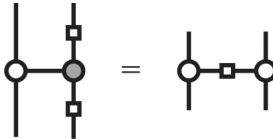
для вывода того факта, что в вентиле CNOT левый кубит, называемый *управляющим кубитом*, служит для решения о том, что делать с правым кубитом: ничего или применить \bullet -фазу π :



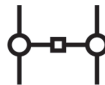
Естественно, можно задаться вопросом, возможно ли построить управляемые версии других операций, например управляемое применение \circ -фазы π . Приведенные выше равенства подсказывают простой способ сделать это с применением правила изменения цвета (10.81):



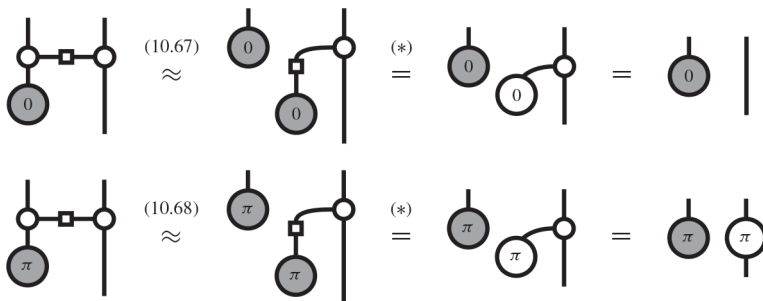
После небольшого упрощения получаем:



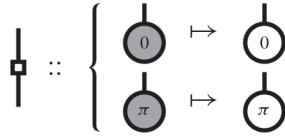
Определение 12.3. *CZ-вентилем* называется диаграмма



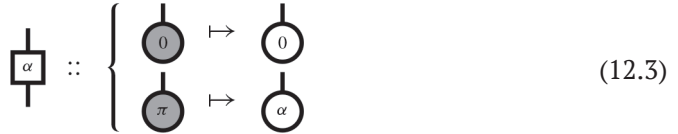
А что, если вместо избирательного применения \circ -фазы π мы хотим избирательно применить произвольную фазу α ? Как построить такую штуку? Ключ дает более внимательное изучение работы CZ-вентиля:



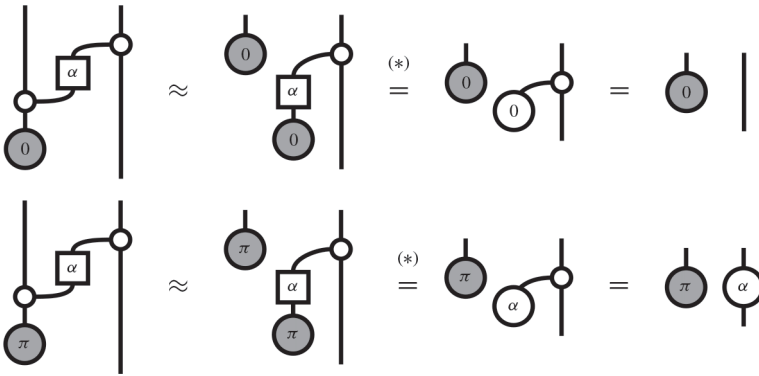
В обоих рассуждениях ключевым шагом, помеченным (*), является место, где *H*-вентиль превращает \bullet -фазовое состояние в \circ -фазовое:



Если бы мы могли обобщить это, заменив π произвольной фазой α :



то имели бы

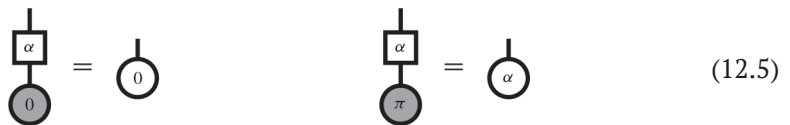


Благодаря ZX-исчислению построить вентиль (12.3) не так уж трудно.

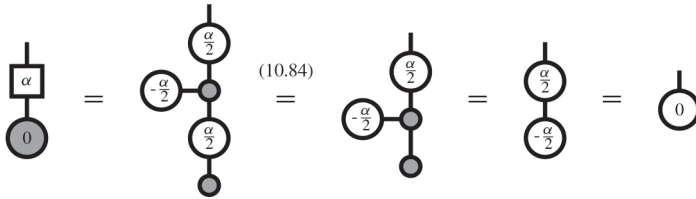
Предложение 12.4. Для



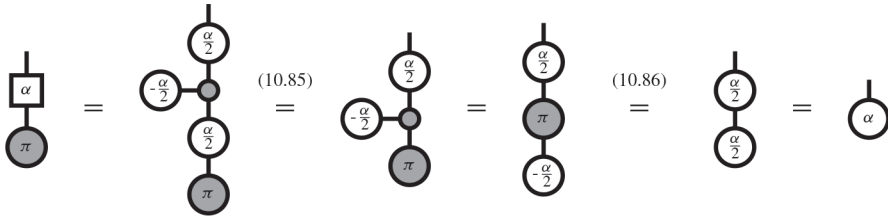
имеет место



Доказательство. Для \bullet -фазы 0 имеем:

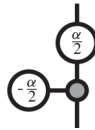


т. е. фазы $\alpha/2$ и $-\alpha/2$ сокращаются, а для \bullet -фазы π



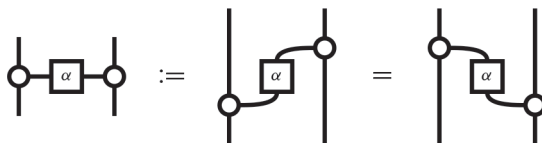
фазы $\alpha/2$ и $\alpha/2$ складываются. □

Замечание 12.5. Если просто смотреть, как α -блок воздействует на состояния Z -базиса, то \circ -фаза в нижней части α -блока не играет никакой роли, т. е. процесс

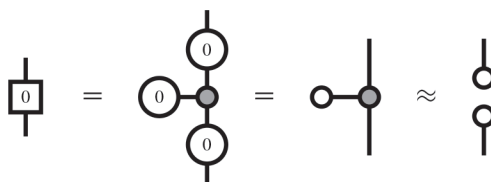


делает то же самое. Важная особенность α -блока состоит в том, что в зависимости от входа обе фазы либо складываются, либо сокращаются. Однако включение этой добавочной фазы удобно, потому что делает α -блок самотранспонированным, а ряд других вещей – более элегантными (см. предложение 12.7 ниже).

Как и H -вентиль, этот α -блок самотранспонированный, поэтому мы можем игнорировать направление провода, не опасаясь путаницы:



Но, в отличие от H -вентилья, этот α -блок не является унитарным для всех α . Например, он даже разделяется:

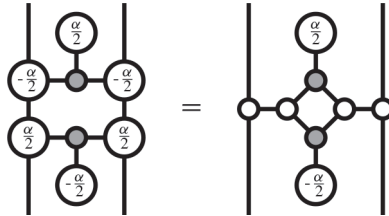


Поэтому, как и пауков в вентиле CNOT, его следует рассматривать как «часть вентиля», на основе которой можно строить интересные квантовые вентиля, самым важным из которых является рассмотренный выше.

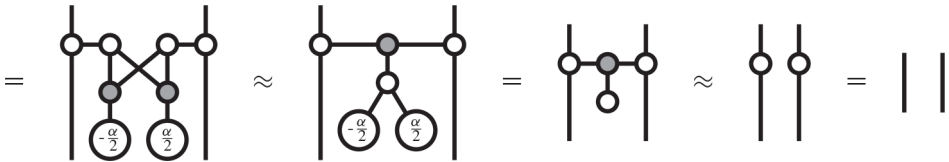
Предложение 12.6. Следующий $CZ(\alpha)$ -вентиль унитарный:

$$\text{CZ}(\alpha) = \text{Phase}(\frac{\alpha}{2}) \text{Phase}(-\frac{\alpha}{2}) \text{Phase}(\frac{\alpha}{2}) \text{Phase}(-\frac{\alpha}{2}) \quad (12.6)$$

Доказательство. Мы воспользуемся тем же приемом, что в разделе 12.1.1, чтобы упростить большую диаграмму. Так как можно выделить 4-цикл



то ясно, какое правило использовать:



и аналогично для второй композиции. □

Можно ожидать, что CZ -вентиль восстанавливается в случае $\alpha := \pi$. Это действительно выглядит многообещающим, поскольку специализация равенств (12.5) дает:

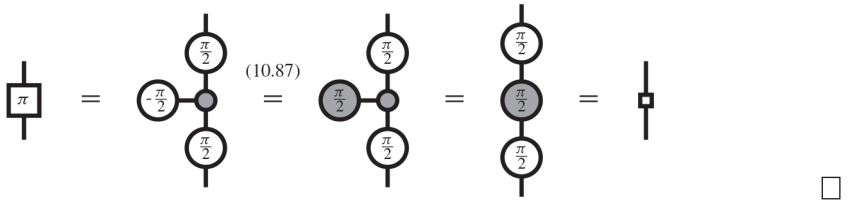
$$\text{CZ}(\pi)_{\text{control } 0} = \text{Line} \quad \text{CZ}(\pi)_{\text{control } \pi} = \text{Phase}(\pi) \quad (12.7)$$

Таким образом, это отображение переводит состояния (дублированного) Z -базиса в состояния (дублированного) X -базиса. Иными словами, складывается впечатление, что оно ведет себя, как H -вентиль. Однако еще из раздела 6.1.5 мы знаем, что дублированный ОНБ не является ОНБ, поэтому все равно нужно проверить, что это действительно H -вентиль.

Предложение 12.7. π -блок эквивалентен H -вентилю:

$$\pi\text{-block} = H\text{-gate} \quad (12.8)$$

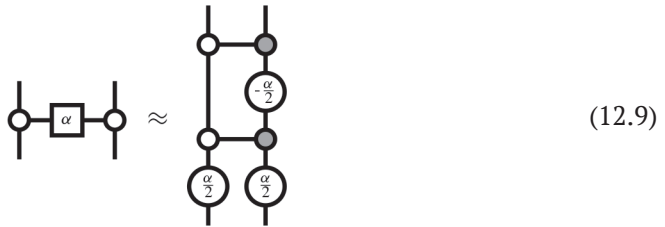
Доказательство. Имеем:



□

Предложение 12.6 дает простую форму CZ(α)-вентиль, который мы построили как ZX-диаграмму с использованием «частей вентиля». Но действительно ли это новый квантовый вентиль, или его можно построить из уже известных базовых вентилях? Ответ снова дает ZX-исчисление.

Упражнение 12.8. Пользуясь ZX-исчислением, покажите, что CZ(α)-вентиль можно построить из вентилях CNOT и фазовых \circ -вентилей следующим образом:

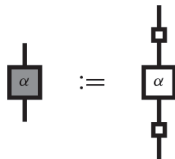


(Указание: правая часть содержит 4-цикл.)

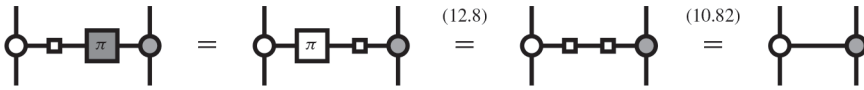
Мы можем рассмотреть X -версию этого вентиля, называемую CX(α)-вентилем, выполнив пред- и посткомпозицию с H -вентилем на втором кубите:



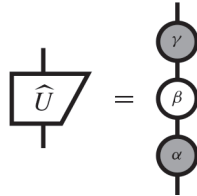
где



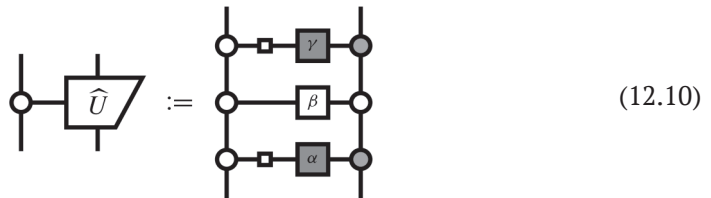
Теперь CNOT (он же CX) возникает как частный случай при $\alpha = \pi$:



Поскольку мы можем конструировать управляемые фазы обоих цветов, то можно сконструировать и управляемые унитарные отображения, используя разложение по углам Эйлера из предложения 9.100. Если \hat{U} имеет разложение



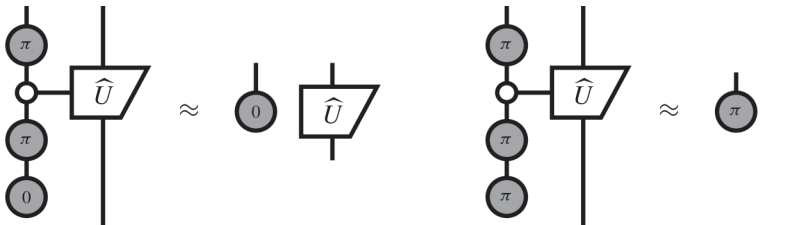
то вентиль «управляемый- \hat{U} » можно построить так:



Унитарное отображение \hat{U} «срабатывает», только если управляющий кубит равен «1»:



Если выполнить пред- и посткомпозицию управляющего кубита с вентилями NOT, то получим инвертированные равенства:



Теперь эти два равенства можно скомбинировать, чтобы избирательно выполнять \hat{U}_0 или \hat{U}_1 в зависимости от значения управляющего кубита:

$$(12.11)$$

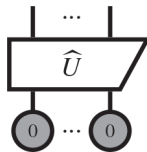
Упражнение 12.9. Проверьте, что матрица *мультиплексного унитарного отображения*, т. е. вентиля вида (12.11), является блочно-диагональной:

$$(12.12)$$

где U_0 и U_1 – матрицы процессов U_0 и U_1 соответственно.

12.1.3. Универсальность схем

Теперь у нас достаточно средств, чтобы показать, что любое квантовое отображение кубитов в кубиты можно выразить ZX-диаграммой. Как было отмечено в разделе 9.4.1, достаточно показать, что любое унитарное отображение можно реализовать в виде ZX-диаграммы. Зная, как это сделать для любого унитарного отображения, мы сможем получить любое состояние в виде:

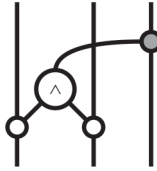


что можно преобразовать в произвольное отображение в силу двойственности процессов и состояний.

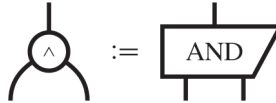
Причин использовать унитарные отображения в качестве промежуточного этапа две. Во-первых, попутно мы докажем, что любое унитарное квантовое отображение можно построить, используя только фиксированное множество унитарных квантовых вентилях, т. е. мы имеем *универсальное множество вентилях* для квантовых вычислений. Во-вторых, поскольку интерес к универсальным множествам вентилях возник еще до появления на свет ZX-диаграмм, большая часть трудной работы уже проделана кем-то другим.

Доказательство того, что любое унитарное отображение можно реализовать в виде ZX-диаграммы, мы проведем в три этапа.

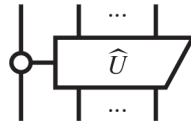
1. Построение вентиля Тоффоли:



с применением только вентиля CNOT и фазовых вентиляей, где



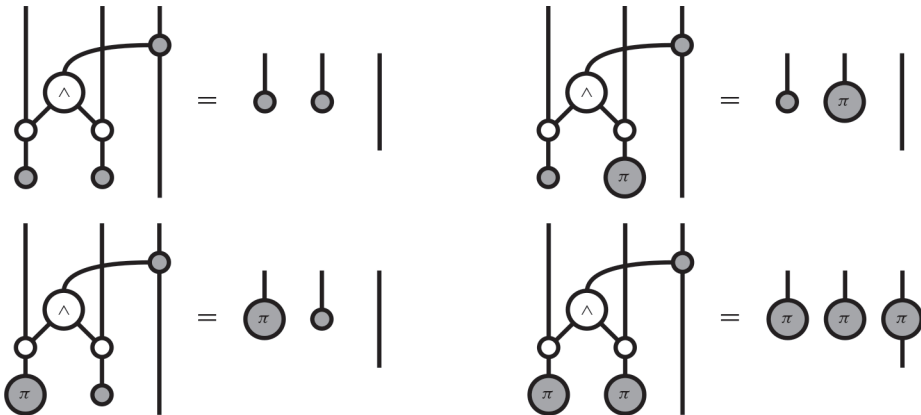
2. Использование вентиля Тоффоли для доказательства того, что если можно построить n -кубитовый вентиль \hat{U} с применением только вентиля CNOT и фазовых вентиляей, то можно построить также вентиль «управляемый- \hat{U} »:



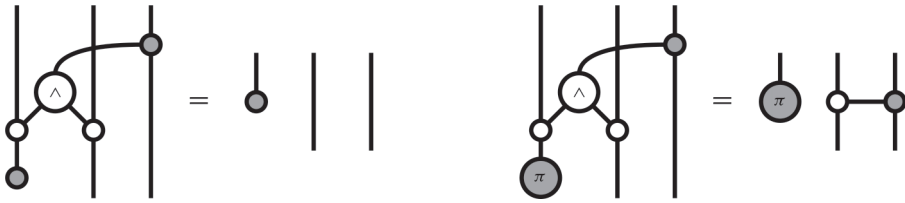
3. Использование этого факта для доказательства того, что если можно построить произвольные унитарные отображения $n - 1$ кубитов, то можно построить и любое унитарное отображение n кубитов.

12.1.3.1. Построение вентиля Тоффоли

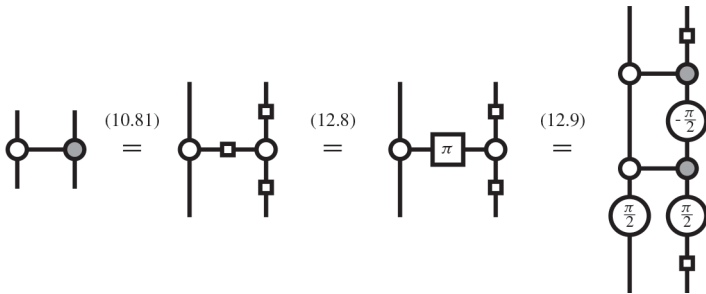
Выше мы изобразили вентиль Тоффоли в терминах вентиля AND, чтобы показать, что он применяет вентиль NOT к третьему кубиту в точности тогда, когда первые два кубита равны «1» (т. е. являются ●-фазами π):



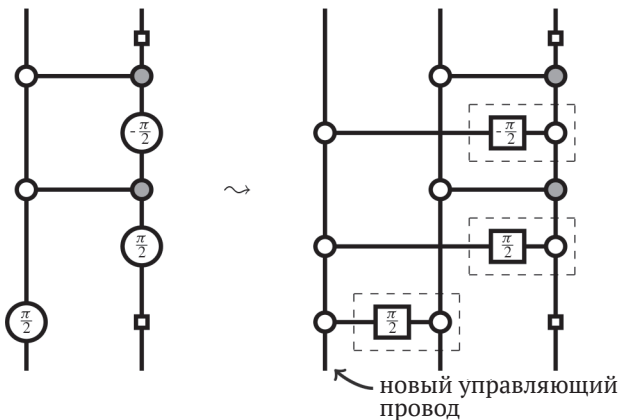
Как выясняется, построить вентиль AND не так-то просто (см. упражнение 12.10 ниже), поэтому перейдем сразу к вентилю Тоффли. Сначала заметим, что вентиль Тоффли можно рассматривать и по-другому – как «управляемый-CNOT»:



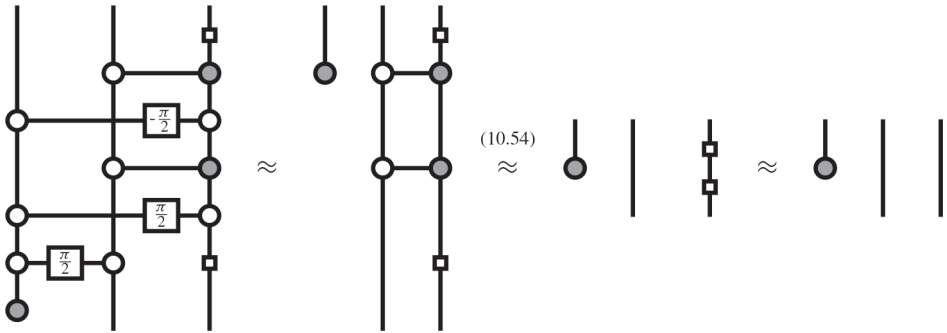
Но как же «включать и выключать CNOT»? Сначала запишем CNOT в терминах CZ(π)-вентиля, который, в свою очередь, можно записать в терминах CNOT и Z-фазовых вентилях:



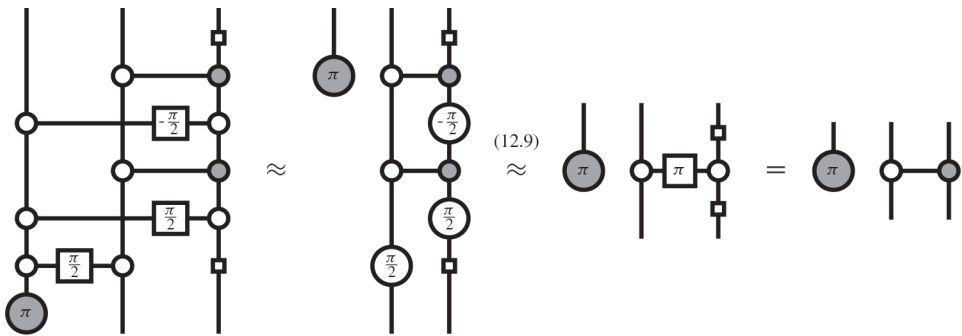
Тем самым мы просто преобразовали все фазовые вентили в управляемые фазовые вентили:



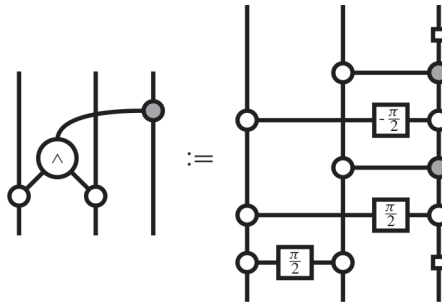
Теперь у нас появился новый управляющий провод. Если на вход управляющего кубита подать «0», то с остальными двумя кубитами ничего не произойдет:



а если подать «1», то будет применен вентиль CNOT:

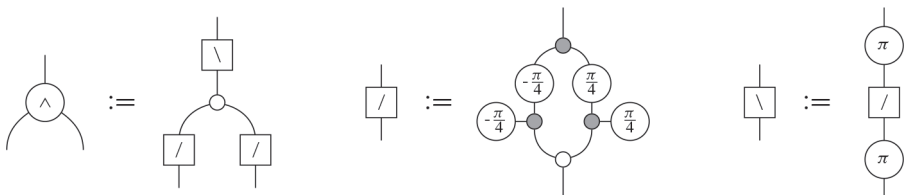


Вот оно! Таким образом, полагаем:



Поскольку каждый из $CZ(\alpha)$ -вентилей выше можно выразить через CNOT и фазовые вентили, то это верно и для вентиль Тоффли.

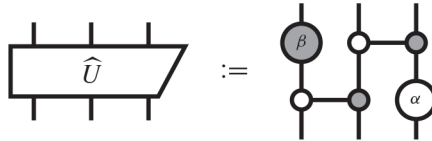
Упражнение 12.10. Придумайте альтернативное построение вентиль Тоффли, доказав предварительно, что следующее линейное отображение дает вентиль AND:



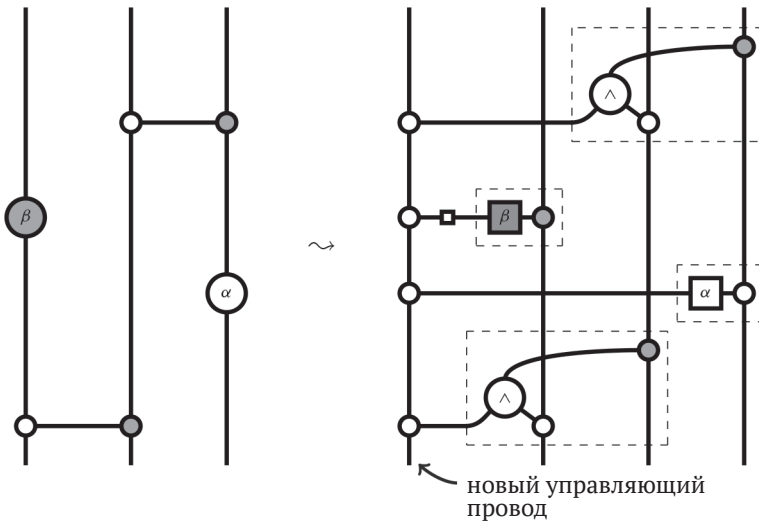
(Указание: сначала вычислите отображение «/» для состояний Z-базиса, а затем покажите, что «\» обратно к нему.)

12.1.3.2. Построение управляемых унитарных отображений

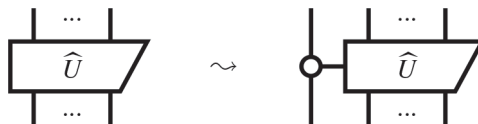
Покончив с шагом 1, мы можем разобраться с шагом 2, применив очень похожий прием. Предположим, что \hat{U} – унитарное отображение n кубитов, построенное из вентилей CNOT и фазовых вентилей, например:



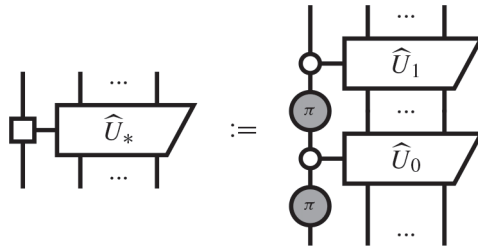
Тогда можно построить «управляемый- \hat{U} », добавив новую линию управления, которая «включает» или «выключает» каждый вентиль в схеме. То есть каждый фазовый вентиль становится управляемым фазовым вентилем, а каждый CNOT становится «управляемым-CNOT», т. е. вентилем Тоффоли. Наш пример принимает вид:



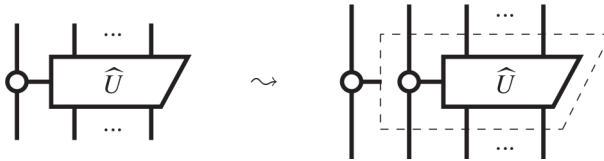
Таким образом, результирующая схема, по построению, является вентилем «управляемым- \hat{U} »:



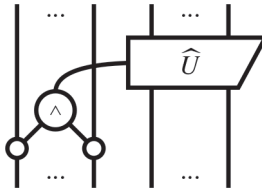
Имея управляемые операции, мы можем построить мультиплексор так же, как сделали в (12.11):



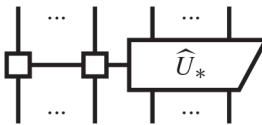
Далее, поскольку схема «управляемый- \hat{U} » сама состоит из CNOT и фазовых вентилей, мы можем повторить процесс добавления линии управления и получить вентиль «управляемый-управляемый- \hat{U} »:



Этот процесс можно повторить n раз и получить вентиль « n -управляемый- \hat{U} », который можно было бы записать так:



Упражнение 12.11. Следуя (12.11), воспользуйтесь n -управляемыми унитарными отображениями для построения n -кубитового мультиплексного унитарного отображения, т. е. вентиля



такого, что для любой битовой строки $\vec{i} := i_1 i_2 \dots i_n$ вентиль применяет следующее унитарное отображение к самому правому кубиту:

(12.13)

12.1.3.3. Собираем все вместе

Этот раздел можно было бы озаглавить «Уродливая матричная часть».

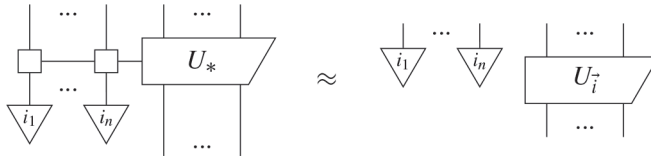
Основная теорема опирается на обобщение разложения по углам Эйлера на унитарные матрицы большого размера, которое называется *косинусно-синусным разложением*. Доказательство мы снова опустим, поскольку, по существу, оно представляет собой не что иное, как громоздкие манипуляции с матрицами.

Предложение 12.12. Матрицу любого унитарного отображения можно представить в виде:

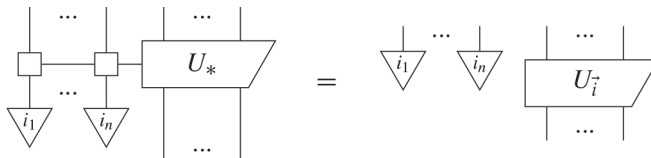
$$\begin{pmatrix} \boxed{U_0} & 0 \\ 0 & \boxed{U_1} \end{pmatrix} \begin{pmatrix} \boxed{C} & \boxed{-S} \\ \boxed{S} & \boxed{C} \end{pmatrix} \begin{pmatrix} \boxed{V_0} & 0 \\ 0 & \boxed{V_1} \end{pmatrix} \quad (12.14)$$

где U_i и V_i – матрицы унитарных отображений, а C и S – матрицы, в которых элемент в позиции (i, i) равен соответственно $\cos \theta_i$ и $\sin \theta_i$, а все остальные элементы равны 0.

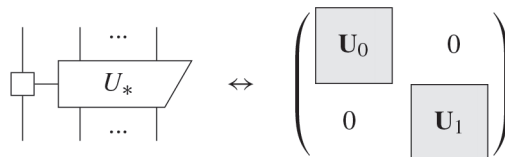
Теперь мы увидим, как построить эти матрицы из уже имеющихся вентилях. Раскрытие (12.13) дает:



Коль скоро унитарные отображения $U_{\tilde{i}}$ произвольны, мы можем включить в них число (которое на самом деле является просто глобальной фазой) и получить точное равенство:



В упражнении 12.9 мы уже видели, что обе блочно-диагональные матрицы можно реализовать с помощью мультиплексоров с одним управляющим проводом:



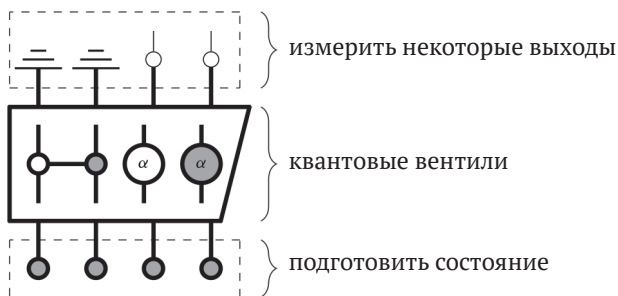
Со средней матрицей дело обстоит немного сложнее.

Но сначала несколько замечаний, чтобы не было претензий. Во-первых, хотя квантовые алгоритмы действительно являются тем «сногшибательным приложением», с которым в последние двадцать лет были связаны большие надежды в части новых квантовых особенностей, все известные к данному моменту квантовые алгоритмы касаются довольно узкого круга задач. Поэтому ни в коем случае нельзя сказать, что, будь у нас квантовые компьютеры, любую задачу можно было бы решить эффективнее.

Во-вторых, анализ квантовых алгоритмов с помощью диаграмм – все еще довольно молодая область. Как вы увидите, в этом направлении имеется некоторый прогресс, но все-таки этот раздел следует читать не как законченную историю, а как предварительный обзор еще только предстоящих исследований (а еще лучше как приглашение поучаствовать в них!). На самом деле диаграммное представление задачи о скрытой подгруппе, изложенное в разделе 12.2.4 (ее частным случаем является квантовый алгоритм разложения на множители), и его связь с сильной дополнительностью были открыты только на последних этапах работы над этой книгой.

12.2.1. (Ложная?) магия квантового оракула

Нам уже встречалась общая форма квантового вычисления в схемной модели:

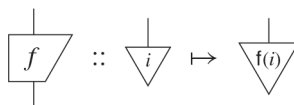


Если мы хотим, чтобы квантовое вычисление было лучше классического компьютера, то должны придумать какой-то способ кодирования классических задач в виде квантовых схем. Очевидно, что подходящее место для этого – большое унитарное отображение в середине. Теперь практически любую вычислительную задачу можно свести к получению информации о функции вида

$$f : \{0, 1\}^n \mapsto \{0, 1\}.$$

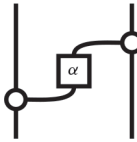
Например, проблема *выполнимости* заключается в ответе на вопрос, существует ли такая битовая строка i , что $f(i) = 1$.

Но как превратить функцию f в унитарное отображение? Для начала мы можем закодировать ее как линейное отображение, как было сделано для классических логических вентилей в разделе 5.3.4:

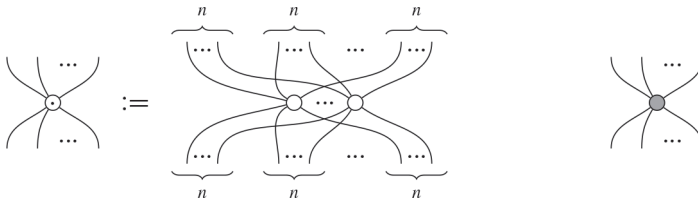


но это линейное отображение (а значит, и квантовое отображение \hat{f}) будет унитарным, только если f – биективное отображение входов на выходы. Это не есть хорошо! В частности, при $N > 1$ это попросту невозможно.

Но, быть может, не все потеряно! Вспомните трюк, которым мы воспользовались для преобразования нашего неунитарного α -блока в двухкубитовое унитарное отображение. Вот как мы это сделали:



И похожую штуку можно повернуть для \hat{f} . Сначала зафиксируем пауков, представляющих входной и выходной типы f :



Вместо \circ -пауков для выходной системы мы возьмем дополнительного паука. Почему? Потому что это необходимо для установления унитарности.

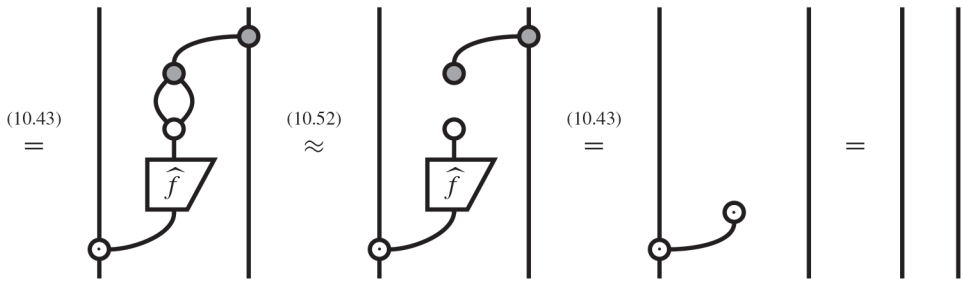
Предложение 12.15. Квантовое отображение

$$\hat{U}_f := D \quad (12.15)$$

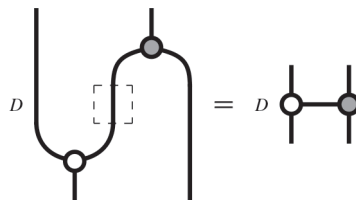
является унитарным для любой функции f тогда и только тогда, когда \circ и \bullet дополнительные.

Доказательство. Сначала предположим, что \circ и \bullet дополнительные. Тогда, используя тот факт, что f – функциональное отображение, имеем:

$$\hat{U}_f \approx \dots = \dots \quad (10.40)$$

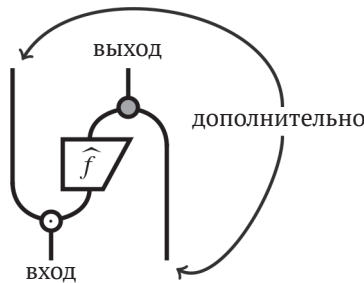


Для другой композиции доказательство аналогично. Обратное, чтобы доказать, что из унитарности (12.15) следует дополнительность, возьмем в качестве \hat{f} простой провод. Тогда отображение

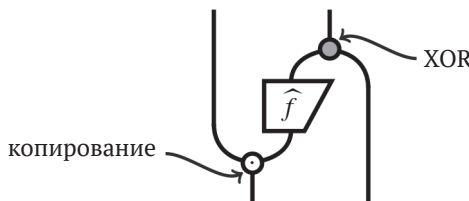


унитарно, откуда в силу предложения 9.50 вытекает дополнительность \circ и \bullet . \square

А что делает \hat{U}_f ? Оно преобразует квантовое отображение \hat{f} в унитарное, присоединив дополнительный вход, соответствующий выходу \hat{f} , и дополнительные выходы, соответствующие входу \hat{f} :



или более конкретно:

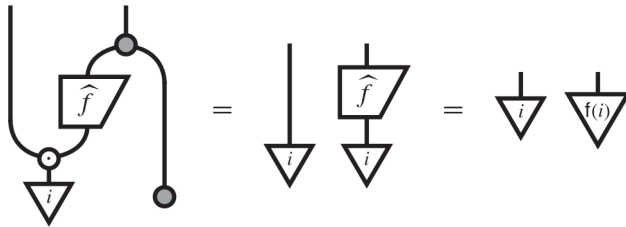


Таким образом, копируется состояние базиса \circ на левом входе \hat{U}_f . Первая из этих копий подается на первый выход \hat{U}_f , вторая – на вход \hat{f} , а затем к соответствующим

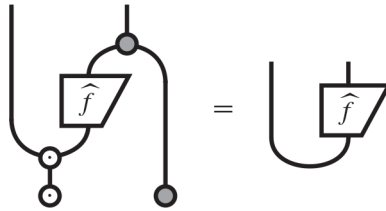
ющему выходу и второму входу \widehat{U}_f применяется операция XOR. Если в качестве второго входа \widehat{U}_f взять



то мы сможем вычислить функцию f для любого входа:



Круто, правда? Теперь посмотрим, что произойдет, если подать на первый вход что-то, не являющееся классической битовой строкой:



Вместо того чтобы получать на выходе значение f для одного конкретного входа, мы получаем всю функцию f , закодированную в виде состояния. Иными словами, мы имеем суперпозицию значений f на всех возможных входах:

$$\text{Circuit} = \text{double} \left(\sum_{i \in \{0,1\}^n} \begin{matrix} \downarrow \\ i \end{matrix} \begin{matrix} \downarrow \\ f \end{matrix} \begin{matrix} \downarrow \\ i \end{matrix} \right) = \text{double} \left(\sum_i \begin{matrix} \downarrow \\ i \end{matrix} \begin{matrix} \downarrow \\ f(i) \end{matrix} \right)$$

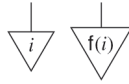
Ух ты! Вот теперь вы, наверное, понимаете, откуда вся эта суматоха по поводу квантовых вычислений. Ведь

*один квантовый процесс может вычислять функцию
одновременно для всех входных значений!*

Этот единственный процесс \widehat{U}_f , который, похоже, обладает божественным знанием о функции f , называется *квантовым оракулом*. Но насколько он все-таки божественный?

Разумеется, у нас теперь масса информации о f , но как до нее добраться? Она закодирована в квантовом состоянии, поэтому единственное, что мы можем сде-

лать, – измерить его. Если мы не поостережемся и решим измерить первую систему относительно \bullet , то вся эта расчудесная информация превратится всего в один исход измерения:



и у нас даже возможности выбрать i нет! Иными словами, потратив 10 млн долл. на сборку хитроумного квантового компьютера, мы смогли только вычислить f при каком-то случайном значении i . Поистине монументально бессмысленная трата денег!

12.2.2. Алгоритм Дойча–Йожи

Так что же, квантовые вычисления – одно большое надувательство? Нет, конечно! Но необходимо проявить немалую изобретательность, чтобы не пасть жертвой разрушений, причиняемых квантовыми измерениями.

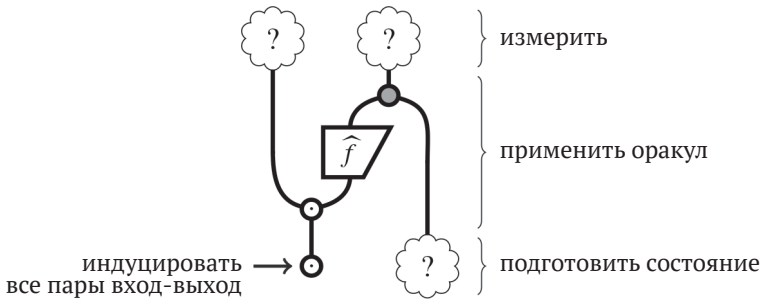
Хотя мы никогда не получим доступа ко всем парам входных и выходных значений f , существует много других в высшей степени нетривиальных вопросов относительно f , которые имеют ответы, выражаемые одним значением. И есть надежда, что, проявив достаточное хитроумие, мы сможем с помощью одного измерения получить ответ на вопрос, который в классическом случае требует знания многих (а то и всех) пар вход-выход f . Это позволило бы добиться для некоторых задач производительности, куда большей, чем у классического компьютера.

Очередная плохая новость (не последняя) заключается в том, что спектр вопросов, на которые можно получить ответ в результате одного измерения, сильно ограничен. Например, доказано, что вышеупомянутая проблема выполнимости не относится к числу таких вопросов.

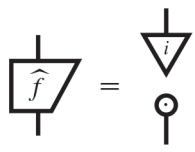
Можно также задать вопрос, возвращает ли функция f один и тот же ответ для любого входа, т. е. является ли она *постоянной*. Конечно, если бы мы знали ответ на этот вопрос, то проблема выполнимости оказалась бы тривиальной (почему?). Поэтому у этой задачи также не существует решения. Но, быть может, мы сможем куда-нибудь продвинуться, сделав какое-то предположение о f ?

Вопросы, которые позволяют решить квантовые алгоритмы, – это некоторые задачи с *предусловием*, т. е. задачи, в которых какая-то информация о функции («предусловие») известна заранее, а мы пытаемся узнать что-то еще. В случае алгоритма Дойча–Йожи вопрос заключается в том, верно ли, что функция либо является постоянной, либо обладает каким-то другим свойством «X». Задачей с *предусловием* ее делает то, что «X» более специфично, чем «не постоянна». Чтобы понять, чем должно быть «X», мы приступим к построению алгоритма и посмотрим, что нам понадобится.

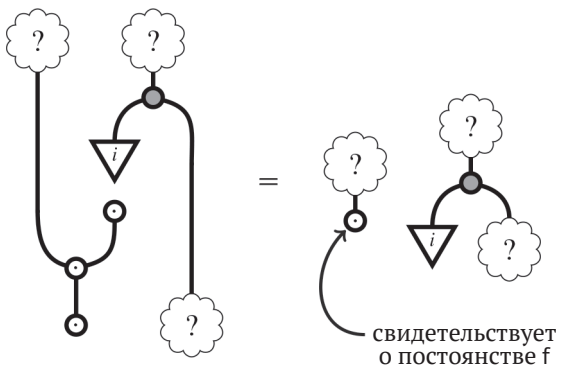
Начнем с очень общего предположения – что квантовый оракул применяется для заданной функции f на суперпозиции всех входов:



Если f постоянна, или, что эквивалентно, постоянно отображение \hat{f} , то оно должно иметь вид:



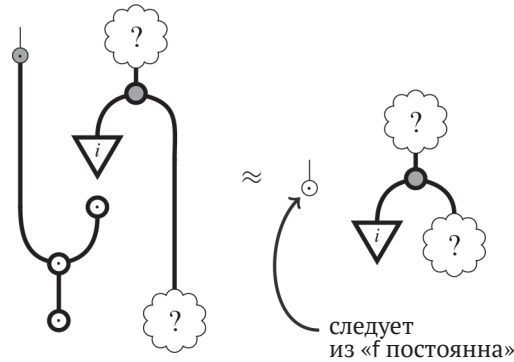
То есть оно просто удаляет свой вход и выдает на выходе постоянное значение i . Подставляя это в наш (будущий) алгоритм, получаем:



Таким образом, диаграмма распадается, и левая часть больше не зависит от значений f , а содержит состояние, которое свидетельствует о том, что f постоянна. Ко всему прочему, это состояние оказывается собственным состоянием \bullet -измерения:

(10.77)

Отсюда:



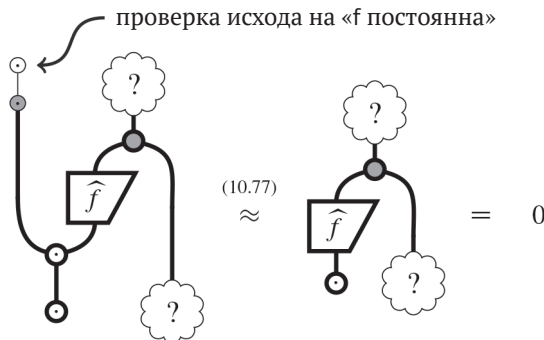
Отлично! Теперь мы знаем, что постоянство f гарантирует, что:

$$\text{Measurement symbol} = \text{Hadamard gate} \text{ with } 0 \text{ on the control line} \dots \text{Hadamard gate} \text{ with } 0 \text{ on the control line} \tag{12.16}$$

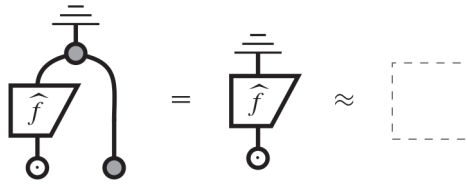
будет исходом \bullet -измерения первого выхода оракула.

Замечание 12.16. Отметим, что здесь мы измеряем не выход функции, а нечто «дополнительное», добавленное нами для обеспечения унитарности квантового оракула. Так что это «дополнительное» оказалось крайне важным само по себе!

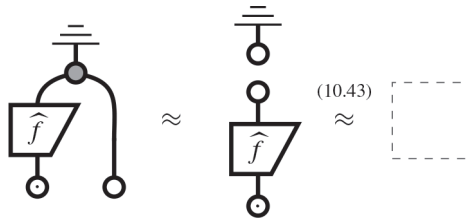
Итак, мы знаем, что если f постоянна, то мы обязательно получим такой исход. Но даже если f не постоянна, мы все равно можем получить такой же исход. Именно тут в игру вступает наше «X». Свойство «X» функции должно быть выбрано так, чтобы исход (12.16) никогда не встретился; это будет гарантировать, что раз мы наблюдаем этот исход, то f обязана быть постоянной. «Никогда не встретился» означает нулевую вероятность, т. е. f должна обладать свойством «X» тогда и только тогда, когда:



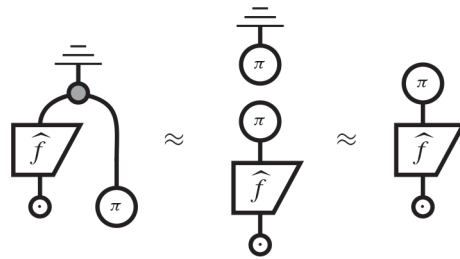
У нас все еще есть некоторая свобода в выборе подходящего ? . Благодаря причинности облако в верхней части ни для чего не используется, поэтому можно считать его отбрасыванием. Для экспериментов остается только состояние, подаваемое на второй вход оракула. Сначала попробуем \bullet -состояние, которое использовалось в предыдущем разделе. Но в силу причинности имеем:



Поэтому такой выбор нам ничего не дает. Тогда попробуем другой цвет. К сожалению, поскольку \hat{f} получается из функции на \circ -базисе, удача нам опять не сопутствует:



У нас кончаются варианты! Ну, еще одна попытка:



Ага! Похоже, это хотя бы может обратиться в ноль для некоторых функций f . Так что же означает равенство

$$\begin{array}{c} \pi \\ \circ \\ \hline \hat{f} \\ \circ \end{array} = 0 \tag{12.17}$$

для функции f ? \circ -эффект с фазой π почти совпадает с удалением, только мы задаем фазу -1 при «удалении» второго базисного состояния:



Итак, если

$$\begin{array}{c} \pi \\ \circ \\ \downarrow \\ \boxed{f} \\ \downarrow \\ \circ \end{array} = \begin{array}{c} \pi \\ \circ \\ \downarrow \\ \boxed{f} \\ \downarrow \\ \sum_i \begin{array}{c} \downarrow \\ i \end{array} \end{array} = \sum_i \begin{array}{c} \pi \\ \circ \\ \downarrow \\ \begin{array}{c} \downarrow \\ f(i) \end{array} \end{array} = \sum_{f(i)=0} 1 + \sum_{f(i)=1} (-1) = 0$$

то количество значений i таких, что $f(i) = 0$, должно быть таким же, как количество значений, для которых $f(i) = 1$. Это означает, что функция f *сбалансирована*.

Таким образом, мы нашли настоящий квантовый алгоритм! Вот он.

Дано. Функция

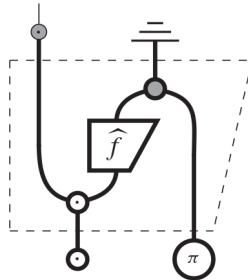
$$f : \{0, 1\}^n \mapsto \{0, 1\}$$

с предположением, что она либо *постоянна*, т. е.

- f всегда возвращает 0 или всегда возвращает 1, либо *сбалансирована*, т. е.
- f возвращает 0 столько же раз, сколько 1.

Задача. Является ли f постоянной или сбалансированной?

Квантовый алгоритм. Выполнить



и если получится исход

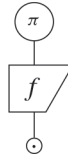


то f постоянна, иначе сбалансирована.

В классическом алгоритме мы должны проверить, по меньшей мере, половину входов плюс 1, чтобы с уверенностью сказать, постоянна f или сбалансирована. Иначе говоря, нам нужно *опросить* f , по меньшей мере, $2^{n-1} + 1$ раз. Поразительно, но в квантовом алгоритме достаточно всего одного опроса!

Замечание 12.17. Заметим, что если мы хотим, чтобы этот алгоритм был эффективным, то должны предположить, что унитарный оракул можно реализовать эффективно, например с помощью квантовых вентилях. Это, конечно, зависит от функции f . Однако если существует эффективный способ реализовать f на классическом компьютере, то ее можно эффективно реализовать и с помощью квантовых вентилях. Интересующегося читателя отсылаем к литературе, упомянутой в разделе «Исторические замечания и ссылки» в конце главы.

Обобщая (12.17), можно сказать, что число



измеряет «степень сбалансированности» f . Оно положительно, если f порождает больше нулей, чем единиц, отрицательно, если нулей меньше, чем единиц, а чем оно больше по абсолютной величине, тем больше разность между количеством нулей и единиц. Мы воспользуемся этим фактом в следующем алгоритме.

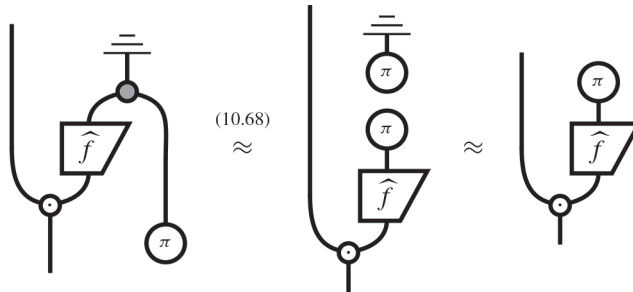
12.2.3. Квантовый поиск

Теперь мы знаем, что квантовые процессы позволяют ускорить решение, по меньшей мере, одной задачи. К сожалению, не так уж часто от знания того, является функция постоянной или сбалансированной, зависит жизнь или смерть. Но, быть может, мы сможем воспользоваться тем, чему научились, чтобы сделать что-то действительно полезное.

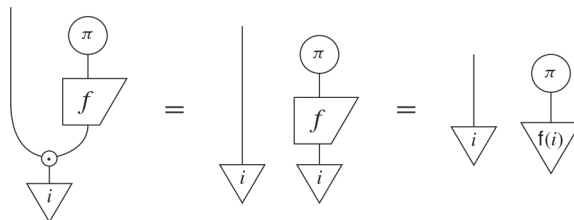
Суть алгоритма Дойча–Йожи заключается в том, что \ominus -эффект с фазой π удаляет результат f , если он равен 0, и вводит фазу -1 , если он равен 1:

$$\begin{array}{c} \pi \\ \circ \\ | \\ \triangle \\ 0 \end{array} = \text{---} \quad \begin{array}{c} \pi \\ \circ \\ | \\ \triangle \\ 1 \end{array} = -1 \text{---} \quad (12.18)$$

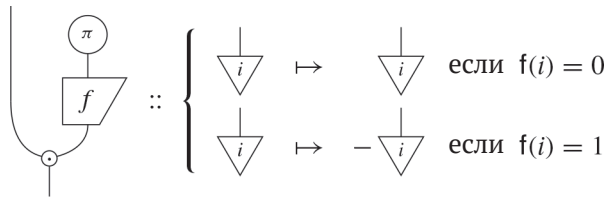
Подключение \ominus -состояния с фазой π ко второму входу нашего оракула дает:



Недублированная версия этого процесса воздействует на классические входы следующим образом:



Отсюда в силу (12.18) имеем:



Как видим, любое i , для которого $f(i) = 1$, «помечается» путем обращения знака. Поэтому, применяя этот процесс ко «всем входам вместе», получаем:

$$\text{Control} \circ f \circ \pi = \sum_i \downarrow_i - \sum_{f(i)=1} \downarrow_i \quad (12.19)$$

В алгоритме Дойча–Йожи мы использовали это состояние, чтобы различить постоянную и сбалансированную функции с помощью одного измерения. Но что, если мы смогли бы придумать измерение, которое выдает на выходе только одну из «помеченных» битовых строк i ? Это решило бы очень полезную задачу поиска. Многие трудные вычислительные задачи сводятся к поиску.

Предположим, что имеется набор предметов (например, яблок), содержащий как хорошие (например, свежие), так и плохие (подгнившие). Мы хотим выбрать свежее яблоко. Это легко, если яблок много, а подгнило только одно, но очень трудно в противном случае, потому что нам придется проверять каждое яблоко. В терминах функций предположим, что имеется функция

$$f : \{0, 1\}^n \mapsto \{0, 1\},$$

где 0 обозначает «подгнившее», а 1 – «свежее». Можно ли найти свежее яблоко, т. е. такое i , для которого $f(i) = 1$?

Упрощение левой части (12.19) дает:

$$f \circ \pi = \sum_{f(i)=0} \downarrow_i - \sum_{f(i)=1} \downarrow_i$$

Теперь всем хорошим яблокам соответствует знак «минус». Сравнивая это с предыдущим состоянием:

$$\text{Control} \circ \pi = \sum_i \downarrow_i \quad (12.20)$$

мы видим, что вычитание двух состояний устраняет подгнившие яблоки:

$$\begin{array}{c} \circ \\ | \\ - \\ \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \end{array} = 2 \sum_{f(i)=1} \begin{array}{c} | \\ \diagdown \\ i \\ \diagup \end{array}$$

Замечательно! Стало быть, просто измерив результат, мы найдем свежее яблоко. Таким образом, задача поиска свелась к нахождению такого унитарного отображения, что

$$\begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \mapsto \begin{array}{c} \circ \\ | \\ - \\ \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \end{array}$$

Очевидно, что оно должно состоять из двух членов: один порождает (12.20) в виде константы, стирая вход, а второй вводит фазу -1 и больше ничего не делает. Поэтому положим:

$$\begin{array}{c} \diagdown \\ d \\ \diagup \end{array} := \lambda \begin{array}{c} \circ \\ | \\ - \\ \circ \\ | \end{array} - \begin{array}{c} | \end{array}$$

Тогда:

$$\begin{array}{c} \diagdown \\ d \\ \diagup \end{array} :: \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \mapsto \left(\lambda \begin{array}{c} \circ \\ | \\ \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \\ | \\ \circ \end{array} \right) - \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array}$$

Теперь мы можем выбрать λ , так чтобы лишнее число в первом члене



сократилось. В предыдущем разделе мы видели, что это лишнее число измеряет «сбалансированность» f :

$$\begin{array}{c} \circ \\ | \\ \begin{array}{c} \diagup \\ f \\ \diagdown \\ \pi \end{array} \end{array} = \begin{array}{c} \pi \\ \circ \\ | \\ \begin{array}{c} \diagdown \\ f \\ \diagup \end{array} \\ | \\ \circ \end{array} = \sum_{f(i)=0} 1 + \sum_{f(i)=1} (-1) = N_0 - N_1$$

Следовательно, свежим должно быть ровно одно яблоко из четырех. Таким образом, мы (заново) открыли следующий квантовый алгоритм поиска:

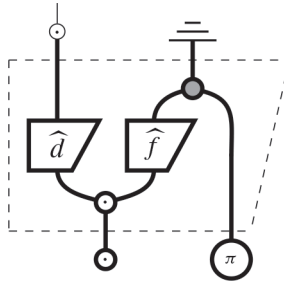
Дано. Функция

$$f : \{0, 1\}^n \mapsto \{0, 1\}$$

с предположением, что ровно одна из четырех битовых строк отображается в 1.

Задача. Найти битовую строку, которая отображается в 1.

Квантовый алгоритм. Выполнить



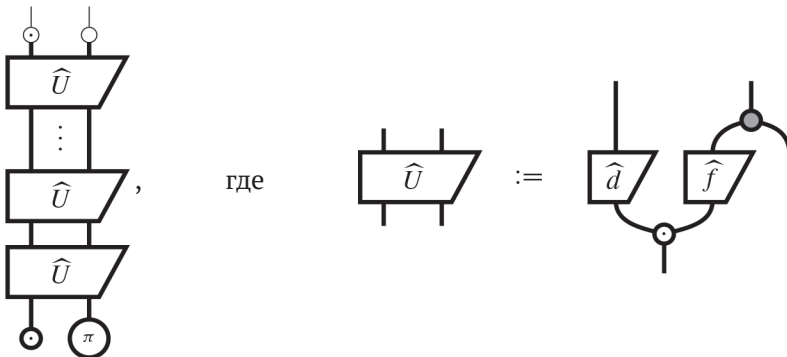
где

$$d \text{ (gate symbol)} := \frac{2}{N} \begin{matrix} \circ \\ | \\ \circ \end{matrix} - \begin{matrix} | \\ \circ \end{matrix}$$

Тогда мы непременно найдем такую битовую строку.

В классическом случае вероятность найти хорошую битовую строку при одном испытании равна $\frac{1}{4}$, и если уж совсем не повезет, то придется провести $3N/4 + 1$ испытаний. А квантовый алгоритм дает результат после первой же попытки!

Конечно, если помечено меньше (или больше!), чем $D/4$ элементов, то вероятность получить непомеченный элемент ненулевая. Однако мы можем повысить свои шансы, просто повторяя унитарную часть протокола:



После каждой итерации вероятность получить помеченный элемент возрастает, и можно показать, что при одном помеченном элементе вероятность получить

непомеченный исход обращается в ноль приблизительно после \sqrt{D} итераций. Эта многошаговая версия называется *алгоритмом Гровера*.

12.2.4. Задача о скрытой подгруппе

Чтобы подвести черту под обсуждением квантовых алгоритмов, рассмотрим задачу о скрытой подгруппе, решение которой на сегодняшний день является, пожалуй, самым важным квантовым алгоритмом. Почему? Ведь совершенно не ясно, почему вдруг нас должны интересовать «подгруппы» и как они там «скрыты», а значит, не понятно, с чего такое внимание к задаче о скрытой подгруппе. Но есть, по крайней мере, одна веская причина: если мы сможем эффективно решить задачу о скрытой подгруппе, то практически вся современная криптография пойдет прахом! Дело в том, что алгоритмы разложения на простые множители (факторизации) и нахождения дискретного логарифма, которые, как упоминалось во введении к этой главе, можно использовать для взлома многих криптографических систем, являются частными случаями задачи о скрытой подгруппе. Кто же знал, что всякие непонятные задачи из теории групп как-то связаны с криптографией? (Ответ: любой криптограф.)

Мы ограничимся коммутативными группами и воспользуемся классификацией сильно дополнительных пауков из раздела 9.3.6. Для любой коммутативной группы G существует система (которую будем обозначать тоже G) и пара сильно дополнительных пауков \circ/\bullet , которые кодируют G . То есть для

$$\left\{ \begin{array}{c} | \\ \downarrow G \\ \triangle g \end{array} \right\}_{g \in G} \cong \left\{ \begin{array}{c} | \\ \bullet G \\ \kappa_g \end{array} \right\}_{g \in G}$$

имеем:

$$\begin{array}{c} \begin{array}{c} \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \text{---} \\ \kappa_g \end{array} \approx \begin{array}{c} | \\ \kappa_g \end{array} \begin{array}{c} | \\ \kappa_g \end{array} \quad \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_g \end{array} \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_{g'} \end{array} = \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_{g+g'} \end{array} \end{array} \quad (12.22)$$

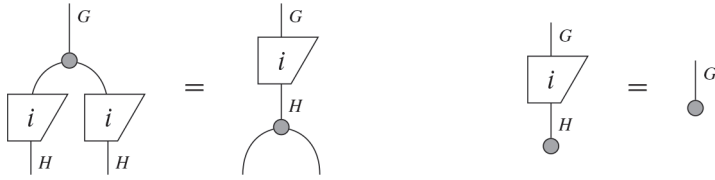
Обратите внимание, что провода помечены. Дело в том, что теперь мы используем другую пару сильно дополнительных пауков для кодирования подгруппы $H \subseteq G$:

$$\begin{array}{c} \begin{array}{c} \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \text{---} \\ \kappa_h \end{array} \approx \begin{array}{c} | \\ \kappa_h \end{array} \begin{array}{c} | \\ \kappa_h \end{array} \quad \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_h \end{array} \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_{h'} \end{array} = \begin{array}{c} | \\ \bullet \\ \text{---} \\ \text{---} \\ \kappa_{h+h'} \end{array} \end{array} \quad (12.23)$$

Чтобы засвидетельствовать тот факт, что это подгруппа G , мы введем *отображение включения*, которое погружает элементы H в G :

$$\begin{array}{c} | \\ \square \\ | \end{array} \begin{array}{c} G \\ i \\ H \end{array} \quad :: \quad \begin{array}{c} | \\ \bullet \\ \kappa_h \end{array} \mapsto \begin{array}{c} | \\ \bullet \\ \kappa_h \end{array}$$

Включение сохраняет единицу и групповую операцию H , поэтому i является гомоморфизмом групп:



Снова обратите внимание, что провода помечены, чтобы отличать пауков для G в (12.22) от пауков для H в (12.23).

H «скрыта» посредством фактор-группы G/H . Это новая группа, элементами которой являются множества элементов G , называемые классами эквивалентности. Если положить

$$[g] := \{g' \in G \mid \exists h \in H . g' = g + h\},$$

то множество

$$G/H := \{ [g] \mid g \in G \}$$

оказывается группой с единицей $[0]$ и групповой операцией

$$[g] + [g'] := [g + g'].$$

Как и для двух других групп, мы зафиксируем сильно дополнительную пару пауков для кодирования G/H :



На этот раз мы получаем отображение, определенное на G , которое называется фактор-отображением



и отображает каждый элемент $g \in G$ в элемент $[g] \in G/H$. Как и i , отображение q является гомоморфизмом групп:



$$(12.24)$$

Отметим, что если $h \in H$, то фактор-отображение переводит h в элемент $[h] \in G/H$. Но тогда $h = 0 + h$, так что $[h] = [0]$. Следовательно, любой элемент H отображается в единицу. На диаграмме это означает, что композиция i и q приводит к удалению H и выдаче единицы:

(12.25)

Ну вот, теперь мы готовы «скрыть» H . Пусть дана функция

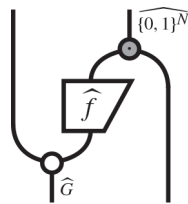
$$f : G \mapsto \{0, 1\}^N$$

с предположением, что она допускает такое разложение:

(12.26)

где фраза «инъективная функция» означает просто, что f' – функциональное отображение и изометрия. Можно ли определить, чему равна H ?

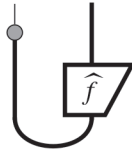
Как обычно, мы будем использовать пауков для построения оракула для f :



где \odot/\circ – произвольная дополнительная пара пауков для системы битовых строк (обещаем – последняя). Квантовые оракулы полюбились нам прежде всего тем, что они позволяют подготавливать такие состояния:

(12.27)

Посмотрим, что случится, если мы измерим левую систему с помощью \bullet :



Исходы отдельных измерений соответствуют эффектам \bullet -ОНБ, которые совпадают с элементами группы, закодированными как \circ -фазы:

(12.28)

Мы можем определить, какие элементы группы получены таким образом, с помощью леммы об адьюнкте фактор-отображения.

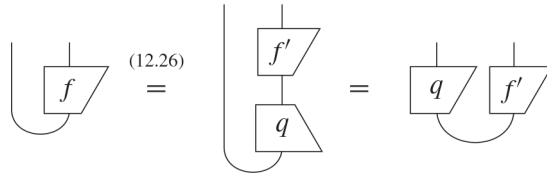
Лемма 12.19. Если i – отображение включения, а q – фактор-отображение, то

(12.29)

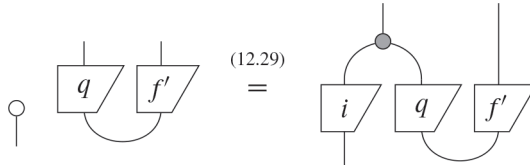
Доказательство. Имеем:

□

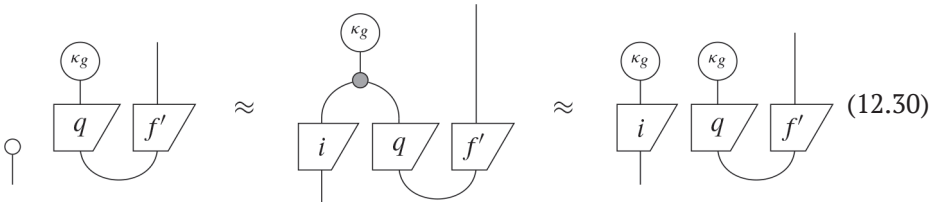
Глядя на предусловие для f в контексте (12.27), имеем:



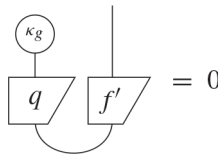
Выполнив \otimes -композицию с \circ -эфффеком в левой части, получаем:



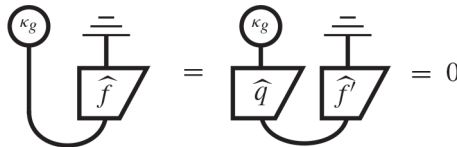
Теперь подключение \circ -фазы κ_g дает:



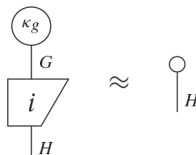
Таким образом, либо



и тогда вероятность получить исход, соответствующий κ_g , равна



либо мы можем сократить это состояние в обеих частях (12.30), что дает:



На самом деле отсюда нетрудно вывести, что \approx -равенство в действительности выполняется точно. Поэтому мы можем заключить, что путем измерения левой системы оракула, как в (12.28), мы всегда получаем исходы, соответствующие элементам группы $g \in G$, где

$$\begin{array}{c} \textcircled{\kappa_g} \\ | \\ G \\ \square \\ | \\ H \end{array} = \begin{array}{c} \textcircled{} \\ | \\ H \end{array} \tag{12.31}$$

Это и все, что нам необходимо для решения задачи о скрытой подгруппе. Но чтобы убедиться в этом, необходимо лучше понять, что означает приведенное выше равенство. Хотя κ_g не является удалением:

$$\begin{array}{c} \textcircled{\kappa_g} \\ | \\ \end{array} \neq \begin{array}{c} \textcircled{} \\ | \\ \end{array}$$

в силу (12.31) оно действует как удаление, если ограничить его на подгруппу H ; т. е. если $h \in H$, то

$$\frac{1}{\sqrt{D}} \begin{array}{c} \textcircled{\kappa_g} \\ \textcircled{\kappa_h} \end{array} = \boxed{\phantom{\text{diagram}}}$$

В теории групп множество фаз, которые «локально» удаляют подгруппу H , называется аннулятором H :

$$H' := \left\{ g \in G \mid \forall h \in H : \frac{1}{\sqrt{D}} \begin{array}{c} \textcircled{\kappa_g} \\ \textcircled{\kappa_h} \end{array} = \boxed{\phantom{\text{diagram}}} \right\}$$

Для любой подгруппы существует классический алгоритм вычисления ее аннулятора, который, по существу, сводится к решению некоторой системы уравнений. Но что, если мы знаем только аннулятор подгруппы? В таком случае можно воспользоваться следующим фактом.

Упражнение* 12.20. В предположении, что имеются помеченные классические фазы такие, что

$$\begin{array}{c} \textcircled{\kappa_h} \\ \textcircled{\kappa_g} \end{array} = \begin{array}{c} \textcircled{\kappa_g} \\ \textcircled{\kappa_h} \end{array}$$

покажите, что $(H')' = H$. (Указание: докажите, что $H \subseteq (H)'$ и что размеры H и $(H)'$ одинаковы. Для доказательства последнего сначала покажите, что H' имеет такой же размер, как G/H .)

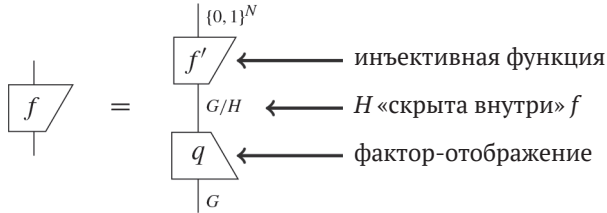
Вуаля! После не такого уж большого количества обращений к оракулу наше квантовое измерение дает нам генераторы H' , т. е. элементы, достаточные для получения любого элемента H' с помощью групповой операции. Затем мы можем

применить какую-нибудь классическую постобработку для вычисления генераторов $(H)'$, а это в силу упражнения* 12.20 и есть H . Резюмируем.

Дано. Коммутативная группа G и функция

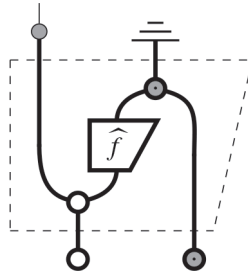
$$f : G \mapsto \{0, 1\}^N$$

с предположением, что существует такая подгруппа $H \subseteq G$, что



Задача. Найти H .

Квантовый алгоритм. Выполнить



и получить исход



для $g \in H'$. Повторять, пока не будет получено порождающее множество для H' . Воспользоваться этим множеством для классического вычисления $(H')' = H$.

Но как перейти отсюда к факторизации? Предположим, что вначале имеется функция

$$f : \mathbb{Z} \mapsto \{0, 1\}^N$$

и мы выполняем алгоритм нахождения скрытой подгруппы H :

$$\{kr \bmod D\}_k \subseteq \mathbb{Z},$$

т. е. группы, состоящей из всех чисел, кратных r по модулю D . Тогда оказывается, что f имеет период r , т. е. для любого x

$$f(x) = f(x + r).$$

Но почему это интересно? Объясним. Если мы можем найти период функции

$$f(x) := a^x \bmod D$$

для случайно выбранных значений a , то мы сумеем эффективно факторизовать D ! Чтобы убедиться в этом, предположим, что функция выше имеет период r :

$$a^x = a^{x+r} \pmod{D}.$$

Тогда после простых алгебраических преобразований получаем:

$$a^r - 1 = 0 \pmod{D}.$$

Если нам немного повезет, то r будет четным числом, поэтому, полагая $b := a^{r/2}$, получим:

$$b^2 - 1 = 0 \pmod{D}.$$

Факторизация левой части дает:

$$(b + 1)(b - 1) = 0 \pmod{D}.$$

Поэтому D делит произведение $b + 1$ и $b - 1$. Но тогда должно быть верно одно из двух: либо D делит $b + 1$ или $b - 1$, либо оба эти числа содержат нетривиальные множители D . Если верно последнее (а вероятность этого не меньше вероятности первого), то мы можем эффективно найти множитель как наибольший общий делитель $b + 1$ и D .

Замечание 12.21. Внимательный читатель, вероятно, заметил одну проблему в этом выводе: коммутативная группа \mathbb{Z} не является конечной! Однако если выбрать очень большое q , то мы сможем выполнить этот алгоритм для функции $f : \mathbb{Z}_q \mapsto \{0, 1\}^N$, определенной на циклической группе \mathbb{Z}_q , и с высокой вероятностью получить тот же результат.

Упражнение 12.22. Покажите, что однобитовая задача Дойча–Йожи для функции

$$f : \{0, 1\} \mapsto \{0, 1\}$$

является частным случаем задачи о скрытой подгруппе для f . Покажите, что для $N > 1$ и

$$f : \{0, 1\}^N \mapsto \{0, 1\}$$

не существует групповой операции на множестве $\{0, 1\}^N$, которая превращала бы задачу Дойча–Йожи в частный случай задачи о скрытой подгруппе.

12.3. ОСНОВАННЫЕ НА ИЗМЕРЕНИИ КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Основанные на измерении квантовые вычисления (МВQC) – альтернативный подход к универсальным квантовым вычислениям. Вместо того чтобы втискивать всю вычислительную структуру в унитарные отображения, в МВQC все квантовые процессы являются измерениями. Впервые нечто подобное нам встретилось в разделе 7.2.2 в форме вентиляльной телепортации. А сейчас мы представим модель МВQC, основанную на *графовых состояниях* (см. раздел 9.4.5) и измерениях одного кубита. Эта модель известна также как *односторонняя модель* квантовых вычислений. В ней вычисление состоит из трех шагов:

- 1) подготовка графового состояния;

- 2) выполнение однокубитовых измерений, так что последующие измерения могут управляться исходами предыдущих с помощью *прямого распространения*;
- 3) необязательная классическая постобработка исходов измерений.

Ключом к успеху является использование обратного действия (см. раздел 7.2.1) однокубитовых измерений, для того чтобы можно было (недетерминированно) реализовать произвольные квантовые эффекты. Их можно будет применить к графовому состоянию, и этого достаточно для реализации любого квантового вычисления. Например, если выбрать измерения, дающие такие эффекты:



то следующий фрагмент графового состояния



можно будет преобразовать в любое однокубитовое унитарное отображение:

(12.32)

Красиво, правда? В этом разделе мы увидим, не только как восстановить произвольные одно- и многокубитовые вентили с помощью измерений, но и как сделать это детерминированно, применяя технику, похожую на ту, которой мы пользовались для квантовой вентильной телепортации.

Преимущество парадигмы MBQC над схемной моделью состоит в том, что если уж имеется графовое состояние, то все последующие вычисления можно произвести с помощью одних лишь однокубитовых процессов. В рамках существующей технологии операции над несколькими кубитами, например CNOT, могут пред-

ставлять большую сложность и часто вносят слишком большую декогеренцию, что делает их бесполезными для квантовых вычислений. В сочетании с тем фактом, что некоторые графовые состояния сравнительно просто подготовить в лабораторных условиях, это делает МВQC многообещающим способом практической реализации квантовых вычислений.

12.3.1. Графовые и кластерные состояния

В разделе 9.4.5 мы ввели графовые состояния



для доказательства полноты ZX-исчисления. Технология МВQC основана на *квантовых графовых состояниях*, получаемых путем дублирования:

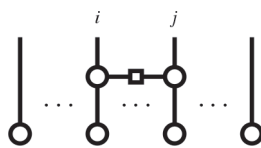


Эти многокубитовые состояния можно реализовать с помощью простой схемы следующим образом.

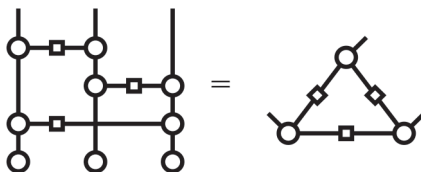
1. Подготовить n кубитов в \bigcirc -состоянии:



2. Чтобы ввести ребро между i -м и j -м кубитами, применить CZ-вентиль:

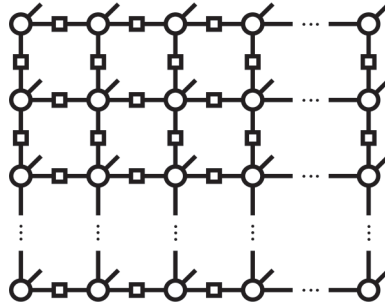


Поскольку все пауки сливаются, не важно, в каком порядке применять CZ-вентили. Мы в любом случае получим графовое состояние



Из всех графовых состояний чаще всего изучают так называемые *кластерные состояния*.

Определение 12.23. *Двумерным кластерным состоянием* называется графовое состояние, вершины которого образуют сетку $m \times n$:

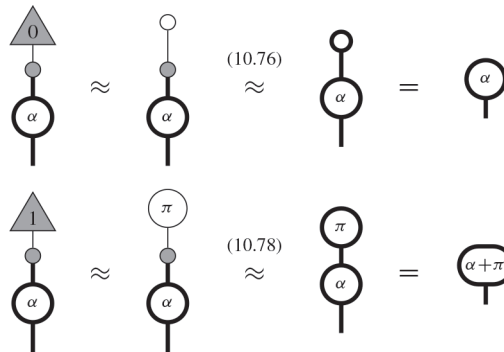


12.3.2. Измерение графовых состояний

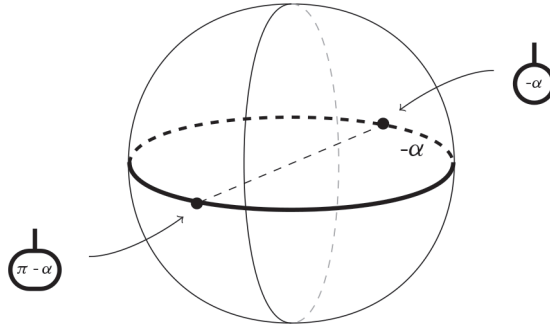
Вся магия MBQC заключена в однокубитовых измерениях. На самом деле достаточно рассмотреть всего два вида измерений:



Поскольку X_α -измерение состоит из α -фазы, за которой следует X -измерение, с ним ассоциированы такие квантовые эффекты:

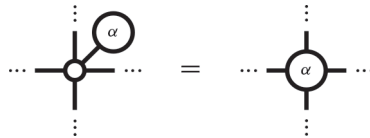


Следовательно, X_α -измерение сводится к измерению в некотором ОНБ на экваторе сферы Блоха:



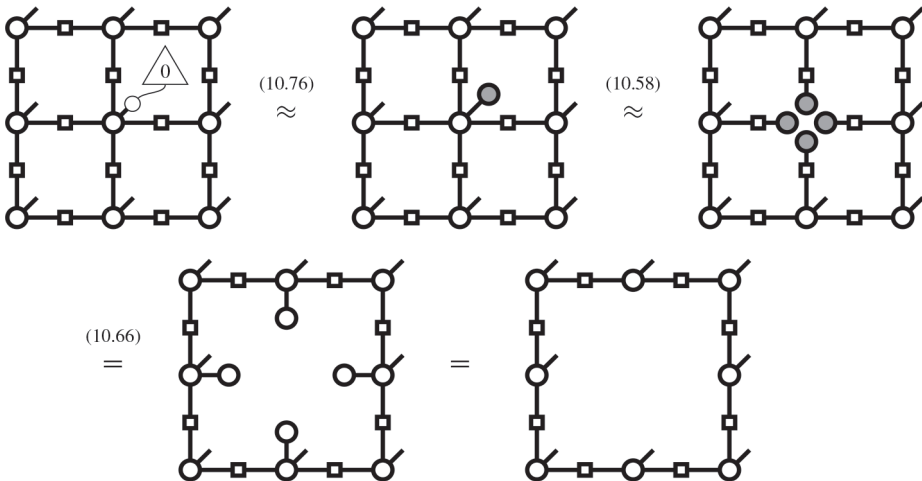
Частный случай, X_0 , конечно, является обычным X -измерением.

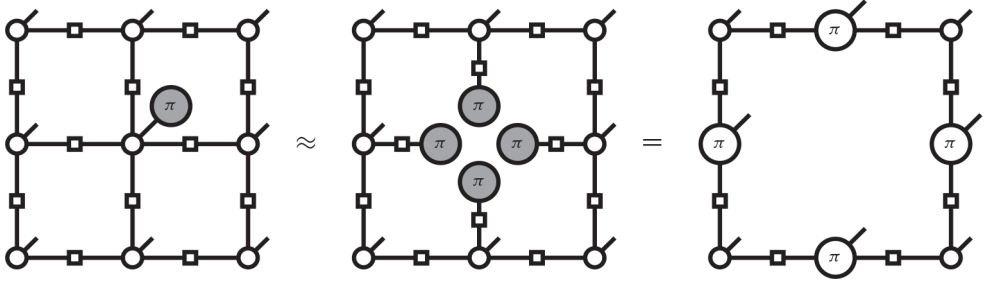
Полезность X_α -измерения заключается в том, что оно вводит фазы в графовое состояние. Например, если при измерении одного кубита мы получаем исход 0, то вводим \ominus -фазу α :



Если же мы получаем исход 1, то вместо α порождается фаза $\alpha + \pi$, что мы рассматриваем как ошибку, которую позже нужно будет исправить. Как это сделать, мы увидим в следующем разделе. Тщательно выбирая место, где производить X_α -измерения, мы можем порождать как \ominus -фазы, так и \bullet -фазы, как делали в (12.32) для реализации произвольного однокубитового унитарного отображения.

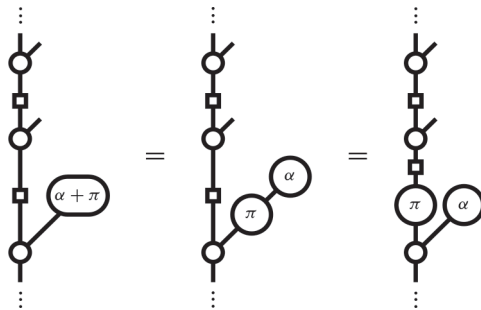
В то время как X_α -измерения вводят фазы, Z -измерения можно использовать для вырезания нежелательных кубитов из графового состояния. Например, если при выполнении Z -измерения двумерного кластерного состояния получается исход 0, то остается дырка:



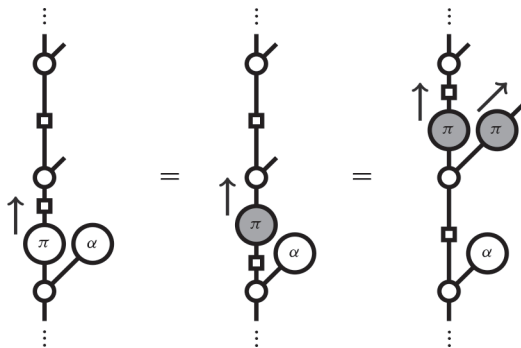


Таким образом, мы можем исправить ошибку, просто применив π -фазу к всем соседям измеренного кубита.

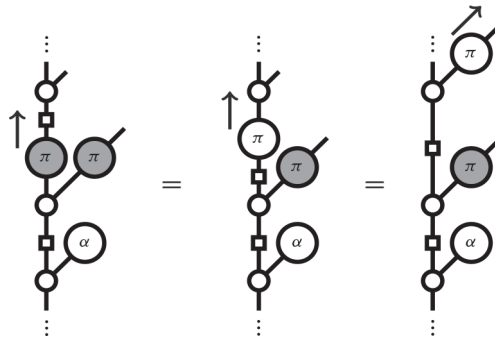
В случае X_α -измерения корректировку можно выполнить, «проталкивая» ошибку вдоль графового состояния, пока она не окажется только на выходных проводах, где ее можно исправить. Посмотрим, как это работает для одного измерения цепочки трех кубитов. Измерение первого кубита дает ошибку π . Применив правила слияния пауков, мы можем сдвинуть эту ошибку на ребро графового состояния:



Теперь, применив правила изменения цвета, π -копирования и слияния пауков, можно протолкнуть π вверх. После прохода через второй кубит ошибка все еще остается в графовом состоянии:



но после прохода через третий кубит она оказывается только на выходных проводах:



Сцепляя все вместе, получаем:

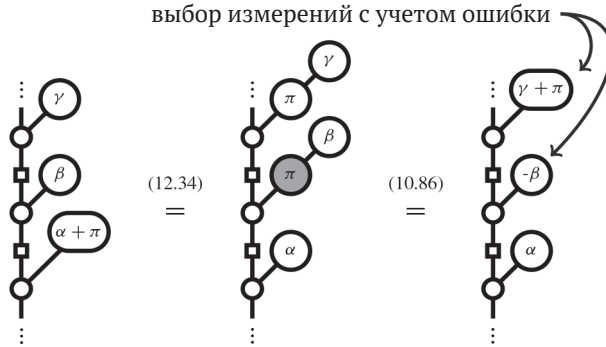
(12.34)

Теперь можно применить корректировки на втором и третьем кубитах, чтобы исправить ошибку в первом измерении:

(12.35)

что детерминированно дает фазовый вентиль с фазой α .

Если мы собираемся также измерить второй и третий кубиты, то получим эти корректировки даром, просто внося поправки в выбор последующих измерений:



Разумеется, эти измерения также могут дать ошибки, которые тоже придется исправлять.

Упражнение 12.24. Как вы стали бы исправлять ошибку измерения X_α в кластерном состоянии? Каково общее правило для любого графового состояния?

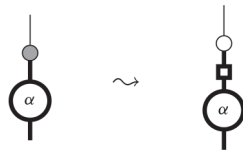
Очевидно, что изменить выбор измерения можно, только если измерения еще не произведены. Поэтому выбранный порядок измерений влияет на то, когда мы сможем внести эти поправки (и сможем ли вообще).

Упражнение* 12.25. Можно ли измерять кубиты в кластерном состоянии в таком порядке, чтобы оказалось возможным прямое распространение всех корректировок? А в произвольном графовом состоянии?

12.3.4. Прямое распространение с помощью классических проводов

Прямое распространение вроде бы работает неплохо, но где-то по дороге мы начали работать с эффектами, а не с измерениями, поэтому потеряли классические провода и, стало быть, явный поток классических данных. Можно ли их вернуть? Конечно! И вот один из способов сделать это.

Сначала сделаем все классические данные одного цвета, немного модифицировав прежнее определение X_α -измерения:

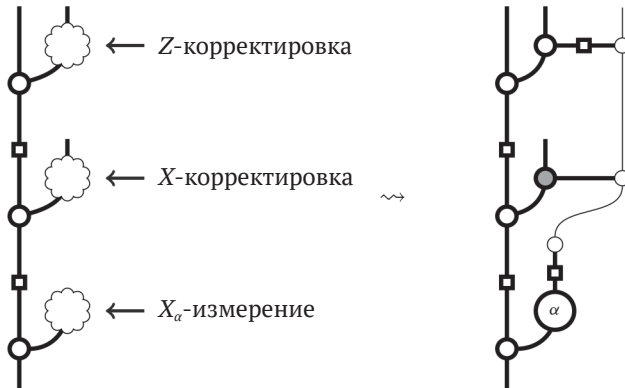


Для корректировок мы определим КК-отображения, которые в зависимости от классического входного бита либо применяют фазу π , либо не делают ничего. Нам понадобится два вида корректировок:

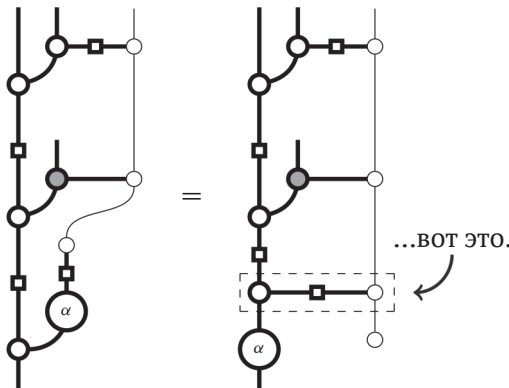


Заметим, что это почти то же самое, что корректировки (10.47), которые мы использовали раньше для квантовой телепортации. Есть только два отличия: перекрашивание классических данных в один цвет, соответствующий ассоциированным измерениям, и сохранение копии классических данных вместо ее удаления. Скоро мы увидим, зачем это нужно.

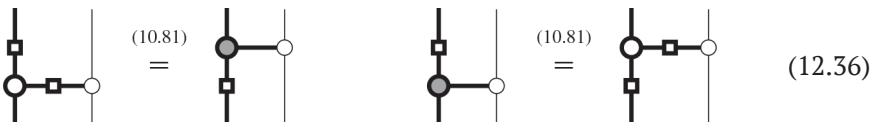
Теперь процедуру корректировки (12.35) можно переписать в виде:



Результат измерения распространяется вперед по классическому проводу и дважды используется для внесения двух корректировок. Сейчас мы покажем, что по-прежнему можем рассуждать, как и раньше, несмотря на все дополнительные провода. Единственное отличие состоит в том, что вместо проталкивания π по диаграмме, как в (12.35), мы должны попытаться протолкнуть...



Как и раньше, есть несколько ходов для выталкивания ошибки. Ход первого типа переставляет корректировку с H -вентилем, попутно меняя ее (квантовый) цвет:



Ход второго типа – проталкивание Z -корректировки сквозь \circ -паука:

$$(12.37)$$

что является не чем иным, как слиянием квантовых пауков. Ход третьего типа копирует X -корректировку сквозь \bullet -паука:

$$(12.38)$$

Это правило следует из сильной дополнителности:

$$(10.59)$$

И последнее правило сокращает две одинаковые корректировки:

$$(12.39)$$

Оба эти равенства – следствия дополнителности:

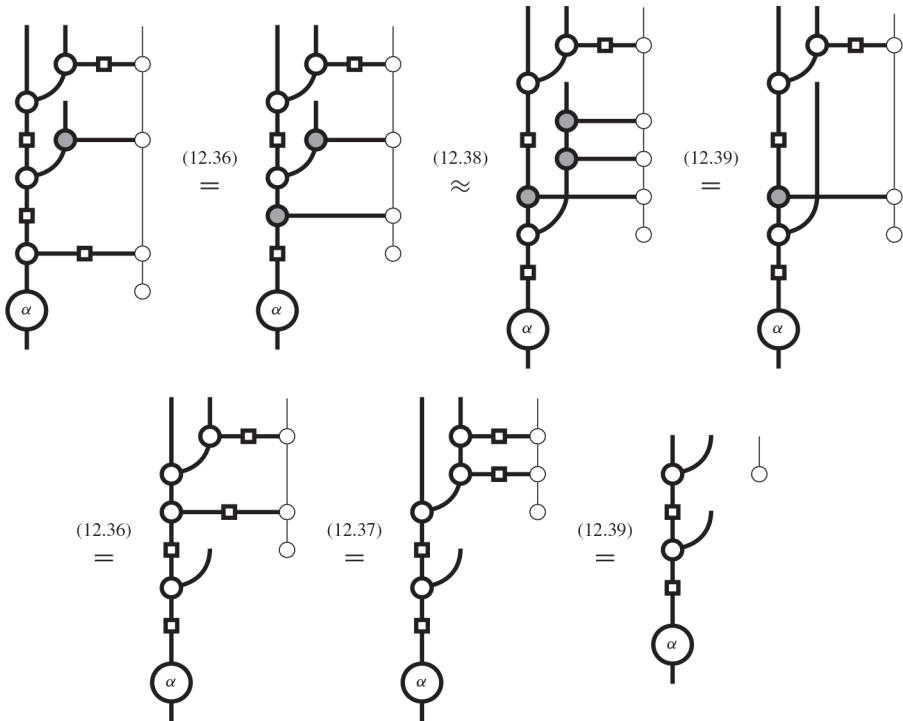
$$(10.53)$$

$$(10.81)$$

$$(10.53)$$

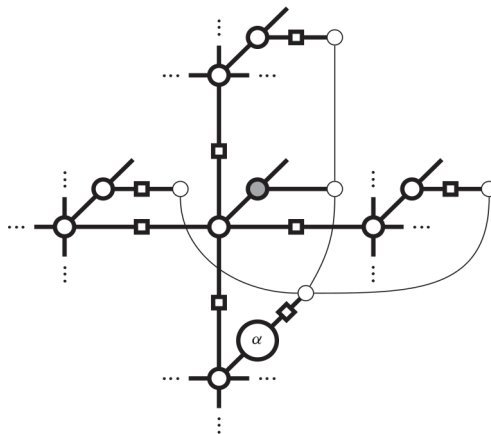
$$(10.82)$$

Теперь посмотрим на эти ходы в действии:



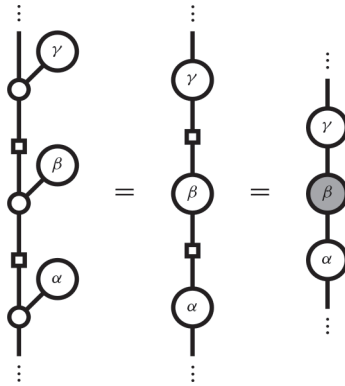
Таким образом, мы детерминированно получаем фазовый вентиль с фазой α – как и ожидалось. Единственный след измерения – сам исход, который, как можно видеть, является равномерным распределением вероятностей.

Упражнение 12.26. Воспользуйтесь правилами прямого распространения для доказательства того, что следующая диаграмма детерминированно дает фазу α на нижнем кубите

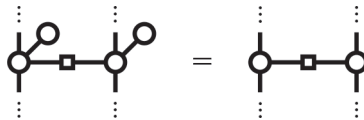


12.3.5. Универсальность

Как было показано, мы можем построить произвольные однокубитовые унитарные отображения вида

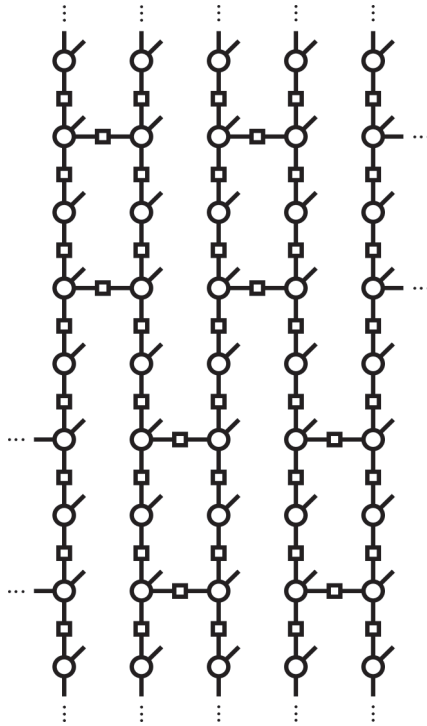


а получить CZ-вентили еще проще:

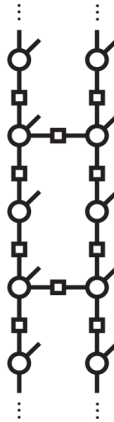


Так что, в принципе, у нас имеется все необходимое для универсального квантового вычисления (см. построение в разделе 12.1). Но как собрать все это в схему? Одно из возможных решений – начать с большого кластерного состояния и «вырезать» схему нужной нам формы с помощью Z -измерений, как в (12.33). А для заполнения фаз можно будет воспользоваться X_α -измерениями. Эта идея работает, и именно так первоначально и была доказана универсальность.

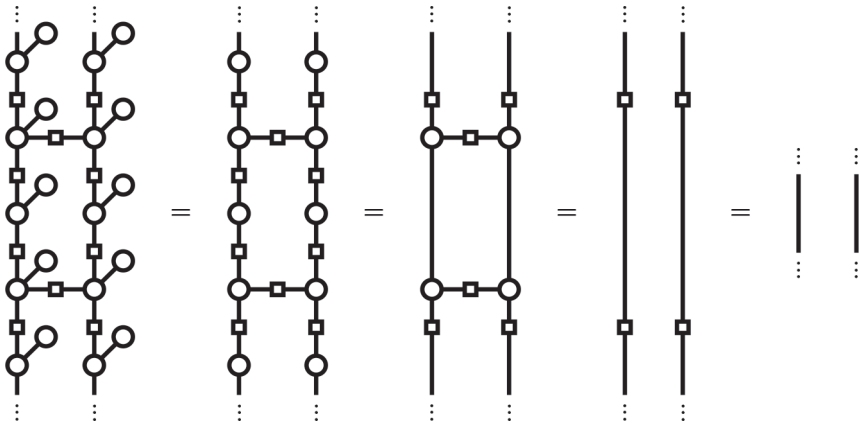
Однако если по-умному подойти к выбору начального графового состояния, то мы сможем продемонстрировать универсальность, обойдясь лишь X_α -измерениями, а вырезание не понадобится. Приятная особенность подобного подхода состоит в том, что все вычисление теперь включает только список углов. Такое состояние существует и называется *кирпичной кладкой*:



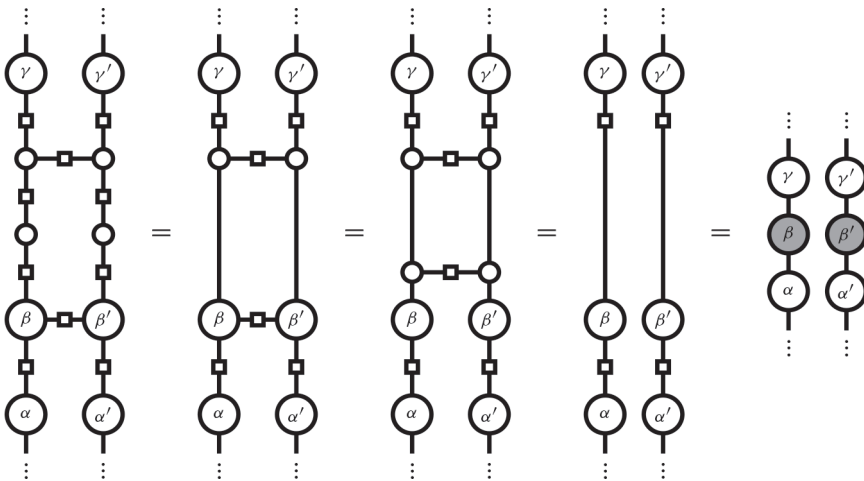
Это орнамент из повторяющихся «кирпичей»:



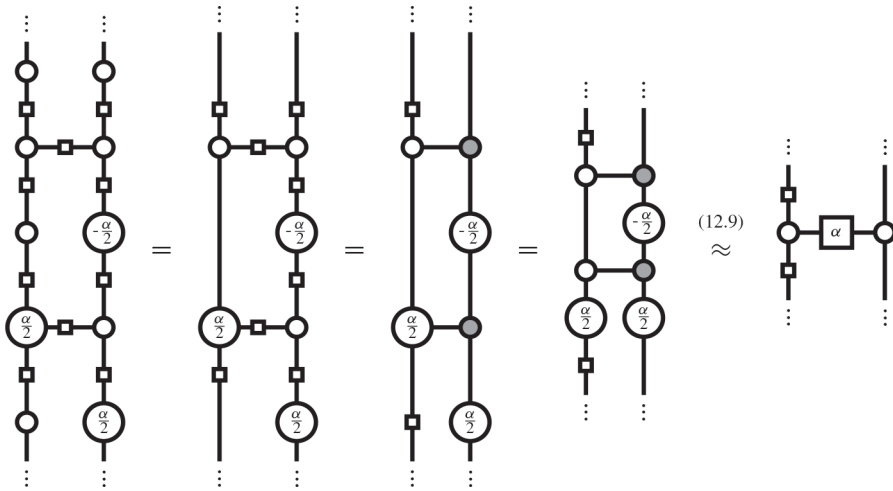
которым можно воспользоваться, чтобы решить поставленную задачу за счет одного лишь выбора углов. Если всюду выбрать 0, то кирпич не делает ничего:



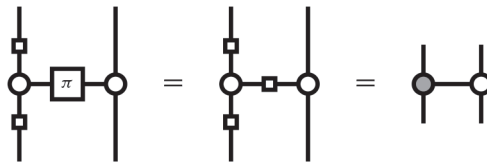
А если сделать так:



то в результате получится два произвольных однокубитовых унитарных отображения. Ну и пора поставить завершающую точку. Если бы мы могли преобразовать кирпич в CZ-вентиль, то все было бы сделано, поскольку CZ-вентили плюс однокубитовые вентили уже обеспечивают универсальность. Однако, как мы видели выше, расстановка повсюду фаз 0 создает два взаимно уничтожающихся CZ-вентилей. Но если мы поступим немного умнее:

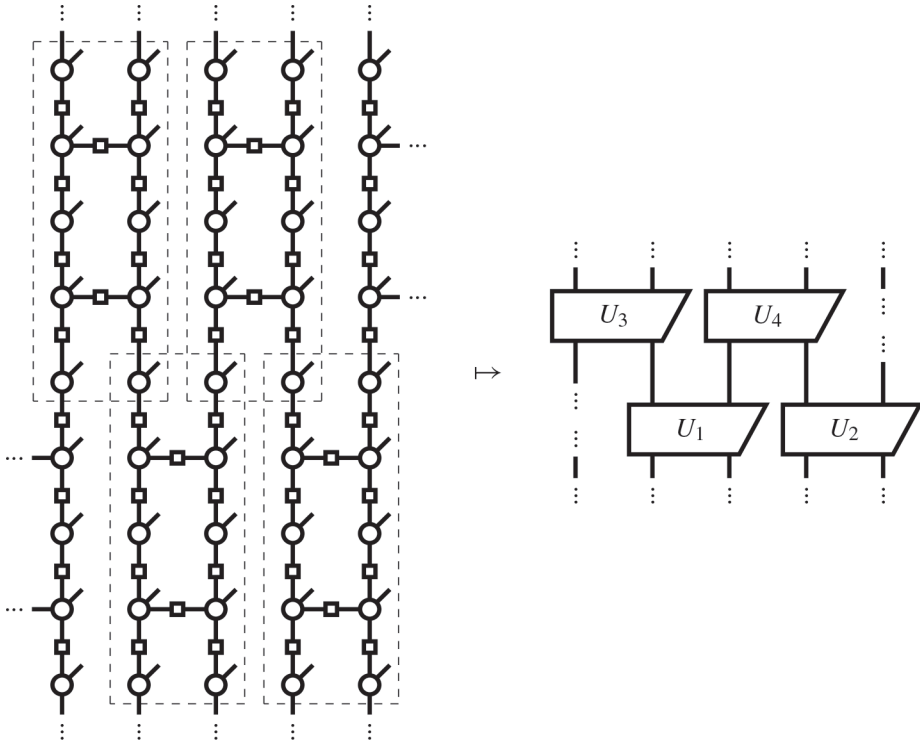


то возникнет управляемый фазовый вентиль. Это должно сработать! Действительно, при выборе $\alpha := \pi$ этот кирпич дает вентиль CNOT:



Стало быть, мы имеем универсальное множество квантовых вентиляей.

Чтобы собрать из этих вентиляей произвольную схему, мы можем задавать углы измерения для каждого кирпича (и складывать углы, если кирпичи перекрываются). Тогда кирпичную кладку в целом можно будет преобразовать в схему, состоящую из чередующихся квантовых вентиляей:



а этого достаточно для порождения любой схемы.

Упражнение 12.27. Покажите, что схему, состоящую из чередующихся однокубитовых унитарных отображений и вентилях CNOT, можно преобразовать в произвольную схему.

Чтобы последний кусочек головоломки встал на место, мы должны не только уметь восстанавливать любую схему, но и делать это **детерминированно**. Для этого должен существовать такой порядок измерения кубитов, чтобы ошибки всегда можно было распространить вперед на еще не измеренные кубиты.

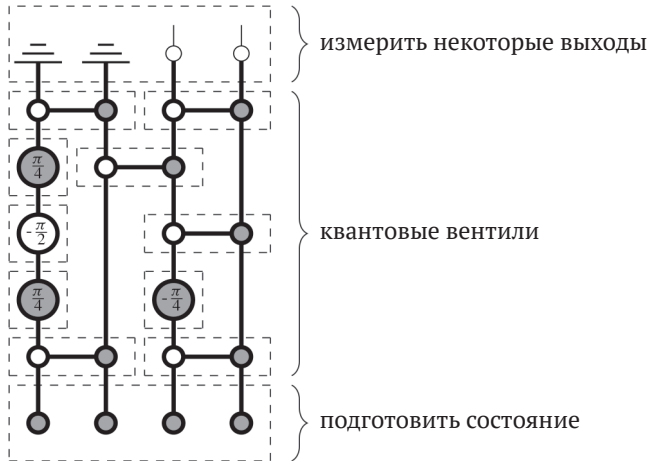
Упражнение 12.28. Покажите, что любую ошибку в строке k можно исправить, применяя корректировки только к строкам $k + 1$ и $k + 2$.

Следовательно, можно детерминированно получить любую схему, измеряя кубиты построчно, и мы доказали следующую теорему.

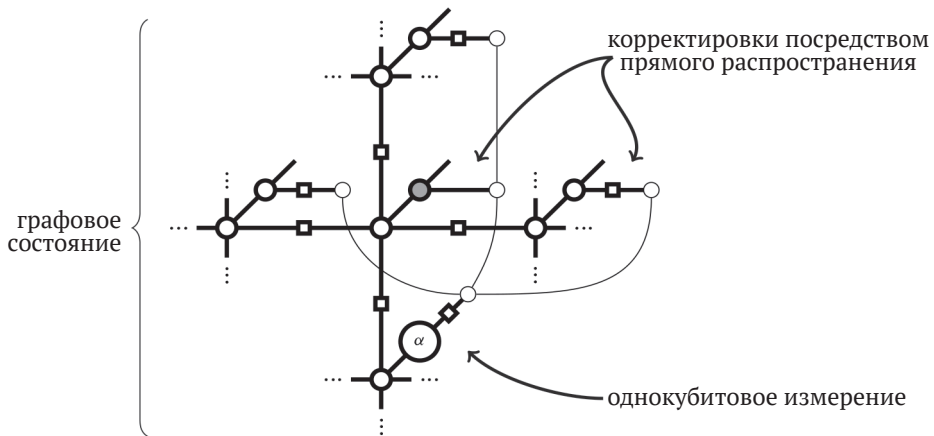
Теорема 12.29. Основанное на измерении квантовое вычисление с состояниями, образующими кирпичную кладку, и X_α -измерениями является универсальным.

12.4. Итоги: что следует запомнить

1. Существуют две важные модели квантовых вычислений: *модель квантовых схем*:

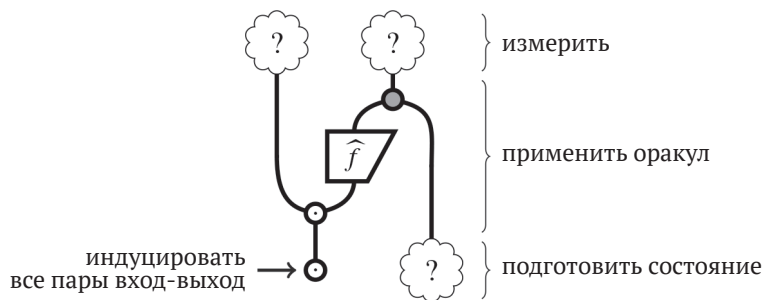


и основанные на измерении квантовые вычисления:



Обе модели *универсальны* в том смысле, что позволяют реализовать любое унитарное отображение кубитов в кубиты.

2. Любое функциональное отображение можно преобразовать в унитарное квантовое отображение, называемое *квантовым оракулом*, с помощью дополнительной пары пауков. Это составляет основу большинства квантовых алгоритмов:



3. Большинство квантовых алгоритмов решает задачи с предусловием. Мы рассмотрели следующие:

| Алгоритм | Предусловие | Задача | Диаграмма |
|-------------------|--|---|-----------|
| Дойча-Йожи | f постоянная или сбалансированная | Какая именно? | |
| Квантового поиска | f отображает одну из четырех битовых строк в 1 | Найти такое i , для которого $f(i) = 1$ | |
| Скрытая подгруппа | f принимает одинаковые значения на элементах некоторой подгруппы $H \subseteq G$ | Найти H | |

Частным случаем задачи о скрытой подгруппе является задача о *нахождении периода*, решение которой позволяет эффективно разлагать большие числа на множители.

12.5. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Первые намеки на квантовые вычисления появились в работе Paul Benioff (1980), где были описаны квантово-механические модели компьютеров, и в работе знаменитого математика Юрия Манина (Yuri Manin, 1980), предложившего идею квантовых вычислений. Но она была написана во времена холодной войны и по-русски. Поэтому многие приписывают квантовые вычисления Ричарду Фейнману из-за лекции, которую он прочел в МТИ в 1981 году. (Отметим, что это уже второй раз, когда имя Фейнмана упоминается в этой книге в нелицеприятном свете.) Первый универсальный квантовый компьютер был описан в работе Дэвида Дойча (David Deutsch, 1985), использовавшего понятие *квантовой машины Тьюринга*. С тех пор ее место прочно заняла более простая схемная модель, также принадлежащая Дойчу (Deutsch, 1989). Первое доказательство универсальности схемной модели дано в работе Varenco et al. (1995). Приведенное нами доказательство частично основано на гораздо более простом доказательстве из работы Shende et al. (2006).

Алгоритм Дойча–Йожи опубликован в работе Deutsch and Jozsa (1992), алгоритм разложения на множители – в работах Shor (1994, 1997), и алгоритм квантового поиска – в работе Grover (1996). Алгоритм нахождения скрытой подгруппы, а также сведение к нему алгоритма Шора и задачи Саймона предложены в работе Jozsa (1997). В сообществе, связанном с квантовыми вычислениями, широко распространено заблуждение, будто алгоритм Дойча–Йожи является частным случаем этой же задачи, но, как показано в упражнении 12.22, это так только при $N = 1$. К недавним исследованиям квантовых алгоритмов относятся работы Ambainis (2010) и Montanaro (2015).

Применениям квантового пикторализма к квантовым схемам посвящены работы Voixo and Heunen (2012) и Ranchin and Coecke (2014), в которых можно найти решение упражнения* 12.1. Основы диаграммного подхода к квантовым алгоритмам были заложены в работе Vicary (2013) и получили дальнейшее развитие в работах Zeng and Vicary (2014) и Zeng (2015). Диаграммный вывод алгоритма нахождения скрытой подгруппы описан в работе Gogioso and Kissinger (2016).

Односторонняя модель MBQC впервые предложена в работе Raussendorf and Briegel (2001) и развита в работе Raussendorf et al. (2003). Графовые состояния предложены в работе Hein et al. (2004). Диаграммный подход впервые предложен в работах Coecke and Duncan (2008, 2011) и развит в работе Duncan and Perdrix (2010). Методы, применявшиеся ранее в модели MBQC, были усовершенствованы с применением ZX-исчисления в работе Duncan and Perdrix (2010); в работе Horsman (2011) дано основанное на ZX-исчислении изложение *топологической MBQC* (Raussendorf et al., 2007). Обзор MBQC в контексте ZX-исчисления приведен в работе Duncan (2012).

Хотя практически пригодных квантовых компьютеров еще не существует, в лабораторных условиях достигнут значительный прогресс. Первая реализация квантового алгоритма на трехбитовом квантовом компьютере на ядерном магнитном резонансе осуществлена в Оксфорде Джонсом с коллегами (Jones et al. 1998). В 2000 году компьютер на пяти кубитах был реализован в Мюнхене, а компьютер на семи кубитах – в Лос-Аламосе. Улучшилась также достоверность квантовых вычислений. Например, в работе Ballance et al. (2016) реализованы одно- и двухкубитовые вентили с достоверностью 99,9 % на захваченных ионах. Первая реализация MBQC была осуществлена в Вене (Walther et al. 2005).

Глава 13

Квантовые ресурсы

В своей жизни я возносил только одну молитву: «О, Боже, сделай моих врагов смешными. И Господь даровал мне это».

– Вольтер,
письмо Этьену Нозлю Дамилавиллю, 1767

Банкиры с Уолл-стрит могут иметь все, что пожелают, в каких угодно количествах, но эта глава для всех остальных – людей, более ограниченных в средствах. На протяжении этой книги предполагалось, что мы, подобно квантовым банкирам, имеем доступ к любым нужным нам процессам в любом количестве. Например, говоря о телепортации, мы предполагали, что можем получать состояния Белла, когда нам заблагорассудится, и производить совместные измерения пар систем. Говоря о нелокальности, мы считали, что вокруг полно ГХЦ-состояний, поэтому мы можем сделать достаточно измерений и убедиться в том, как рушатся предположения о локальности. А в случае МВQC мы полагали, что в нашем распоряжении имеются гигантские графовые состояния, необходимые для реализации универсального квантового вычисления.

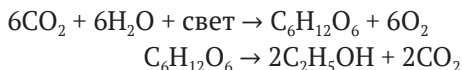
Но, как и следовало ожидать, все эти предметы отнюдь не дешевы! Для реализации квантовых процессов, включающих несколько систем, обычно необходимо узкоспециализированное оборудование и много часов работы. Поэтому, когда дело доходит до таких *ресурсов*, надлежит думать о том, как бы сделать как можно больше, затратив как можно меньше. Это, конечно, относится не только к квантовым состояниям, но и к любым другим ресурсам: углю, нефти, атомной, ветровой и солнечной энергии, некоторым химическим веществам или просто эмоциям.

В отношении любого ресурса важно, что именно с его помощью можно сделать. Если рассматривать блага, получаемые от использования ресурсов (например, теплые, комфортабельные жилища или безопасную связь) как сами ресурсы, то практически все вопросы о ресурсах сводятся к двум:

- 1) можно ли данный ресурс преобразовать в какой-то другой?
- 2) какое количество ресурса X потребно для получения ресурса Y?

Именно на эти вопросы призвана ответить *ресурсная теория*.

Идея «преобразования ресурсов», в частности, находит очень явное выражение в изучении химических реакций, где встречаются формулы вида:



Такая формула означает, что мы можем преобразовать вещество в левой части в вещество в правой части. И хотя формула не сообщает деталей фактического осуществления подобного преобразования, она все же дает два весьма полезных факта. Во-первых, указано, какое количество одного ресурса нужно для получения определенного количества другого, а во-вторых, перечисляются все ресурсы, в которые может быть преобразован данный ресурс. Очевидно, что чем шире диапазон веществ, в которые можно преобразовать ресурс, тем он ценнее.

Это верно для ресурсов любого вида, включая приведенные выше квантовые. Мы перечислили несколько запутанных состояний, которые хороши для различных задач, но если некоторое запутанное состояние легко преобразовать в другое запутанное состояние, то очевидно, что оно должно находиться на вершине пищевой цепочки. Эта идея лежит в основе *ресурсной теории запутывания*.

Конечно, запутывание – не единственный квантовый ресурс, представляющий интерес. Учитывая, что реальные устройства обычно реализуют квантовые процессы ненадежно и вносят при этом значительный шум, вполне естественно строить изучение *чистоты* квантовых состояний как ресурсную теорию. Есть и другие, еще более утонченные ресурсы. Например, при выполнении квантового распределения ключей обобществление системы отсчета, т. е. согласование Z - и X -пауков, – это важнейший ресурс.

Но что такое на самом деле ресурсная теория? Ну, конечно же, это процессная теория! Точнее, это процессная теория с весьма своеобразной интерпретацией: типы в ней представляют ресурсы, а процессы – преобразования. Из процессной теории можно вывести *отношение конвертируемости*, которое, в свою очередь, дает *курс конвертации* ресурсов, подходящие *меры* (стоимости), сведения о наличии в теории *катализаторов* и т. д.

Попутно мы сделаем два интересных наблюдения. В ходе изучения ресурсных теорий чистоты и запутывания мы увидим, что хотя отношения конвертируемости в них выглядят «количественными», мы тем не менее сможем доказать теоремы о строгой характеристике с помощью диаграмм. Более того, при изучении запутывания трех кубитов мы увидим, что каждый из максимальных *классов запутывания* характеризуется определенным видом пауков. Один из таких пауков нам уже прекрасно знаком, поскольку он был главным персонажем последних пяти глав. А вот другой паук на него совсем не похож. Вместо того чтобы радостно сливаться со своими соседями, он взрывается:

$$\text{Circular node with two triangles} = \frac{1}{D} \text{Vertical chain of four nodes with two triangles each}$$

13.1. РЕСУРСНЫЕ ТЕОРИИ

Ресурсная теория – это, по сути дела, процессная теория, только с другой фразеологией.

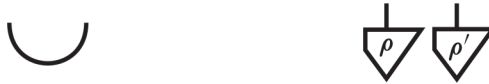
Определение 13.1. *Ресурсной теорией* называется процессная теория, типы которой называются *ресурсами*, а процессы – *преобразованиями ресурсов*.

И это меняет все!

Например, мы могли бы определить ресурсную теорию **пищи**, в которой системами являются ингредиенты, а процессами – способы приготовления блюд, т. е. преобразования одного вида пищи в другой. Сырую морковь можно преобразовать в вареную, а вареную морковь и чашку бульона – в суп. Другой пример – теория **энергии**, в которой ресурсами являются формы энергии, а преобразования ресурсов превращают одну форму энергии в другую: уголь в тепло, тепло в электричество, электричество в работу и т. д.

13.1.1. Бесплатные процессы

Для процессных теорий, например теории **квантовых процессов**, все состояния данного типа рассматриваются одинаково. Однако очевидно, что между следующими двумя состояниями существует большая разница в плане того, что с ними можно делать:



Например, первое позволяет осуществить телепортацию, а второе – нет. Чтобы отразить это различие в рамках процессной теории, мы будем рассматривать сами состояния как разные типы. Таким образом, состояния в такой процессной теории, как **квантовые процессы**, становятся типами в конструируемой ресурсной теории. Одни типы (т. е. ресурсы) полезны для телепортации, а другие – абсолютно бесполезны.

В нашей теории типы будут связаны посредством процессов (т. е. преобразований ресурсов). Но какими должны быть эти процессы? Один из вариантов – взять в качестве преобразований ресурса ρ в ресурс ρ' все процессы исходной процессной теории, которые трансформируют ρ в ρ' :

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \Phi \\ | \\ \text{---} \\ | \\ \rho \end{array} = \begin{array}{c} \text{---} \\ | \\ \rho' \end{array} \tag{13.1}$$

Однако так мы не получим ничего полезного. Например, если мы изучаем запутывание, то хотели бы, чтобы из структуры ресурсной теории **запутывания** можно было узнать, что состояние Белла – гораздо более ценный ресурс, чем произвольное разделяемое состояние. Но если включить в качестве преобразований ресурсов все процессы, то мы просто сможем использовать следующий процесс

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} :: \begin{array}{c} \text{---} \\ | \\ \rho \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \rho' \\ \text{---} \end{array} \mapsto \begin{array}{c} \text{---} \\ \text{---} \end{array} \tag{13.2}$$

для преобразования любого состояния, включая разделяемые, в состояние Белла!

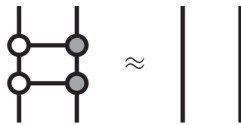
Поэтому мы должны отличать те процессы, которые позволяют «создать» большее количество нашего ресурса (в данном случае запутывания), от тех, которые не позволяют. Например, квантовый процесс



допустим, поскольку он может только уничтожить запутывание, а квантовый процесс (13.2) недопустим, поскольку он способен создать запутывание там, где его раньше не было.

Процесс, который только уменьшает (или сохраняет неизменным) представляющий интерес ресурс, называется *бесплатным процессом*. Этот термин подразумевает, что остальные процессы «стоят дорого», поэтому мы хотим воздержаться от их использования. Композиция двух бесплатных процессов тоже должна быть бесплатной, поэтому бесплатные процессы образуют подтеорию ресурсной теории.

Замечание 13.2. С другой стороны, платные процессы обычно не образуют процессной теории. Например, вентиль CNOT может породить новое запутывание, поэтому не должен быть бесплатным, но двукратное применение CNOT



не делает ничего, поэтому, конечно же, бесплатно!

Заметим, что *бесплатные состояния* являются процессами в \mathbf{F} :



которые преобразуют «ничто» в само состояние. Это точно соответствует идее «бесплатности»: получить что-то, не отдав взамен ничего.

Все это можно учесть, специализировав определение 13.1 на такие ресурсные теории, которые получаются из базовой процессной теории.

Определение 13.3. Пусть дана процессная теория \mathbf{P} и подтеория \mathbf{F} *бесплатных процессов*. Определим соответствующую ресурсную теорию

P-состояния/F

как процессную теорию, в которой:

- типами являются состояния \mathbf{P} ;
- процессами являются процессы \mathbf{F} , которые преобразуют ρ в ρ' .

Красота таких ресурсных теорий заключается в том, что никогда не нужно определять точный смысл фразы «состояние располагает объемом ресурса X». Например, ниже мы увидим, что вопрос, «насколько» запутано данное состояние,

поставлен некорректно, потому что состояния могут быть запутаны различными неэквивалентными способами. С другой стороны, если мы определили, что такое бесплатные процессы, то можем сразу же приступить к сравнению ресурсов.

13.1.2. Сравнение ресурсов

Определение 13.4. Пусть дана ресурсная теория \mathbf{R} . Говорят, что ресурс A может быть преобразован в ресурс B , и записывают это в виде:

$$A \geq B,$$

если в \mathbf{R} существует процесс, отображающий A в B :



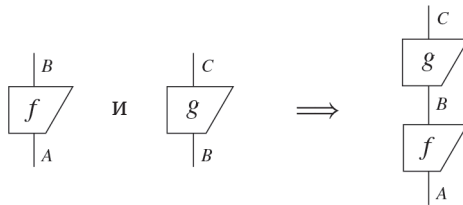
Ресурсы A и B называются *эквивалентными*, если $A \geq B$ и $B \geq A$. В таком случае мы пишем:

$$A \simeq B.$$

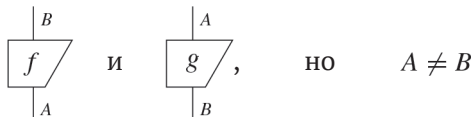
У этого определения есть три очевидных следствия. Во-первых, отношение \geq *рефлексивно*, т. е. $A \geq A$, т. к. тождественный процесс преобразует A в себя:



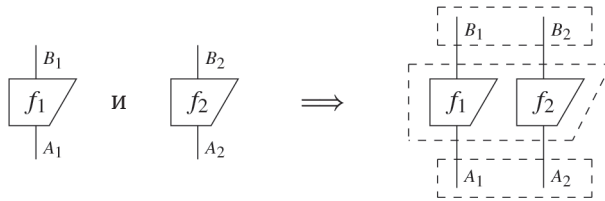
Оно также *транзитивно*, т. е. если $A \geq B$ и $B \geq C$, то $A \geq C$ в силу \circ -композиции:



Из этих двух свойств вытекает, что отношение \geq является отношением *предпорядка*. Однако \geq необязательно является отношением *частичного порядка*, т. е. предпорядка, обладающего еще свойством антисимметричности: если $A \geq B$ и $B \geq A$, то $A = B$, поскольку вполне можно представить себе ресурсы, которые преобразуются друг в друга, но при этом не равны. То есть может случиться, что



Отношение \geq не только является предпорядком, но и согласуется с операцией \otimes :



Сводя все вместе, получаем следующую теорему.

Теорема 13.5. Если R – множество ресурсов в ресурсной теории, то четверка

$$(R, \geq, \otimes, I)$$

образует *предупорядоченный моноид*. Это означает, что тройка (R, \otimes, I) является моноидом:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C), \quad A \otimes I = A = I \otimes A,$$

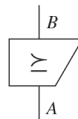
(R, \geq) определяет предпорядок:

$$A \geq A, \quad A \geq B \text{ и } B \geq C \Rightarrow A \geq C,$$

и обе эти структуры согласованы:

$$A_1 \geq B_1 \text{ и } A_2 \geq B_2 \Rightarrow A_1 \otimes A_2 \geq B_1 \otimes B_2.$$

Замечание 13.6. Предупорядоченный моноид можно эквивалентно определить как процессную теорию, в которой существует не более одного процесса любого заданного типа, который можно было бы записать в виде:



Наличие такого процесса просто устанавливает тот факт, что $A \geq B$. Поэтому переход от ресурсной теории к предупорядоченному моноиду (R, \geq, \otimes) можно рассматривать как переход от большой процессной теории с кучей разных процессов к гораздо меньшей, в которой мы только запоминаем, существовали процессы заданного типа или нет.

В самом начале книги мы видели, что в процессных теориях \circ -композиция и \otimes -композиция процессов рассматриваются на равных. Аналогично конвертируемость ресурсов тесно переплетена с \otimes -композицией систем. Хотя монету в один фунт, вероятно, нельзя преобразовать в дом в Оксфорде, миллион таких монет позволит приобрести нечто вроде



Следовательно, добавление \otimes дает возможность обменять некое количество одного ресурса на некое количество другого. Иными словами, мы можем выразить курс, по которому один ресурс конвертируется в другой.

Определение 13.7. Для ресурсов A и B в ресурсной теории *курсом конвертации* называется величина

$$r(A \succeq B) := \text{supremum} \left\{ \frac{N}{M} \mid \underbrace{A \otimes \dots \otimes A}_M \succeq \underbrace{B \otimes \dots \otimes B}_N \right\}.$$

Если рассматривать ресурсную теорию, содержащую только описанный выше процесс, то курс конвертации фунтов в дома в Оксфорде равен $1/1\,000\,000$. То есть один фунт конвертируется в одну миллионную часть дома в Оксфорде. Чудо что за сделка!

Замечание* 13.8. Поскольку курс конвертации вычисляется как точная верхняя грань, в общем случае он может быть иррациональным числом. Взять, к примеру, теорию, в которой ресурсами являются куски веревки, из которых можно строить разные фигуры, при необходимости разрезая. Тогда для получения окружности диаметра 1 понадобятся 4 веревки длины 1:



а для получения двух окружностей – только 7 таких веревочек:



Для трех окружностей нужно 10 веревок, для четырех – 13 и т. д. Продолжая до бесконечности, мы будем приближаться к оптимальному курсу, который определяется точной верхней гранью:

$$\supremum \left\{ \frac{1}{4}, \frac{2}{7}, \frac{3}{10}, \frac{4}{13}, \dots \right\} = \frac{1}{\pi}$$

Таким образом, для получения одной окружности оптимально необходимо π кусков веревки.

Отношение конвертируемости полностью забывает о том, что такое процессы в ресурсной теории, а помнит лишь, существует ли некий процесс. Тем не менее оно уже содержит немало информации о структуре ресурсной теории. Например, оно сообщает, есть ли в нашей ресурсной теории катализаторы, т. е. ресурсы C , для которых:

$$A \otimes C \geq B \otimes C, \text{ но } A \not\geq B.$$

Оно также говорит, являются ли ресурсы *количественно-подобными*:

$$\left. \begin{array}{l} A_1 \otimes A_2 \simeq B_1 \otimes B_2 \\ A_1 \geq B_1 \end{array} \right\} \implies B_2 \geq A_2,$$

т. е. ведут себя как «количество чего-то», характеризуемое тем, что целое всегда является суммой своих частей. Аналогично, оно говорит, являются ли ресурсы *не-взаимодействующими*:

$$A \geq B_1 \otimes B_2 \implies \exists A_1, A_2 : \left\{ \begin{array}{l} A \simeq A_1 \otimes A_2 \\ A_1 \geq B_1 \\ A_2 \geq B_2 \end{array} \right. .$$

Это означает, что если ресурс порождает несколько объектов, то мы можем «разрезать его» и произвести каждый объект независимо.

Упражнение 13.9. Докажите, что если ресурсная теория количественно-подобная и не-взаимодействующая, то она также *некаталитическая*:

$$A \otimes C \geq B \otimes C \Rightarrow A \not\geq B.$$

13.1.3. Измерение ресурсов

Физики, как и многие другие, любят вещественные числа. В этом нет ничего плохого, пока любовь не превращается в одержимость. Когда речь заходит об измерении значения ресурса, числа могут быть частью истории, но история ими никогда не исчерпывается, поскольку они зачастую не способны передать важную информацию. Это связано с тем, что на множестве вещественных чисел определен не просто частичный, а *полный порядок*, т. е. для любых двух вещественных чисел a и b имеет место

$$\text{либо } a \geq b, \text{ либо } b \geq a.$$

Поэтому если мы хотим сравнивать два ресурса, сопоставив им вещественные числа, то всегда будем иметь

$$A \geq B \quad \text{или} \quad B \geq A.$$

Но что, если неверно ни то, ни другое?

Важнейший пример дает запутывание. Хотя использование чисел для измерения запутывания отлично работает для пары кубитов, в разделе 13.3.2 мы увидим, что если система чуть посложнее (например, состоит из трех кубитов), то все ломается, как раз потому что появляются несравнимые состояния. Вместо «большого» или «меньшего» запутывания эти состояния дают разные виды запутывания. Однако это не помешало ученым придумать кучу способов измерить запутывание вещественными числами, которые хорошо работают для одних состояний и плохо для других.

С другой стороны, когда речь заходит об измерении нечистоты квантовых состояний, появляется знаменитое число, называемое *энтропией*, которое прекрасно подходит, чтобы оценить степень нечистоты состояния.

Но прежде чем забираться в эти дебри, зададимся вопросом: как сопоставить ресурсам числа, чтобы не возникало противоречий? Начнем с наделения множества положительных вещественных чисел $\mathbb{R}_{\geq 0}$ структурой предупорядоченного моноида. В качестве \geq мы всегда берем обычное упорядочение положительных вещественных чисел, но тогда для определения \otimes есть много вариантов. Например, мы можем взять в качестве \otimes сумму двух положительных вещественных чисел. Тогда очевидно, что

$$a \geq a' \text{ и } b \geq b' \Rightarrow a + b \geq a' + b'.$$

Но можно также использовать в этом качестве операцию

$$\max(a, b) := \begin{cases} a & \text{если } a \geq b \\ b & \text{если } b \geq a \end{cases}$$

Упражнение 13.10. Покажите, что операция \max ассоциативна:

$$\max(a, \max(b, c)) = \max(\max(a, b), c)$$

и совместима с \geq , т. е.:

$$a \geq a' \text{ и } b \geq b' \Rightarrow \max(a, b) \geq \max(a', b').$$

В зависимости от выбора той или иной операции мы получаем два разных предупорядоченных моноида:

$$\mathcal{R}^+ := (\mathbb{R}_{\geq 0}, \geq, +, 0), \quad \mathcal{R}^{\max} := (\mathbb{R}_{\geq 0}, \geq, \max, 0),$$

и два соответствующих им вида мер.

Определение 13.11. Пусть дана ресурсная теория. *Аддитивной мерой* называется функция

$$M : (R, \geq, \otimes) \rightarrow \mathcal{R}^+,$$

где

$$A \geq B \Rightarrow M(A) \geq M(B), \quad M(A \otimes B) = M(A) + M(B).$$

Аналогично *супремальной мерой* называется функция

$$M : (R, \geq, \otimes) \rightarrow \mathcal{R}^{\max},$$

где

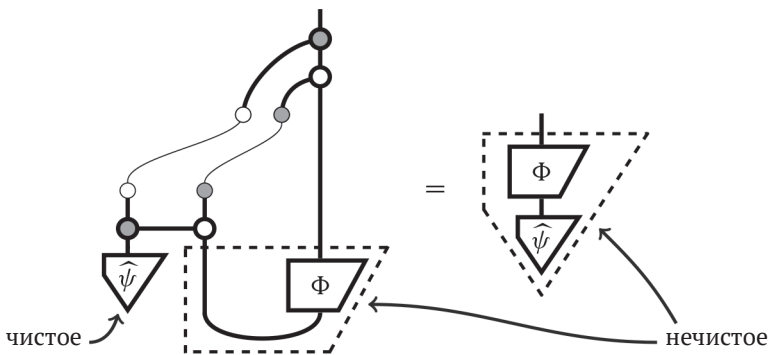
$$A \geq B \Rightarrow M(A) \geq M(B), \quad M(A \otimes B) = \max(M(A), M(B)).$$

Мера дает только частичную информацию о ресурсной теории и отношении конвертируемости \geq в ней. Важно отметить, что меры можно использовать для доказательства того, что данный ресурс нельзя преобразовать в другой, потому что если $M(A) < M(B)$, то не может быть так, что $A \geq B$. Однако обратное неверно. Возможно, что $M(A) \geq M(B)$, даже если преобразования $A \geq B$ не существует.

С другой стороны, обычно числа гораздо проще сравнивать, чем ресурсы, с которыми они ассоциированы, поэтому в тех редких случаях, когда мера действительно полностью отражает свойства отношения \geq , мы бываем очень довольны.

13.2. ТЕОРИЯ ЧИСТОТЫ

Как правило, в квантовой теории мы ценим максимально чистые состояния и процессы. Например, состояние Белла в квантовой телепортации ценно не только потому, что оно запутанное, но и потому, что оно чистое. Если вместо этого мы будем использовать в телепортации нечистое состояние, то результирующее состояние унаследует нечистоту:



Подобное введение небольшой толики нечистоты не страшно, да, собственно, и неизбежно, потому что чистые состояния – недостижимый на практике идеал. Но если нечистоты слишком много, то довольно скоро мы начнем получать мусор, например максимально смешанное состояние. Поэтому чистота – важный ресурс. В этом разделе мы определим ресурсную теорию для чистоты и покажем, как можно сравнивать и численно выражать чистоту состояний.

13.2.1. Сравнение чистоты

Если предметом наших забот является именно чистота, то бесплатными должны быть в точности те процессы, которые не могут создать новую чистоту. В частности, они должны сохранять максимальную нечистоту:

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \diagup \\ \Phi \\ \diagdown \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \frac{1}{D'} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

или эквивалентно:

$$\frac{D'}{D} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \diagup \\ \Phi \\ \diagdown \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad (13.3)$$

где D – размерность входа Φ , а D' – размерность его выхода.

Определение 13.12. Пусть теория **унитальных квантовых отображений** – это подтеория теории **каузальных квантовых отображений**, полученная ограничением на процессы, удовлетворяющие условию (13.3). Тогда

чистота := каузальные квантовые состояния/унитальные
квантовые отображения.

Следующее предложение дает альтернативную характеристику унитарных квантовых отображений.

Предложение 13.13. Квантовое отображение Φ унитарно тогда и только тогда, когда

$$\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \diagup \\ \Phi \\ \diagdown \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \quad \text{и} \quad \frac{D'}{D} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \diagup \\ \Phi \\ \diagdown \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

каузальны.

Доказательство. Унитарные квантовые отображения каузальны по определению, а если применить адъюнкцию к (13.3), то получающееся равенство выражает каузальность $(D'/D)\Phi$. \square

Так, в частности, если входные и выходные типы квантового отображения Φ имеют одинаковую размерность, то Φ унитарно в точности тогда, когда Φ и адъюнкт Φ каузальны. Поэтому если квантовое отображение чистое и унитарное, то оно само и его адъюнкт должны быть изометриями, откуда сразу вытекает следующая характеристика.

Следствие 13.14. Чистое квантовое отображение унитарно тогда и только тогда, когда оно унитарно.

Получается, что чистые унитарные отображения могут существовать только между системами одинаковой размерности, поэтому, в частности, не существует

чистых унитарных состояний или эффектов. Среди нечистых отображений существует ровно одно унитарное состояние:

$$\frac{1}{D} \underline{\underline{\underline{\mathbb{1}}}}$$

Это следует из того, что отбрасывание – единственный каузальный эффект. Следовательно, максимально смешанное состояние – единственное бесплатное состояние в теории **чистоты**. Поэтому разумно ожидать, что его можно получить путем преобразования из любого другого состояния. Это действительно возможно, потому что процесс, который отбрасывает состояние и заменяет его максимально смешанным:

$$\frac{1}{D} \underline{\underline{\underline{\mathbb{1}}}} :: \rho \triangleright \mapsto \frac{1}{D} \underline{\underline{\underline{\mathbb{1}}}}$$

очевидно, унитарный, а потому является бесплатным в теории **чистоты**. Отсюда:

$$\rho \triangleright \geq \frac{1}{D} \underline{\underline{\underline{\mathbb{1}}}}$$

Не так поразительно, что процесс, который добавляет шум в заданное состояние

$$(1-p) \left| + \frac{p}{D} \underline{\underline{\underline{\mathbb{1}}}} \right. \tag{13.4}$$

также является бесплатным в теории **чистоты**; он называется *шумовым отображением*. Поскольку

$$(1-p) \left| + \frac{p}{D} \underline{\underline{\underline{\mathbb{1}}}} \right. :: \rho \triangleright \mapsto (1-p) \rho \triangleright + \frac{p}{D} \underline{\underline{\underline{\mathbb{1}}}}$$

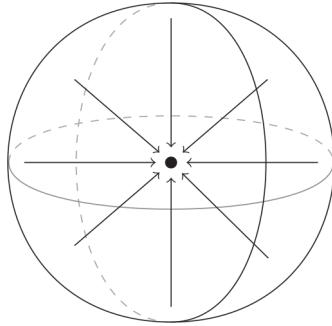
то

$$\rho \triangleright \geq (1-p) \rho \triangleright + \frac{p}{D} \underline{\underline{\underline{\mathbb{1}}}}$$

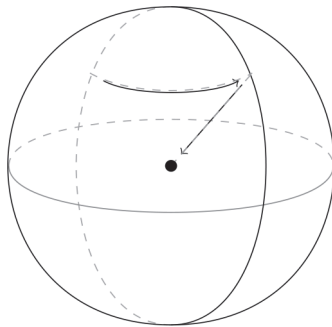
Замечание 13.15. В литературе по квантовой информации, а особенно по квантовой оптике, шумовое отображение часто называют *деполяризующим каналом*.

Итак, какие состояния можно преобразовать в другие с помощью унитарных квантовых отображений? Если изначально ограничиться кубитами, то мы получим представление об этом, взглянув на геометрию шара Блоха. Мы уже знаем, что унитарные и шумовые отображения – бесплатные процессы, поэтому можем

посмотреть, как они воздействуют на шар Блоха. Поскольку шумовое отображение просто смешивает свое входное состояние с максимально смешанным состоянием, оно сдвигает любую точку шара Блоха ближе к центру:



Мы знаем, что унитарные отображения описывают вращения шара Блоха, поэтому посредством композиции шумового отображения с унитарным любую точку шара Блоха можно перевести в любую другую точку, расположенную ближе к его центру (или находящуюся на том же расстоянии от центра):



Поэтому если ρ' расположена от центра сферы Блоха не дальше, чем ρ , то $\rho \geq \rho'$ принадлежит теории чистоты. На самом деле верно и обратное. Но вместо того чтобы доказывать это напрямую, мы можем дать характеристику этому отношению конвертируемости, пригодную для любой размерности. Мы воспользуемся следующим отношением предпорядка.

Определение 13.16. Для распределений вероятностей

$$\downarrow_p \leftrightarrow \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix} \quad \downarrow_q \leftrightarrow \begin{pmatrix} q^1 \\ \vdots \\ q^n \end{pmatrix}$$

говорят, что p мажорирует q , и пишут

$$\downarrow_p \geq \downarrow_q$$

если после расположения чисел в каждом распределении вероятностей в порядке убывания

$$p^1 \geq p^2 \geq \dots \geq p^n, \quad q^1 \geq q^2 \geq \dots \geq q^n$$

имеют место неравенства:

$$\left\{ \begin{array}{l} p^1 \geq q^1 \\ p^1 + p^2 \geq q^1 + q^2 \\ \vdots \\ p^1 + \dots + p^n \geq q^1 + \dots + q^n \end{array} \right. . \quad (13.5)$$

Легко проверить, что это отношение предпорядка, и называется оно *мажорирующим порядком*. Оно не является отношением частичного порядка, поскольку одинаковые элементы, расположенные в разном порядке, например точечные распределения, эквивалентны относительно мажоризации:

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \simeq \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \simeq \dots \simeq \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

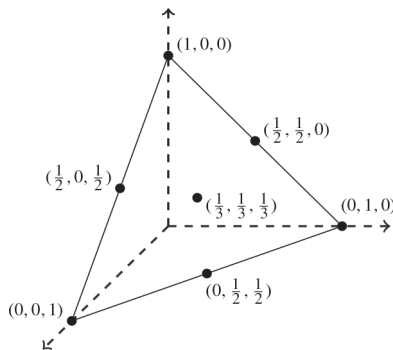
но, очевидно, не равны. Более того, даже если рассматривать распределения вероятностей с точностью до переупорядочения элементов, все равно полного порядка не получится, потому, например, что

$$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix} \not\asymp \begin{pmatrix} \frac{3}{4} \\ \frac{1}{8} \\ \frac{1}{8} \end{pmatrix} \quad \begin{pmatrix} \frac{3}{4} \\ \frac{1}{8} \\ \frac{1}{8} \end{pmatrix} \not\asymp \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \end{pmatrix}.$$

Упражнения 13.17. Распределения вероятностей

$$\triangleleft p \leftrightarrow \begin{pmatrix} p^1 \\ p^2 \\ p^3 \end{pmatrix}$$

можно представить точками треугольника, если рассматривать p_i как координаты:



Для произвольного распределения вероятностей p' изобразите область треугольника, содержащую все распределения вероятностей p , для которых:

$$\downarrow p \geq \downarrow p'$$

а также область, в которой

$$\downarrow p' \geq \downarrow p$$

Мажоризация дает предпорядок, который можно преобразовать в предупорядоченный моноид, взяв в качестве операции \otimes обычную параллельную композицию распределений вероятностей:

$$\downarrow p \quad \downarrow p'$$

Чтобы показать, что эта операция согласована с мажорирующим порядком, полезно дать альтернативную характеристику мажоризации. Эта характеристика ближе к духу ресурсных теорий в том смысле, что представляет мажоризацию как отношение конвертируемости – с помощью дважды стохастических отображений.

Определение 13.18. *Дважды стохастическими отображениями* называются классические процессы f (см. определение 8.11) такие, что

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \text{---} \circ \end{array} = \frac{1}{D'} \circ \downarrow \quad (13.6)$$

Или, эквивалентно, классические отображения f , для которых

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array} \quad \text{и} \quad \frac{D'}{D} \begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \end{array}$$

каузальны.

Предложение 13.19. Следующие утверждения эквивалентны:

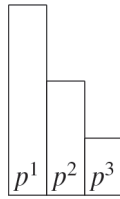
- p мажорирует q :

$$\downarrow p \geq \downarrow q$$

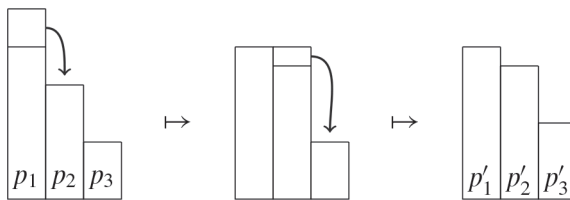
- существует дважды стохастическое отображение такое, что:

$$\begin{array}{c} \downarrow \\ \boxed{f} \\ \downarrow \\ \downarrow p \end{array} = \downarrow q$$

Доказательство (набросок). Мажорирующий предпорядок допускает интерпретацию с помощью «ханойской башни», где p_1, \dots, p_n представляют разные стопки:



Для реализации преобразования мы сначала «перемещаем» $p^1 - q^1$ с p^1 на p^2 , так что p^1 становится q^1 , затем перемещаем $(p^1 + p^2 - q^1) - q^2$ с $p^1 + p^2 - q^1$ на p^3 , так что p^2 становится q^2 , и так далее, например:



Чтобы это было возможно, необходимо выполнение условий:

$$p^1 - q^1 \geq 0, \quad p^1 + p^2 - q^1 - q^2 \geq 0, \quad \dots \quad p^1 + \dots + p^{n-1} - q^1 - \dots - q^{n-1} \geq 0,$$

которые после переноса всех q^i в правые части неравенств в точности совпадают с условиями мажоризации. Поскольку композиция дважды стохастических отображений также обладает свойством дважды стохастичности, достаточно показать, что «ханойские перемещения» можно реализовать дважды стохастическими отображениями, и наоборот. Оставляем это в качестве упражнения. □

Упражнение 13.20. Покажите, что если p мажорирует q , то существует дважды стохастическое отображение, переводящее p в q , для чего предъявите матрицы, реализующие «ханойские перемещения» в приведенном выше доказательстве. Указание: воспользуйтесь тем фактом, что матрица общего дважды стохастического отображения 2×2 имеет вид:

$$\begin{pmatrix} 1 - x & x \\ x & 1 - x \end{pmatrix},$$

где $0 \leq x \leq 1$. Обратно, покажите, что если f – дважды стохастическое отображение, а p – распределение вероятностей, то $p \geq f \circ p$ – мажорирующий предпорядок, определенный в (13.5).

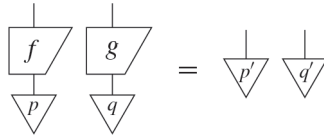
Таким образом, имеем следующее

Предложение 13.21. Мажоризация в сочетании с \otimes -композицией наделяет множество распределений вероятностей для классической системы структурой предупорядоченного моноида.

Доказательство. Если для дважды стохастических отображений f и g имеют место равенства



т. е. $p \geq p'$ и $q \geq q'$, то



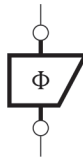
а т. к. $f \otimes g$ – очевидно, дважды стохастическое отображение, то $p \otimes q \geq p' \otimes q'$. \square

Унитарные квантовые отображения характеризуются тем, что они, как и их адьюнкты, каузальны, и дважды стохастические отображения обладают в точности тем же самым свойством. Тут просто напрашивается теорема, и действительно эти понятия взаимосвязаны посредством кодирования и измерения.

Теорема 13.22. Если классическое отображение f дважды стохастическое, то

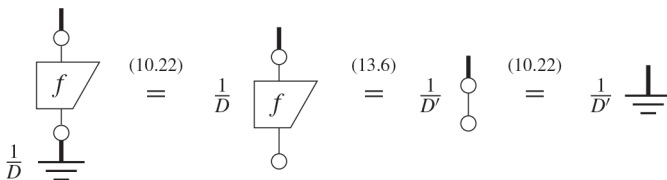


является унитарным квантовым отображением, а если квантовое отображение Φ унитарно, то



является дважды стохастическим (классическим) отображением.

Доказательство сразу следует из того, что измеритель и кодировщик каузальны, как и их адьюнкты. Например, унитарность (13.7) можно установить следующим образом:



\square

Замечание 13.23. Мы старались не отступать от стандартной терминологии, но, конечно, было бы лучше называть дважды стохастические отображения «уни-

тальными классическими отображениями», а унитарные квантовые отображения – «дважды каузальными квантовыми отображениями».

Это соответствие между унитарными квантовыми отображениями и дважды стохастическими отображениями транслируется в соответствие между конвертируемостью квантовых состояний и конвертируемостью распределений вероятностей. Мостом здесь служит спектральная теорема, которая в силу предложения 8.56 позволяет выразить квантовое состояние в терминах распределения вероятностей.

Лемма 13.24. Если ρ и ρ' – квантовые состояния с такими разложениями:

$$\begin{array}{c} \text{---} \\ \diagdown \\ \rho \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ \widehat{W} \\ \diagup \\ \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \diagdown \\ p \\ \diagup \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ \diagdown \\ \rho' \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ \widehat{W}' \\ \diagup \\ \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \diagdown \\ p' \\ \diagup \\ \text{---} \end{array} \quad (13.8)$$

где \widehat{W} и \widehat{W}' – унитарные отображения, а p и p' – распределения вероятностей, то следующие утверждения эквивалентны:

- существует унитарное квантовое отображение Φ такое, что

$$\begin{array}{c} \text{---} \\ \diagdown \\ \Phi \\ \diagup \\ \text{---} \\ \text{---} \\ \diagdown \\ \rho \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ \rho' \\ \diagup \\ \text{---} \end{array} \quad (13.9)$$

- существует дважды стохастическое отображение f такое, что:

$$\begin{array}{c} \text{---} \\ \diagdown \\ f \\ \diagup \\ \text{---} \\ \text{---} \\ \diagdown \\ p \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ p' \\ \diagup \\ \text{---} \end{array} \quad (13.10)$$

Доказательство. Предположим, что ρ и ρ' связаны унитарным квантовым отображением Φ , как в (13.9). Тогда в силу (13.8):

$$\begin{array}{c} \text{---} \\ \diagdown \\ \Phi \\ \diagup \\ \text{---} \\ \text{---} \\ \diagdown \\ \widehat{W} \\ \diagup \\ \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \diagdown \\ p \\ \diagup \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \diagdown \\ \widehat{W}' \\ \diagup \\ \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ \diagdown \\ p' \\ \diagup \\ \text{---} \end{array}$$

Теперь можно воспользоваться унитарностью, чтобы перенести \widehat{W}' в левую часть:

$$\begin{array}{c} \widehat{W}' \\ \Phi \\ \widehat{W} \\ \circ \\ \triangle p \end{array} = \begin{array}{c} \circ \\ \triangle p' \end{array} \quad (13.11)$$

Тогда измерение обеих частей дает

$$\begin{array}{c} \widehat{W}' \\ \Phi \\ \widehat{W} \\ \circ \\ \triangle p \end{array} \stackrel{(13.11)}{=} \begin{array}{c} \circ \\ \triangle p' \end{array} = \begin{array}{c} \triangle p' \end{array}$$

В силу предложения 13.22 отображение, примененное в левой части к p , является дважды стохастическим, поскольку все участвующие квантовые отображения унитарны. Обратное, из предположения о том, что p и p' связаны дважды стохастическим отображением, как в (13.10), следует, что:

$$\begin{array}{c} \widehat{W}' \\ f \\ \widehat{W} \\ \circ \\ \triangle \rho \end{array} \stackrel{(13.8)}{=} \begin{array}{c} \widehat{W}' \\ \circ \\ f \\ \circ \\ \widehat{W} \\ \widehat{W} \\ \circ \\ \triangle p \end{array} \stackrel{(10.8)}{=} \begin{array}{c} \widehat{W}' \\ \circ \\ f \\ \triangle p \end{array} = \begin{array}{c} \widehat{W}' \\ \circ \\ f \\ \triangle p \end{array} \stackrel{(13.10)}{=} \begin{array}{c} \widehat{W}' \\ \circ \\ \triangle p' \end{array} \stackrel{(13.8)}{=} \begin{array}{c} \triangle \rho' \end{array}$$

где, снова по предложению 13.22, квантовое отображение, примененное в левой части к ρ , унитарно. В более традиционной нотации распределение вероятностей p , связанное с состоянием ρ равенством (13.8), называется *спектром* ρ и обозначается

ется $\text{спес}(\rho)$ (см. определение 5.73). Совместно предложение 13.19 и лемма 13.24 дают следующую характеристику конвертируемости **чистоты** в терминах мажоризации.

Теорема 13.25. Отношение конвертируемости **чистоты** для состояний фиксированной квантовой системы произвольной размерности имеет вид:

$$\downarrow_{\rho} \succeq \downarrow_{\rho'} \iff \text{спес}(\rho) \geq \text{спес}(\rho')$$

где второй знак \geq – мажорирующий порядок.

13.2.2. Измерение (не)чистоты

Типичной мерой чистоты является *энтропия фон Неймана* квантового состояния, которая вычисляется, как описано ниже. Сначала воспользуемся следствием 6.68 для разложения ρ по ОНБ чистых состояний:

$$\downarrow_{\rho} = \sum_i p^i \downarrow_i \quad (13.12)$$

После этого можно вычислить энтропию фон Неймана:

$$S\left(\downarrow_{\rho}\right) := -\sum_i p^i \log_D(p^i)$$

где $\log_D(p^i)$ – логарифм p^i по некоторому фиксированному основанию D , в качестве которого обычно берется размерность одиночной системы, например 2 в случае кубитов. Так определенная энтропия изменяется от 0 для чистых состояний до 1 для максимально смешанного состояния.

Замечание 13.26. Для классического распределения вероятностей

$$\downarrow_p = \sum_i p^i \downarrow_i$$

величина

$$S\left(\downarrow_p\right) := -\sum_i p^i \log_D(p^i)$$

называется *энтропией Шеннона*. Поскольку любое квантовое состояние диагоналируемо, оно кодирует распределение вероятностей в некотором ОНБ. Тогда энтропия фон Неймана равна энтропии Шеннона этого закодированного распределения вероятностей.

Мы почти получили аддитивную меру в смысле определения 13.11. Действительно, оно удовлетворяет соотношению

$$S\left(\begin{array}{c} \downarrow \\ \rho_1 \end{array} \begin{array}{c} \downarrow \\ \rho_2 \end{array}\right) = S\left(\begin{array}{c} \downarrow \\ \rho_1 \end{array}\right) + S\left(\begin{array}{c} \downarrow \\ \rho_2 \end{array}\right) \quad (13.13)$$

что прямо следует из того факта, что

$$\log_D(p^i q^j) = \log_D(p^i) + \log_D(q^j).$$

Кроме того, для произвольных состояний двух систем имеем:

$$S\left(\begin{array}{c} \downarrow \\ \rho \end{array}\right) \leq S\left(\begin{array}{c} \overline{\overline{\overline{\downarrow}}} \\ \rho \end{array}\right) + S\left(\begin{array}{c} \downarrow \\ \overline{\overline{\overline{\rho}}} \end{array}\right)$$

причем равенство достигается тогда и только тогда, когда ρ разделено. Однако энтропия фон Неймана является не мерой чистоты, а мерой нечистоты, т. е. для предпорядка чистоты \geq мы имеем:

$$\begin{array}{c} \downarrow \\ \rho \end{array} \geq \begin{array}{c} \downarrow \\ \rho' \end{array} \implies S\left(\begin{array}{c} \downarrow \\ \rho \end{array}\right) \leq S\left(\begin{array}{c} \downarrow \\ \rho' \end{array}\right)$$

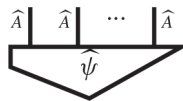
Замечание 13.27. С учетом того, что смешивание – синоним недостатка знания, это означает, что максимально смешанное состояние – «наименее информативное» состояние в противоположность чисто квантовым состояниям, которые «максимально информативны». Таким образом, налицо тесная связь между смешанностью/энтропией квантового состояния и его информационным содержанием. Изучение этого и смежных вопросов – важная часть *квантовой теории информации*.

13.3. ТЕОРИЯ ЗАПУТЫВАНИЯ

Понятие запутывания сильно отличается от чистоты и включает, по меньшей мере, две системы, но, пытаясь охарактеризовать отношение конвертируемости в ресурсной теории запутывания, мы встречаем многие из тех же ингредиентов.

Фактически мы будем изучать две разные ресурсные теории запутывания: одна примерно того же уровня детальности в части отношения конвертируемости, что теория чистоты, а другая гораздо грубее. Вторая теория настолько грубая, что для двух- и трехкубитовых состояний дает лишь конечное число эквивалентных ресурсов. Попутно мы увидим, что одно и то же слово «запутывание» может означать совершенно разные вещи.

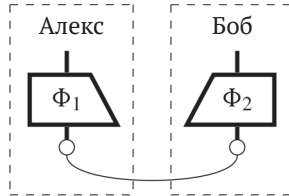
В этом разделе рассматриваются чистые состояния вида



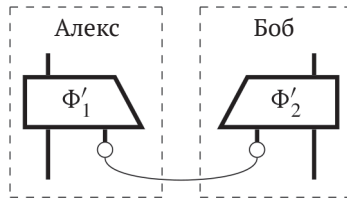
т. е. состояния, тип которых состоит из двух или более копий одной системы. Это не слишком принципиальное предположение, но оно немного упрощает изложение.

13.3.1. LOCC-запутывание

Если предмет нашего интереса – запутывание, то бесплатными будут процессы, не создающие нового запутывания. Мы уже видели, что распутанными являются состояния вида:



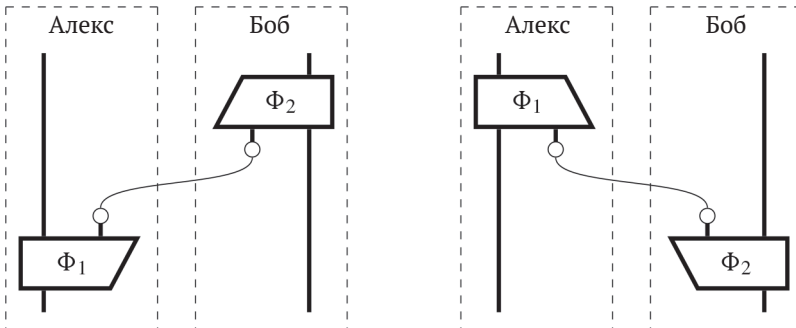
а с учетом обсуждения в разделе 8.3.5 может показаться, будто процессы, не создающие никакого запутывания, имеют вид:



(13.14)

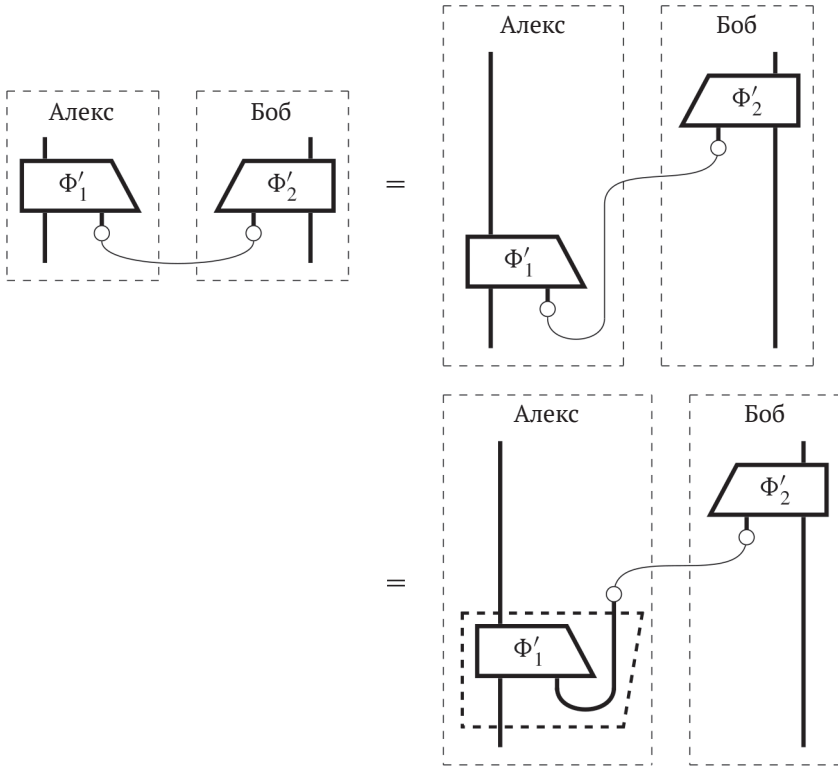
Однако в том обсуждении мы игнорировали каузальность по той простой причине, что состояния всегда каузальны с точностью до числа. Однако для процессов каузальность – нетривиальное требование. В контексте ресурсных теорий важно, что есть возможность практически реализовать «бесплатные» процессы, поскольку иначе в них не было ничего бесплатного! Некаузальные квантовые отображения могут быть реализованы только недетерминированно, и если нам не повезет, то вместо преобразования ресурса мы можем навсегда потерять его. Поэтому пока ограничимся одними каузальными процессами.

Как только на сцене появляется каузальность, мы должны различать следующие случаи: (i) Алекс и Боб разделяют классическую чашку; (ii) Алекс отправляет классические данные Бобу; (iii) Боб отправляет классические данные Алексу. Поэтому в дополнение к (13.14) необходимо рассматривать процессы вида:



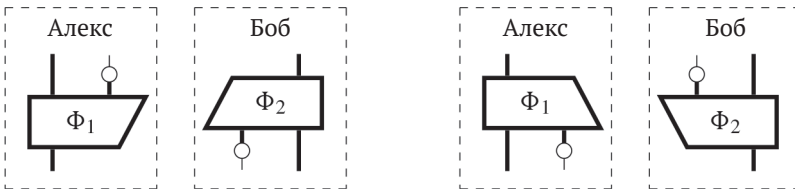
(13.15)

По счастью, начав рассматривать эти две формы, мы можем больше не думать о (13.14), потому что она является частным случаем отправки Алексом классических данных Бобу (или наоборот):



Квантовые процессы вида (13.15) и их композиции называются *LOCC-операциями*, поскольку их можно разложить на процессы двух базовых видов, а именно:

- локальные (каузальные) операции (Local Operations) :=



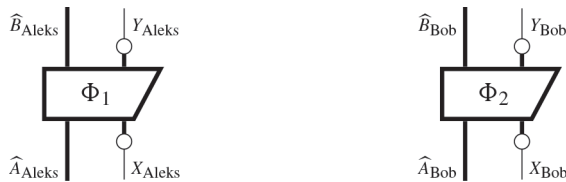
- классические коммуникации (Classical Communication) :=



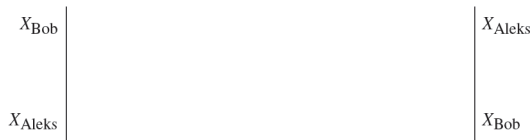
На протяжении всей книги мы рисовали пунктирные блоки с именами людей (или вымерших птиц), но ни разу не сказали формально, что это значит. На самом деле тут все просто. Мы можем объяснить суть дела, создав новую процессную теорию, назовем ее **квантовые процессы**², в которой имеются те же самые процессы, но две копии каждого (классического и квантового) типа, по одному для Алекса и Боба:

$$\hat{A} \rightsquigarrow (\hat{A}_{\text{Aleks}}, \hat{A}_{\text{Bob}}) \quad X \rightsquigarrow (X_{\text{Aleks}}, X_{\text{Bob}}).$$

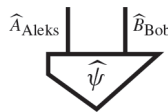
В этой новой процессной теории локальными операциями будут только квантовые процессы, соединяющие типы Алекса с типами Алекса, а типы Боба с типами Боба, например:



Далее, классическая коммуникация – это просто классический провод, один конец которого помечен типом Алекса, а другой – соответствующим типом Боба (или наоборот):



а **чистые квантовые состояния**² – множества состояний вида:

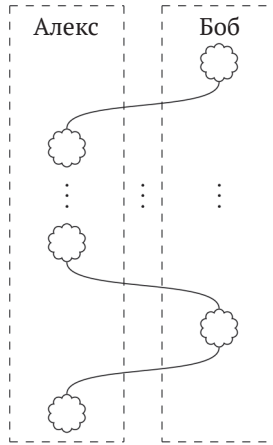


Разумеется, то же самое можно сделать для любого числа агентов.

Определение 13.28. Обозначим **лосс**² подтеорию теории **квантовых процессов**², полученную ограничением на процессы, соответствующие локальным операциям, классической коммуникации и их композициям. Тогда

$$\text{ЛОСС-запутывание}^2 := \text{чистые квантовые состояния}^2 / \text{лосс}^2.$$

Таким образом, общие квантовые процессы, не создающие запутывания, включают игру в пинг-понг классической коммуникацией между двумя агентами:



Как долго должна продолжаться эта игра, чтобы получить самый общий вид преобразований? К счастью, достаточно всего одного использования классической коммуникации, поскольку обе формы (13.15) на самом деле взаимозаменяемы. Чтобы убедиться в этом, мы сначала заметим, что можно поменять местами роли двух систем двухкомпонентного состояния посредством унитарных отображений.

Лемма 13.29. Для любого чистого двухкомпонентного состояния $\hat{\psi}$ существуют унитарные отображения \hat{U} и \hat{V} , которые переставляют местами две системы:

$$\begin{array}{c} \hat{U} \quad \hat{V} \\ \hat{\psi} \end{array} = \begin{array}{c} \text{swap} \\ \hat{\psi} \end{array} \quad (13.16)$$

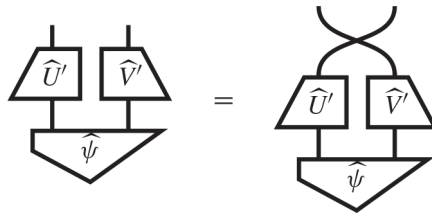
Доказательство. Применение сингулярного разложения из упражнения 8.50 (которое опирается на тот факт, что обе системы одинаковы) к ψ дает:

$$\begin{array}{c} \psi \end{array} = \begin{array}{c} U' \quad V' \\ \circ \\ q \end{array}$$

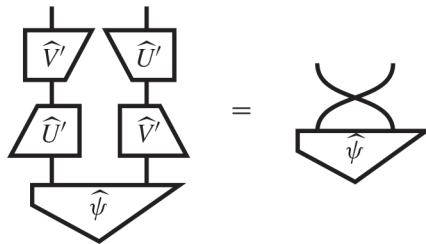
для унитарных отображений U' и V' . Тогда

$$\begin{array}{c} \hat{U}' \quad \hat{V}' \\ \psi \end{array} = \begin{array}{c} \hat{U}' \quad \hat{V}' \\ U' \quad V' \\ \circ \\ q \end{array} = \begin{array}{c} \text{crossing} \\ q \end{array}$$

Поскольку правая часть инвариантна относительно перекмутации, имеем:



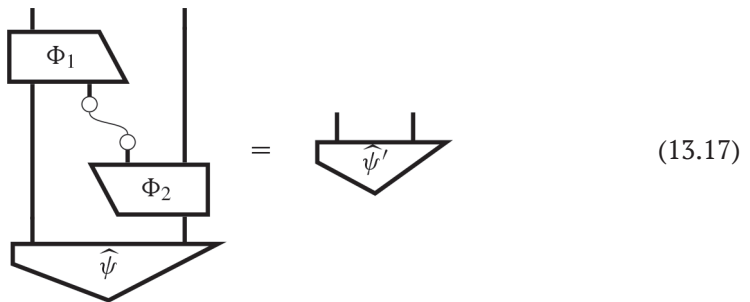
Перенос всех унитарных отображений в левую часть завершает доказательство:



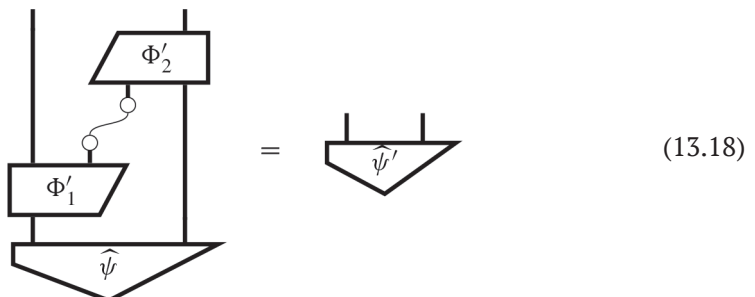
□

Важно, что для реализации этой перекмутации нам нужны только локальные операции. В качестве следствия такой «локальной перекмутации» получаем следующее

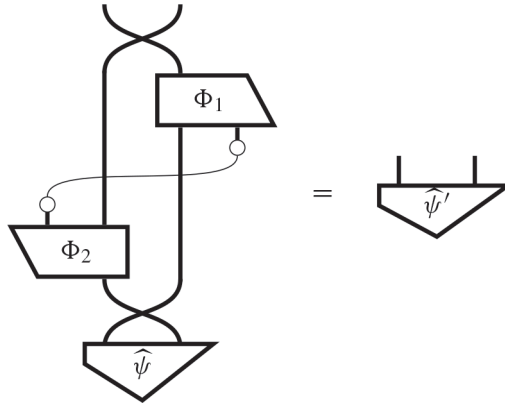
Предложение 13.30. Существуют Φ_1 и Φ_2 такие, что



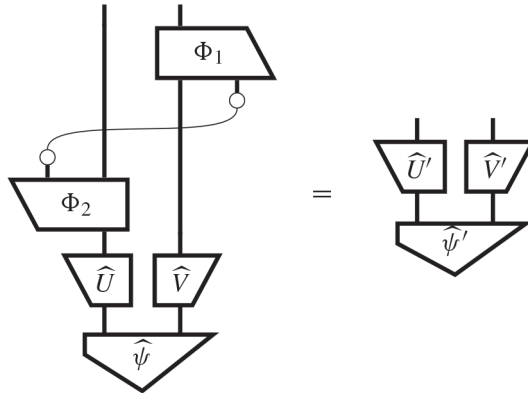
тогда и только тогда, когда существуют Φ'_1 и Φ'_2 такие, что



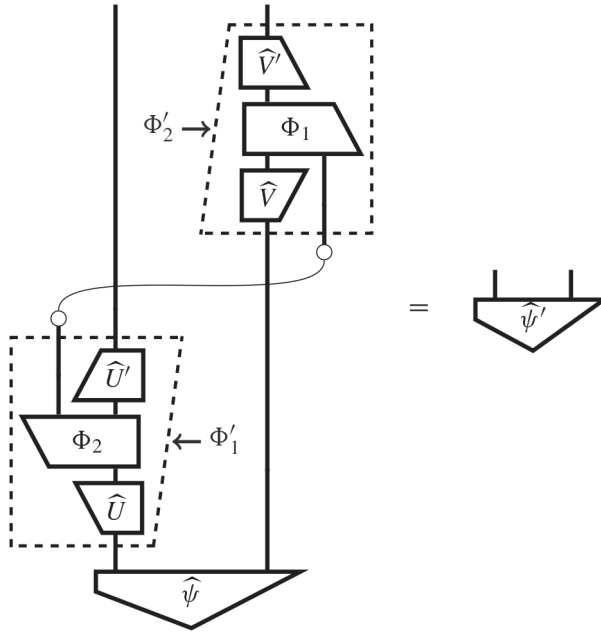
Доказательство. Пусть Φ_1 и Φ_2 удовлетворяют равенству (13.17). Деформация левой части дает:



Далее, поскольку $\hat{\psi}$ и $\hat{\psi}'$ – чистые двухкомпонентные состояния, мы можем применить лемму 13.29 для устранения обеих перекруток:

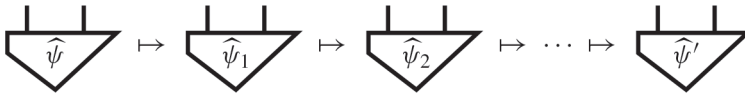


Затем, перенося унитарные отображения в левую часть:

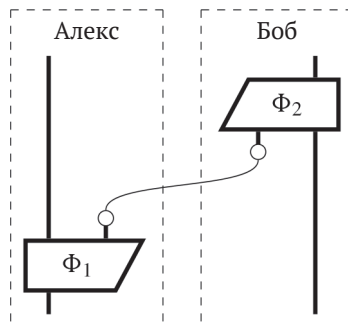


получаем процессы Φ'_1 и Φ'_2 , удовлетворяющие (13.18). Обратное доказывается симметрично. \square

Для простоты предположим, что имеется протокол LOCC, каждый шаг которого детерминированно дает чистое состояние:

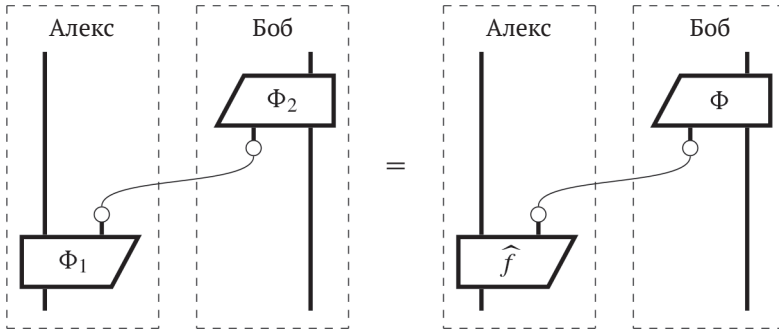


Тогда он состоит из \circ -композиции процессов, удовлетворяющих равенству (13.17) или (13.18). Следовательно, применяя предложение 13.30, мы можем сделать так, что все классические провода будут идти от Алекса к Бобу, и собрать их в один классический провод. Стало быть, мы получаем процесс вида:

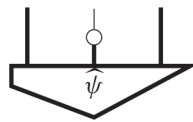


(13.19)

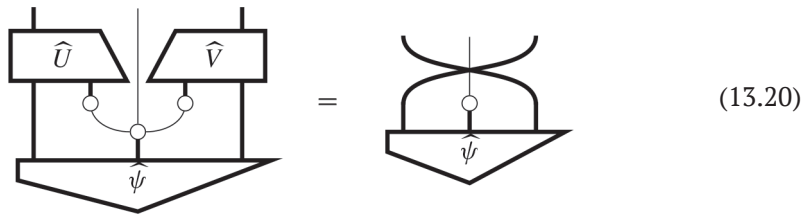
Упражнение 13.31. Покажите, что (возможно, уменьшив размер классической системы), можно дополнительно предположить, что процесс Φ_1 в (13.19) чистый. То есть для любых (каузальных) Φ_1 и Φ_2 существуют (каузальные) \hat{f} и Φ такие, что:



Упражнение* 13.32. Покажите, что любой протокол LOCC можно записать в виде (13.19), не предполагая, что каждый шаг детерминированно дает чистое состояние. Указание: сначала очистите процессы Алекса и Боба, так чтобы каждый шаг давал «недетерминированное» чистое состояние:

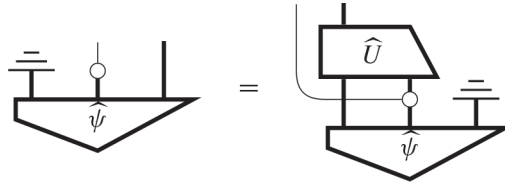


и воспользуйтесь следующим обобщением леммы 13.29: для любого недетерминированного состояния $\hat{\psi}$ существуют управляемые унитарные отображения \hat{U}, \hat{V} такие, что:

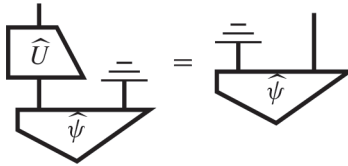


Доказывая характеристику отношения конвертируемости для этой ресурсной теории, мы будем пользоваться следующей леммой, которая говорит, как связаны редуцированные состояния при отбрасывании разных систем.

Лемма 13.33. Для любого недетерминированного двухкомпонентного состояния $\hat{\psi}$ (т. е. чистого двухкомпонентного состояния с классическим выходом) существует управляемое унитарное отображение \hat{U} такое, что два его редуцированных состояния связаны следующим образом:

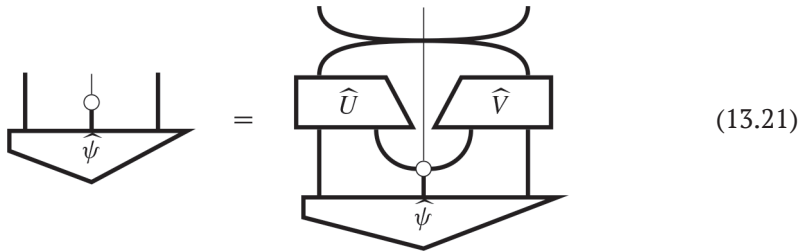


В частном случае, когда классическая система тривиальна, это равенство принимает вид:

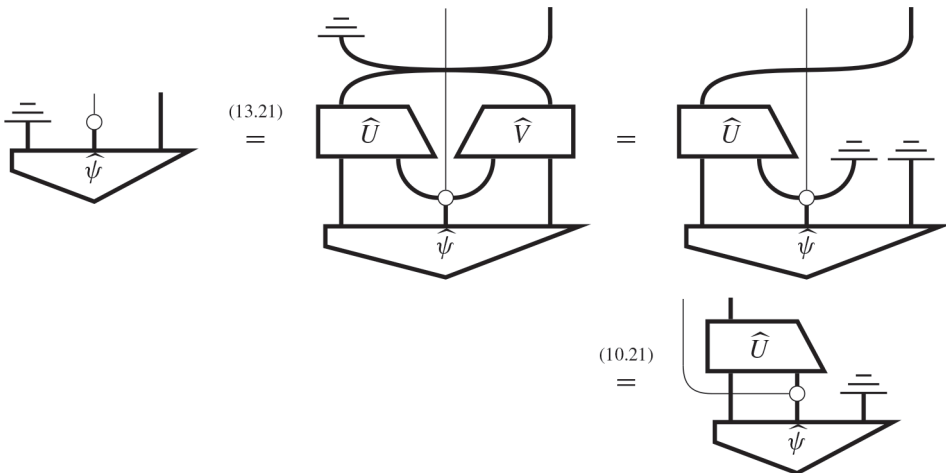


для некоторого унитарного отображения \hat{U} .

Доказательство. Мы можем переписать равенство (13.20) из упражнения* 13.32 в виде:



Тогда, пользуясь каузальностью управляемого унитарного отображения \hat{V} (на втором шаге), получаем:



□

Нам также понадобится следующий факт.

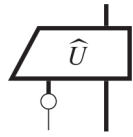
Лемма 13.34. Любая смесь унитарных отображений



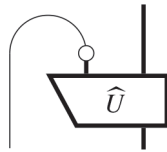
$$(13.22)$$

является унитарным квантовым отображением.


Доказательство. Из равенства (10.45) следует, что для любого управляемого унитарного отображения



его «управляемое обратное отображение»

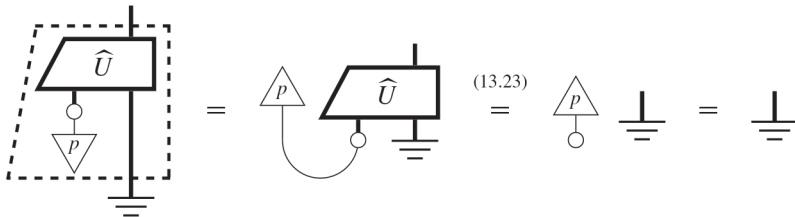


также является управляемым и унитарным и, в частности, оно каузальное:



$$(13.23)$$

Применение адьюнкции к этому равенству дает унитарность (13.22):



□

Теперь у нас достаточно ингредиентов, чтобы охарактеризовать отношение конвертируемости для **ЛОСС-запутывания**², которое очень похоже на такое отношение для **чистоты**.

Теорема 13.35. Если двухкомпонентное состояние $\hat{\psi}$ можно преобразовать в двухкомпонентное состояние $\hat{\psi}'$ в теории **ЛОСС-запутывания**², то существует

унитарное квантовое отображение Ψ , которое преобразует редуцированное состояние $\hat{\psi}'$ в редуцированное состояние $\hat{\psi}$:

$$(13.24)$$

Поэтому отношение конвертируемости в теории **ЛОСС-запутывания**² для двухкомпонентных состояний пары одинаковых фиксированных квантовых систем имеет вид:

$$\hat{\psi} \succeq \hat{\psi}' \implies \text{spec} \left(\hat{\psi}' \right) \succeq \text{spec} \left(\hat{\psi} \right)$$

где второй символ \succeq обозначает мажорирующий предпорядок.

Доказательство. Предположим, что $\hat{\psi} \succeq \hat{\psi}'$. Тогда в силу предложения 13.30 и упражнения 13.31 существуют квантовые процессы \hat{f} и Φ такие, что:

$$(13.25)$$

Начав с правой части (13.24), мы хотим прийти к левой части. Для этого сосредоточимся сначала на локальной операции \hat{f} в левой части (13.25). Применение \hat{f} к $\hat{\psi}$ дает недетерминированное чистое состояние, поэтому, по лемме 13.33, существует управляемое унитарное отображение такое, что:

Удаление классического выхода в обеих частях дает равенство:

$$\text{Diagram (13.26)} \quad (13.26)$$

где мы воспользовались каузальностью, чтобы исключить \hat{f} в левой части. Далее, в силу второй части леммы 13.33 существует унитарное отображение \hat{V} такое, что:

$$\text{Diagram (13.27)} \quad (13.27)$$

Объединяя равенства (13.26) и (13.27) и перенося \hat{V} в правую часть, получаем:

$$\text{Diagram (13.28)} \quad (13.28)$$

Теперь немного модифицируем равенство (13.25), чтобы можно было подставить его в правую часть (13.28). Из предложения 8.59 мы знаем, что если удаление классической системы дает чистое состояние, то классическая система разделяется. Применяя это к равенству (13.25), которое можно переписать в виде

$$\text{Diagram}$$

получаем следующее разделение:

(13.29)

для некоторого распределения вероятностей p . В силу каузальности Φ имеем также:

(13.30)

Отсюда:

(13.31)

Это равенство можно подставить в (13.28), что дает:

В терминологии определения 13.7 это означает ненулевой курс конвертации из $\hat{\psi}$ в $\hat{\psi}'$:

$$r(\hat{\psi} \geq \hat{\psi}') > 0.$$

Поскольку, по теореме 6.94, любое квантовое отображение можно реализовать как ветвь (каузального) квантового процесса, переход к этой, более либеральной разновидности локальной операции эквивалентен принятию в качестве локальных операций любых КК-отображений, а не только каузальных. Эти новые «бесплатные» процессы называются *SLOCC-операциями*, т. к. допускают разложение на базовые процессы двух видов:

- стохастические локальные операции (т. е. потенциально некаузальные КК-отображения) и
- классические коммуникации.

Определение 13.38. Пусть slocc^2 – подтеория теории **квантовых отображений**², полученная ограничением на процессы, реализующие стохастические локальные операции, классические коммуникации и композиции тех и других. Тогда

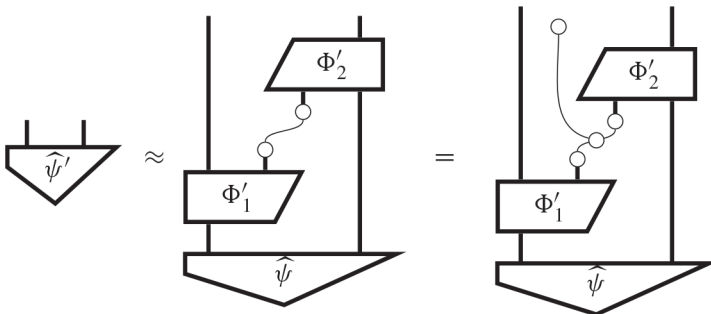
$$\text{SLOCC-запутывание}_2 := \text{чистые квантовые состояния}_2 / \text{slocc}^2.$$

Несмотря на внешнее сходство с теорией **ЛОСС-запутывания**², с этой ресурсной теорией работать гораздо проще. В частности, классическая коммуникация теперь становится нерелевантной.

Теорема 13.39. В теории **SLOCC-запутывания**² двухкомпонентное состояние $\hat{\psi}$ можно преобразовать в двухкомпонентное состояние $\hat{\psi}'$ тогда и только тогда, когда существуют квантовые отображения Φ_1 и Φ_2 такие, что:

(13.32)

Доказательство. Предположим, что $\hat{\psi} \geq \hat{\psi}'$; тогда существуют КК-отображения Φ'_1 и Φ'_2 такие, что:



поэтому в силу предложения 8.59 имеем:

(13.33)

для некоторого p . Поскольку p – (каузальное) распределение вероятностей, должен существовать ОНБ-эффект i такой, что

(13.34)


Отсюда

Полагая


получаем равенство (13.32) (с точностью до подходящим образом выбранного числа). □

Упражнение 13.40. Используя аналогичную технику, покажите, что в качестве локальных операций достаточно рассматривать только чистые квантовые отображения:

Алекс



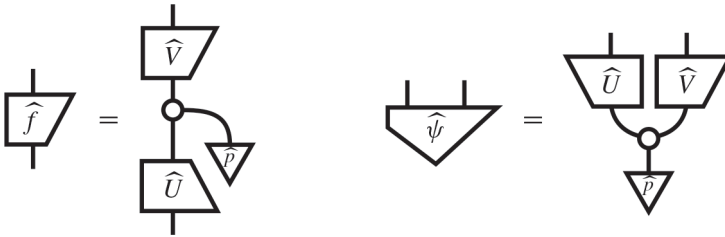
Боб



(13.35)

Чтобы охарактеризовать конвертируемость в теории **SLOCC-запутывания**², мы воспользуемся стандартным понятием из линейной алгебры, адаптировав его к чистым квантовым отображениям.

Определение 13.41. Рангом чистого квантового отображения или двухкомпонентного состояния, представленных в терминах сингулярного разложения:



который записывается соответственно

$$\text{rank} \left(\begin{array}{|c|} \hline \hat{f} \\ \hline \end{array} \right) \qquad \text{rank} \left(\begin{array}{|c|} \hline \hat{\psi} \\ \hline \end{array} \right)$$

называется количество ненулевых элементов матрицы p :

$$\begin{array}{|c|} \hline p \\ \hline \end{array} \leftrightarrow \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix}$$

Замечание 13.42. Как «боковое» сингулярное разложение двухкомпонентного состояния часто называют разложением Шмидта, так для «бокового» ранга двухкомпонентного состояния в литературе часто встречается название *ранг Шмидта*.

Крайние случаи ранга нам уже встречались.

Упражнение 13.43. Сначала покажите, что «максимальный ранг» – то же самое, что «невыврожденность» в смысле определения 4.75, что крышка имеет максимальный ранг и что «ранг 1» – то же самое, что разделимость. Затем покажите, что отношение конвертируемости \geq для **SLOCC-запутывания**² описывается эквивалентностью:

$$\begin{array}{|c|} \hline \hat{\psi} \\ \hline \end{array} \geq \begin{array}{|c|} \hline \hat{\psi}' \\ \hline \end{array} \iff \text{rank} \left(\begin{array}{|c|} \hline \hat{\psi} \\ \hline \end{array} \right) \geq \text{rank} \left(\begin{array}{|c|} \hline \hat{\psi}' \\ \hline \end{array} \right)$$

При этом можете использовать тот факт, что для чистых квантовых отображений \hat{f} и \hat{g}

$$\text{rank} \left(\begin{array}{c} \text{---} \\ | \\ \hat{f} \\ | \\ \text{---} \end{array} \right) \geq \text{rank} \left(\begin{array}{c} \hat{g} \\ \hat{f} \end{array} \right) \quad \text{rank} \left(\begin{array}{c} \text{---} \\ | \\ \hat{g} \\ | \\ \text{---} \end{array} \right) \geq \text{rank} \left(\begin{array}{c} \hat{g} \\ \hat{f} \end{array} \right)$$

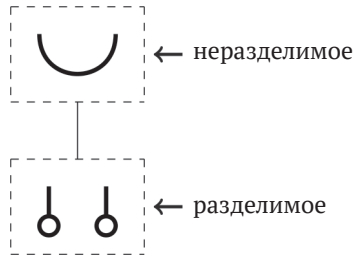
Таким образом, два двухкомпонентных состояния эквивалентны (см. определение 13.4) тогда и только тогда, когда их ранги равны. Так как любое двухкомпонентное состояние кубита должно иметь ранг 1 или 2, например:

$$\text{rank} \left(\begin{array}{c} \text{---} \\ \cup \\ \text{---} \end{array} \right) = 2 \quad \text{rank} \left(\begin{array}{c} \text{---} \\ | \\ \circ \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ | \\ \circ \\ | \\ \text{---} \end{array} \right) = 1$$

существует только два класса эквивалентности: класс состояний, эквивалентных состоянию Белла, и класс состояний, эквивалентных разделимому состоянию. Кроме того, любое разделимое состояние можно получить из неразделимого посредством SLOCC-операций, поэтому:

$$\begin{array}{c} \text{---} \\ \cup \\ \text{---} \end{array} \geq \begin{array}{c} \text{---} \\ | \\ \circ \\ | \\ \text{---} \end{array} \quad \begin{array}{c} \text{---} \\ | \\ \circ \\ | \\ \text{---} \end{array}$$

Поскольку количество классов эквивалентности конечно, это отношение конвертируемости можно изобразить в виде диаграммы конвертируемости:



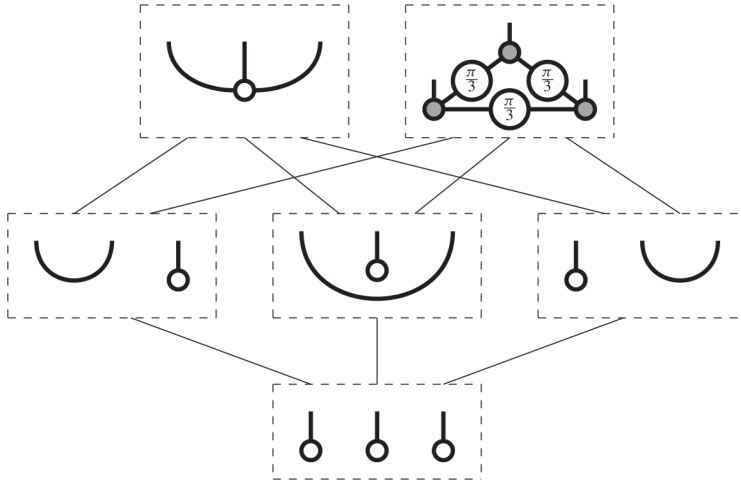
где блоки представляют классы эквивалентности, а идущие вниз ребра – тот факт, что один класс допускает преобразование в другой.

Если LOCC-конвертируемость улавливает количественные различия в запутывании, то SLOCC-конвертируемость гораздо лучше улавливает «качественные» различия, например «разделимое» и «неразделимое». Как мы только что видели, в двухкомпонентном случае это индуцирует очень простое полное упорядочение на классах SLOCC-эквивалентности, обусловленное рангом. Таким образом, для всех двухкомпонентных состояний $\hat{\psi}$ и $\hat{\psi}'$ имеет место одно из двух:

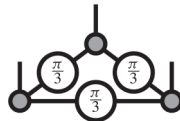
$$\begin{array}{c} \text{---} \\ | \\ \hat{\psi} \\ | \\ \text{---} \end{array} \geq \begin{array}{c} \text{---} \\ | \\ \hat{\psi}' \\ | \\ \text{---} \end{array} \quad \text{или} \quad \begin{array}{c} \text{---} \\ | \\ \hat{\psi}' \\ | \\ \text{---} \end{array} \geq \begin{array}{c} \text{---} \\ | \\ \hat{\psi} \\ | \\ \text{---} \end{array}$$

Однако стоит выйти за рамки двух систем, как ситуация меняется. Появляются состояния, которые являются SLOCC-максимальными, но при этом неэквивалентными.

Теорема 13.44. Отношение конвертируемости для SLOCC-запутывания³, ограниченное на кубиты, описывается следующим образом:



Ключевая особенность этой диаграммы конвертируемости состоит в том, что на верхнем уровне находятся два несравнимых класса, представителями которых являются уже встречавшееся нам ГХЦ-состояние и новое *W-состояние*:



Упражнение 13.45. Покажите, что

$$\begin{array}{c} \text{Spider} \\ \text{with } \pi/3 \text{ gates} \end{array} \approx \begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} + \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 1 \end{array} \begin{array}{c} \downarrow \\ 0 \end{array}$$

Качественные различия в свойствах запутывания ГХЦ-состояния и *W-состояния* несколько тоньше, чем, скажем, разделимое/неразделимое. Например, если в ГХЦ-состоянии отбросить одну систему, то оставшиеся две системы распутываются:

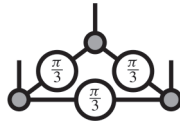
$$\begin{array}{c} \text{Arc with dot} \\ \text{with double line} \end{array} = \begin{array}{c} \text{Arc with dot} \\ \text{with single line} \end{array} = \begin{array}{c} \text{Two dots} \\ \text{with arc} \end{array}$$

тогда как для *W-состояния* это не так. В следующем разделе мы увидим еще более разительное между «ГХЦ-пауками» и этим новым видом «арахнид».

Замечание 13.46. Если число кубитов больше трех, то количество классов SLOCC-эквивалентности перестает быть конечным. Свободных параметров состояния в случае четырех и более систем слишком много, чтобы их можно было взаимно уничтожить посредством SLOCC-операций. Можно продолжить изучение параметризованных классов SLOCC-эквивалентности (или «суперклассов SLOCC») для четырех и более систем, но мы очень далеки от их полного понимания.

13.3.3. Взрывающиеся пауки

W -состояния выглядят не как пауки, а как паучьи оргии:



И что из этого получается? Это не может быть обыкновенный паук из-за следующего факта.

Предложение 13.47. Для любых пауков в двумерной системе состояние



SLOCC-эквивалентно ГНЦ-состоянию.

Доказательство. Из теоремы 8.41 следует, что любой паук соответствует некоторому ОНБ. В частности:

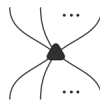
$$\text{Spider with black dot} = \begin{matrix} \downarrow & \downarrow & \downarrow \\ 0 & 0 & 0 \end{matrix} + \begin{matrix} \downarrow & \downarrow & \downarrow \\ 1 & 1 & 1 \end{matrix}$$

Тогда если унитарное отображение U переводит \bullet -ОНБ в \circ -ОНБ, то имеем:

$$\begin{matrix} \hat{U} & \hat{U} & \hat{U} \\ \downarrow & \downarrow & \downarrow \\ \downarrow & \downarrow & \downarrow \end{matrix} = \text{Spider with white dot}$$

□

Поскольку мы не можем получить W -состояние из обычных пауков, то получим его с помощью другого вида арахнид. А именно определим семейство



так что

$$\text{Spider with black dot} \approx \text{Spider-like entangled state with pi/3 gates}$$

Следуя упражнению 13.45, положим:

$$\text{cup} := \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} + \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array}$$

Это легко обобщить с целью порождения n -компонентных состояний. Сначала рассмотрим все битовые строки длины n , содержащие один 0:

$$C_n := \{011\dots 1, 101\dots 1, \dots, 11\dots 10\}.$$

Затем для образования n -компонентного состояния просуммируем по всем битовым строкам $\vec{i} \in C_n$:

$$\text{cup} \dots := \sum_{\vec{i} \in C_n} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_1 \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_2 \dots \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_n$$

Аналогично можно получить входные ноги; нужна лишь небольшая модификация: входные ONB-состояния следует инвертировать. То есть для $\vec{i} := 1 - i$ полагаем:

$$\text{spider} := \sum_{\vec{i} \in C_{m+n}} \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_1 \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_2 \dots \begin{array}{|c|} \hline \downarrow \\ \hline \end{array} i_m \begin{array}{|c|} \hline \uparrow \\ \hline \end{array} i_{m+1} \begin{array}{|c|} \hline \uparrow \\ \hline \end{array} i_{m+2} \dots \begin{array}{|c|} \hline \uparrow \\ \hline \end{array} i_{m+n} \tag{13.36}$$

Эти новые арахниды ведут себя во многом как пауки, только вот слишком сильно любят друг друга. Например, поведение стандартного паука подчиняется уравнениям перекоммутации ног:

$$\text{spider} = \text{spider} = \text{spider} \tag{13.37}$$

Кроме того, если новые арахниды соединены одной ногой, то они сливаются ожидаемым способом:

$$\text{spider} = \text{spider} \tag{13.38}$$

откуда можно вывести большинство обычных свойств пауков. Например, как и пауки, новые существа дают нам чашки и крышки:

$$\text{Loop with two triangles} = \text{Wire with one triangle} = \text{Wire} \quad (13.39)$$

Но если эти арахниды дрыгают двумя (или более) ногами, то перевозбуждаются и взрываются:

$$\text{Node with lines and triangles} \approx \text{Grid of triangles} \quad (13.40)$$

два провода

оставляя грудку дымящихся обрубков ног:

$$\text{Triangle on wire} \approx \text{Downward triangle with line} \quad \text{Two triangles on wire} \approx \text{Upward triangle with line}$$

Определение 13.48. Семейство \blacktriangle линейных отображений называется семейством *антипауков*, если оно удовлетворяет равенствам (13.37), (13.38) и (13.40).

Упражнение 13.49. Покажите, что (13.36) действительно определяет семейство антипауков.

Мы можем выделить ключевое различие между пауками и антипауками, рассмотрев упрощенный вариант слияния пауков и сравнив его с уравнением «антислияния» (13.40), а именно посмотрев, что происходит с одной «петлей»:

$$\text{Loop with white circles} = \text{Wire} \quad \text{Loop with black triangles} \approx \text{Stack of triangles} \quad (13.41)$$

Если в случае пауков мы получаем простой провод, то для антипауков все наоборот: они разделяются. Хотя разделяются они весьма своеобразным способом, но все равно имеет место разделение, и этого достаточно.

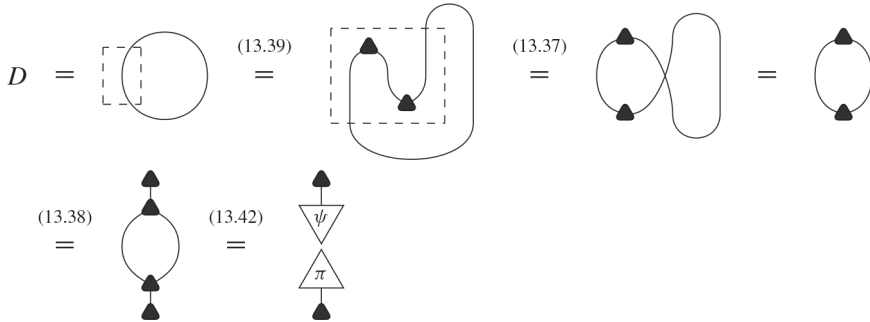
Предложение 13.50. Семейство линейных отображений, удовлетворяющее равенствам (13.37) и (13.38), является семейством антипауков тогда и только тогда, когда

$$\text{Loop with black triangles} = \text{Stack of } \psi \text{ and } \pi \text{ triangles} \quad (13.42)$$

Доказательство. Очевидно, что антипауки удовлетворяют (13.42), если положить:



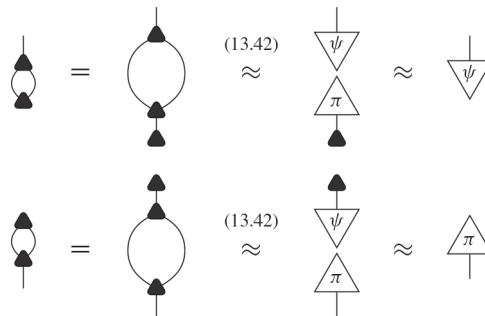
Обратно, предположим, что (13.42) истинно. Тогда имеем:



Поскольку левая часть не равна нулю, оба числа в правой части также должны быть отличны от нуля, т. е.



Теперь можно узнать, чему равны ψ и π с точностью до числа:



Подставляя в (13.42), получаем:



Отсюда уже нетрудно показать, что имеет место (13.40). Оставляем это в качестве упражнения для читателя.

Упражнение* 13.51. Покажите, что ни в каком антипауке в нетривиальной ($D > 1$) системе не может существовать «двойных петель»:

$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = 0 \tag{13.44}$$

(Указание: сначала вычислите число, возникающее в равенстве (13.43).)

Как и в случае обычных пауков и ГХЦ-состояния, уравнения антипауков полностью характеризуют класс SLOCC-эквивалентности W -состояния.

Теорема 13.52. Пусть \blacktriangle – семейство антипауков в двумерной системе. Тогда



SLOCC-эквивалентно W -состоянию.

Доказательство. Сначала заметим, что

$$\begin{array}{c} | \\ \bullet \end{array} \approx \begin{array}{c} | \\ \bullet \\ \bullet \end{array} \tag{13.45}$$

поскольку в противном случае простой провод разделяется:

$$\begin{array}{c} | \\ \bullet \end{array} \stackrel{(13.38)}{=} \begin{array}{c} | \\ \bullet \\ \bullet \end{array} \approx \begin{array}{c} | \\ \bullet \\ \bullet \end{array} \stackrel{(13.38)}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \stackrel{(13.40)}{\approx} \begin{array}{c} \bullet \\ | \\ \bullet \\ \bullet \end{array}$$

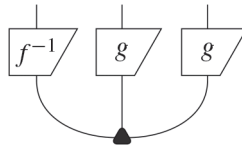
Следовательно, два состояния (13.45) образуют базис двумерной системы, поэтому можно определить обратимое линейное отображение f такое, что:

$$\begin{array}{c} \square \\ f \\ \square \end{array} \begin{array}{c} \triangle \\ 0 \\ \triangle \end{array} \mapsto \begin{array}{c} \bullet \\ | \\ \bullet \\ \bullet \end{array}, \quad \begin{array}{c} \square \\ f \\ \square \end{array} \begin{array}{c} \triangle \\ 1 \\ \triangle \end{array} \mapsto \begin{array}{c} | \\ \bullet \end{array}$$

Если дополнительно положить

$$\begin{array}{c} \square \\ g \\ \square \end{array} := \begin{array}{c} \bullet \\ | \\ \square \\ f \\ \square \end{array}$$

то, подключая эффекты \circ -ОНБ, легко проверить, что



действительно дает W -состояние. □

Резюмируем: мы снова обнаруживаем, что различие между «разделимое» и «неразделимое» играет ключевую роль – на этот раз оно подчеркивает качественную разницу между двумя SLOCC-максимальными состояниями трех кубитов.

13.3.4. Назад к основам: арифметика

Теорема 13.44 утверждает, что существует только два вида неразделимых состояний систем с тремя кубитами, т. е. с точностью до локальных операций любое состояние эквивалентно одному из следующих двух:



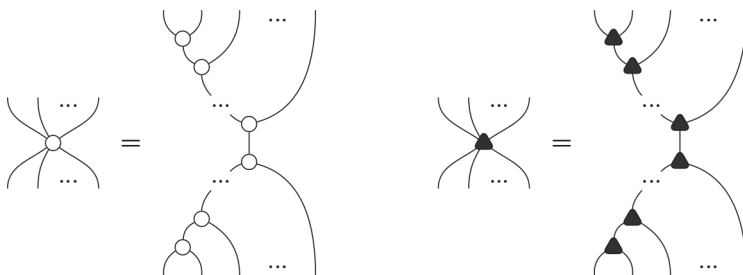
Согнув некоторые провода, мы могли бы с тем же успехом сказать, что любое неразделимое линейное отображение двух кубитов в один с точностью до локальных операций должно быть эквивалентно одному из двух:



или что любое отображение «один в два» должно быть эквивалентно одному из двух:

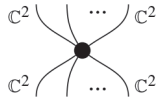


Вследствие слияния (анти)пауков семейство (анти)пауков в целом определяется следующими трехногими пауками:

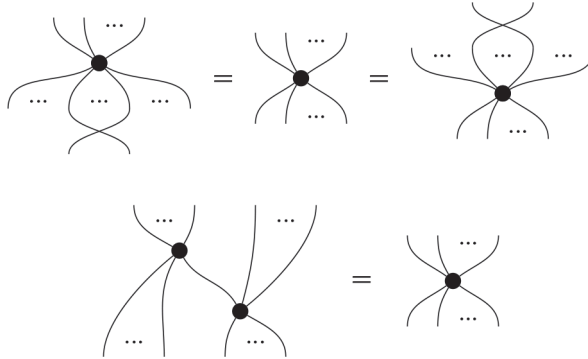


поэтому можно было бы ожидать, что пауки также сведутся к этим двум случаям с точностью до локальных линейных отображений. Так оно и есть.

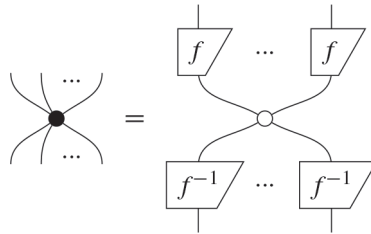
Теорема 13.53. Обозначим



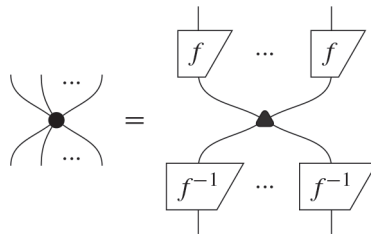
семейство линейных отображений, удовлетворяющих условиям



Тогда \bullet должно быть *изоморфно* либо \circ , либо \blacktriangle . То есть существует изоморфизм (обратимое линейное отображение) f такой, что имеет место либо:



либо



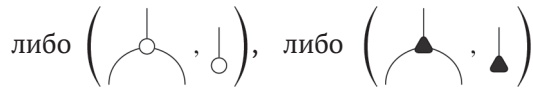
Поэтому пауки и антипауки, строго говоря, являются единственными вариантами семейства «сливающихся» операций над кубитами. На самом деле даже без предположения о наличии целого семейства пауков любая пара отображений



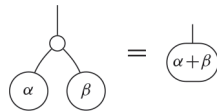
удовлетворяющих условиям



должна быть изоморфна



Но что собой представляют операции \circ и \blacktriangle ? Что они делают? Начнем с того, что мы уже знаем о пауках: как они взаимодействуют с фазовыми состояниями:



Фазовое состояние «кодирует» комплексное число $e^{i\alpha}$, и когда пара фазовых состояний встречается с \circ -пауком, эти числа перемножаются:

$$\begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix} \star \begin{pmatrix} 1 \\ e^{i\beta} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i(\alpha+\beta)} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i\alpha} \cdot e^{i\beta} \end{pmatrix}.$$

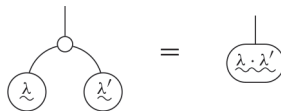
На самом деле в разделе 8.2.2.4 мы видели, что это остается справедливым, даже если заменить комплексные числа вида $e^{i\alpha}$ произвольными комплексными числами:

$$\begin{pmatrix} 1 \\ \lambda \end{pmatrix} \star \begin{pmatrix} 1 \\ \lambda' \end{pmatrix} = \begin{pmatrix} 1 \\ \lambda \cdot \lambda' \end{pmatrix}.$$

то есть положив

$$\begin{pmatrix} 1 \\ \lambda \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 \\ \lambda \end{pmatrix}$$

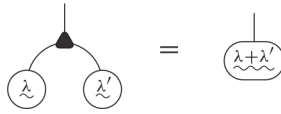
мы будем иметь:



Поскольку эти «обобщенные фазы» образуют базис, мы тем самым полностью охарактеризовали \circ -сопоставление для кубитов. Стало быть,

кубитовые пауки соответствуют умножению.

Если подключить те же самые обобщенные фазовые состояния к \blacktriangle -сопоставлению, то получится нечто удивительное:

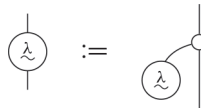


Следовательно:

кубитовые антипауки соответствуют сложению.

Если у нас есть два числа и мы хотим получить из них одно, то первое, что приходит на ум, – сложение и умножение. Удивительно, но при обращении с кубитами ничего другого и не дано!

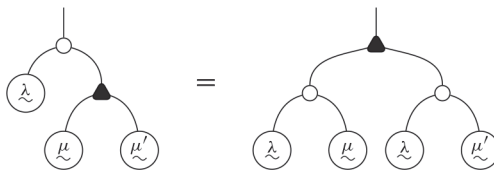
Начав отсюда, мы можем поиграть в игру, аналогичную ZX-исчислению, и начать строить ряд графических правил, регулирующих взаимодействие \circ -паука и \blacktriangle -антипаука. Например, полагая



мы получаем обобщенные фазовые вентили. Затем можно использовать правило копирования



отражающее тот факт, что «умножение» дистрибутивно относительно «сложения»:



– правило, которое нам хорошо известно в символической записи:

$$\lambda \cdot (\mu + \mu') = \lambda \cdot \mu + \lambda \cdot \mu'.$$

Имея только \circ/\blacktriangle и обычную фазу π :

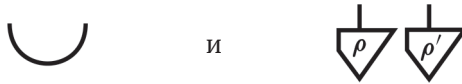


мы получаем универсальный язык для отображений с целочисленными матрицами, т. е. процессную теорию $\mathbf{matrices}(\mathbb{Z}) \subseteq$ **линейные отображения**. Существует

даже графическое исчисление, полное относительно этой теории. И что же это такое? Не скажем, надо же оставить что-то для книги «Еще об изображении квантовых процессов»!

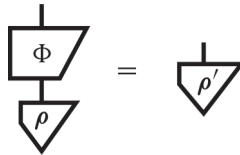
13.4. Итоги: что следует запомнить

1. *Ресурсная теория* – это разновидность процессной теории, в которой типы называются *ресурсами*, а процессы – преобразованиями ресурсов. Она отражает идею о том, что ресурсы (например, состояния) определенных типов ценнее, чем другие; например, запутанные состояния более желанны, чем разделимые:



Если дана произвольная процессная теория \mathbf{P} (например, **квантовых процессов**) и подтеория *бесплатных процессов* \mathbf{F} , то можно построить ресурсную теорию \mathbf{P}/\mathbf{F} , в которой:

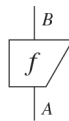
- типами являются состояния \mathbf{P} ;
- процессами, отображающими ρ в ρ' , являются такие процессы Φ в \mathbf{F} , которые преобразуют ρ в ρ' :



2. Если \mathbf{R} – ресурсная теория, то ресурс A можно *преобразовать* в ресурс B :

$$A \geq B$$

тогда и только тогда, когда существует процесс в \mathbf{R} , реализующий это преобразование:



Если буквой R обозначать ресурсы, то для любой ресурсной теории тройка

$$(R, \geq, \otimes)$$

образует *предупорядоченный моноид*, т. е. предпорядок (R, \geq) , для которого:

$$A_1 \geq B_1 \text{ и } A_2 \geq B_2 \Rightarrow A_1 \otimes A_2 \geq B_1 \otimes B_2.$$

3. *Аддитивной мерой* для ресурсной теории называется функция

$$M : (R, \geq, \otimes) \mapsto (\mathbb{R}_{\geq 0}, \leq, +),$$

которая сохраняет структуру предупорядоченного моноида, а *супремальной мерой* – функция

$$M : (R, \succeq, \otimes) \mapsto (\mathbb{R}_{\geq 0}, \leq, \max),$$

также сохраняющая структуру предупорядоченного моноида.

4. Унитарными квантовыми отображениями называются каузальные квантовые отображения Φ , которые дополнительно удовлетворяют условию:

$$\text{Diagram of } \Phi \text{ with } \frac{1}{D} \text{ on the bottom wire} = \frac{1}{D} \cdot \text{Diagram of identity map}$$

Ресурсная теория **чистоты** получается из теории **квантовых отображений**, если в качестве бесплатных процессов взять унитарные квантовые отображения:

чистота := каузальные квантовые состояния/унитарные квантовые отображения.

Отношение конвертируемости для теории **чистоты** характеризуется эквиваленцией:

$$\text{Diagram } \rho \succeq \text{Diagram } \rho' \iff \text{spec}(\rho) \geq \text{spec}(\rho')$$

где второй символ \geq обозначает *мажорирующий предупорядок*:

$$\left\{ \begin{array}{l} p^1 \geq q^1 \\ p^1 + p^2 \geq q^1 + q^2 \\ \vdots \\ p^1 + \dots + p^n \geq q^1 + \dots + q^n \end{array} \right.$$

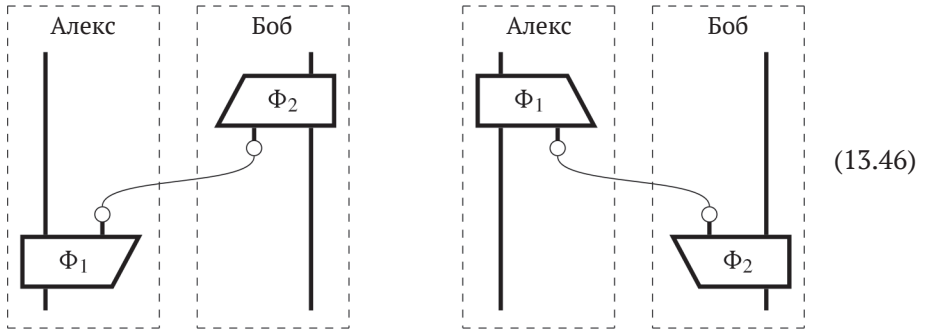
и предполагается, что последовательность p^i убывающая. *Энтропия фон Неймана*

$$S\left(\text{Diagram } \rho\right) := -\sum_i p^i \log_D(p^i)$$

дает аддитивную меру (не)чистоты, а именно:

$$\text{Diagram } \rho \succeq \text{Diagram } \rho' \implies S\left(\text{Diagram } \rho\right) \leq S\left(\text{Diagram } \rho'\right)$$

5. Подтеория **locc²** *LOCC-операций* (локальные операции и классическая коммуникация) состоит из квантовых процессов вида:



Тогда

LOCC-запутывание² := чистые квантовые состояния²/locc².

Отношение конвертируемости для теории **LOCC-запутывания²** характеризуется эквиваленцией:

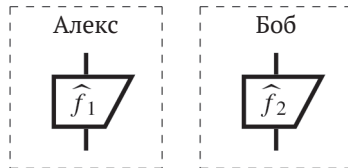
$$\begin{matrix} \text{---} \\ | \\ \text{---} \\ \psi \end{matrix} \geq \begin{matrix} \text{---} \\ | \\ \text{---} \\ \psi' \end{matrix} \iff \text{spec} \left(\begin{matrix} \text{---} \\ | \\ \text{---} \\ \psi' \\ \text{---} \end{matrix} \right) \geq \text{spec} \left(\begin{matrix} \text{---} \\ | \\ \text{---} \\ \psi \\ \text{---} \end{matrix} \right)$$

где второй символ \geq снова обозначает мажорирующий предпорядок.

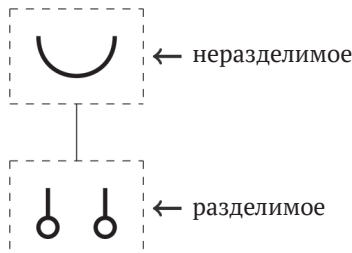
6. Подтеория **slocc²** *SLOCC-операций* (стохастические локальные операции и классическая коммуникация) состоит из (возможно, некаузальных) КК-отображений вида (13.46). Тогда:

SLOCC-запутывание² := чистые квантовые состояния²/slocc².

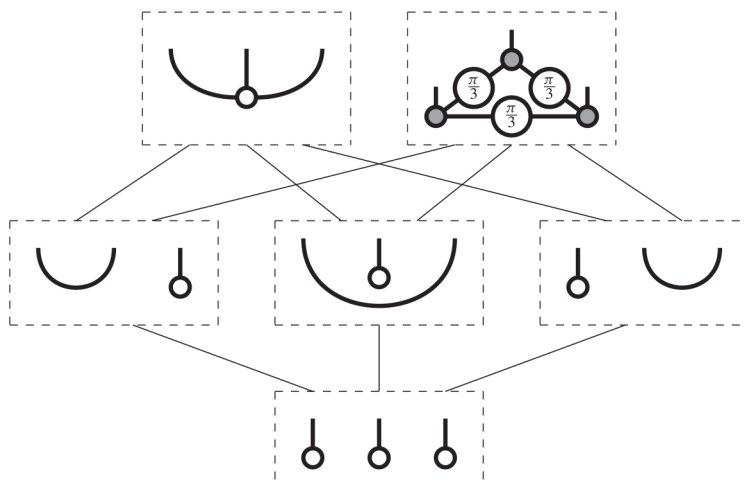
SLOCC-конвертируемость всегда можно реализовать разделимыми чистыми квантовыми отображениями:



т. е. классическая коммуникация необязательна. Для двух кубитов существует только два класса *SLOCC-эквивалентности*:



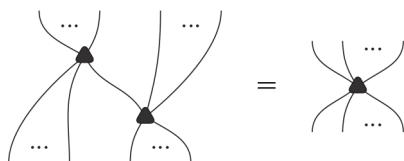
но для трех кубитов картина становится интереснее:



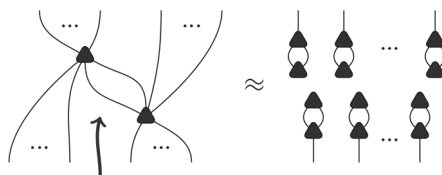
7. Состояния



– это ГХЦ-состояние и *W-состояние*. Для любого семейства пауков над \mathbb{C}^2 ассоциированное трехкомпонентное состояние всегда SLOCC-эквивалентно ГХЦ-состоянию. С другой стороны, для любого семейства *антипауков*, которые по-прежнему сливаются при наличии одного провода:



но взрываются, когда проводов два:



ассоциированное трехкомпонентное состояние



SLOCC-эквивалентно *W-состоянию*.

8. Пауки и антипауки – единственные семейства паукообразных линейных отображений над \mathbb{C}^2 , они соответствуют операциям «сложения» и «умножения»:



13.5. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Принятая нами концепция ресурсной теории в основном сформировалась внутри сообщества квантовой информации. Теоретико-процессная формулировка дана в работе Coecke et al. (2014). Понятие бесплатного процесса впервые появилось в работе Horodecki et al. (2002). Уже предложено много ресурсных теорий, например: запутывания (Horodecki et al., 2009), симметрии (Gour and Spekkens, 2008; Marvian and Spekkens, 2013), чистоты (Horodecki et al., 2003), неравновесности (Gour et al., 2013) и атермальности (Brandão et al., 2013). К описанным исследованиям примыкают работы Fong and Nava-Kopp (2015) и Fritz (2015). Поскольку в настоящее время ресурсная теория как раз выделяется в самостоятельную дисциплину, к моменту, когда вы будете читать этот текст, появится много новых статей.

Анализ, подобный проведенному в этой главе, но в контексте операционных вероятностных теорий (гибрид обобщенных вероятностных теорий и процессных теорий), можно найти в работе Chiribella and Scandolo (2015). В ней представленные здесь результаты фигурируют как аксиоматика термодинамики. Кроме того, наша лемма 13.29 принята за аксиому и называется *аксиомой локальной взаимозаменяемости*.

Энтропия, ассоциированная со смешанными квантовыми состояниями, обсуждалась уже в работе von Neumann (1927), т. е. задолго до основополагающей работы Шеннона, посвященной энтропии (Shannon, 1948), заложившей основы теории информации.

Мажорирующий предпорядок восходит к работе Роберта Франклина Мюрхеда (Robert Franklin Muirhead, 1903), который сделал несколько важных вкладов в математику, но никогда не работал в университете. Теорема 13.25 взята из работы Alberti and Uhlmann (1982). Тот факт, что смесь унитарных отображений дает унитарное квантовое отображение, является обобщением теоремы Биркгоффа в одном из возможных направлений. Эта теорема утверждает, что смеси перестановок и дважды стохастических отображений – в точности одно и то же. Предложение 13.30 заимствовано из работы Lo and Popescu (2001), а теорема 13.35 – из работы Nielsen (1999).

SLOCC-классификация трех кубитов взята из работы Dür et al. (2000). Для четырех и более кубитов количество классов SLOCC-эквивалентности несчетно. Тем не менее можно выделить конечное множество параметризованных «суперклассов» (см., например, Verstraete et al., 2002; Lamata et al., 2007). Форма W -состояния в ZX-исчислении взята из работы Coecke and Edwards (2010).

Трактовка W-состояния как антипауков появилась в работе Coecke and Kissinger (2010), так же как описание взаимодействия пауков с антипауками. Впоследствии эта тема была развита в работах Herrmann (2010) и Kissinger (2012a). Обобщение этих идей на кутриты можно найти в работе Honda (2012). Интерпретация пауков (т. е. ГХЦ-состояний) и антипауков (т. е. W-состояний) как операций «умножения» и «сложения» предложена в работе Coecke et al. (2010b). Полнота соответствующего исчисления доказана в работе Hadzihasanovic (2015).

Глава 14

Программа Quantomatic

Мы призываем вас развивать три главных достоинства программиста: лень, нетерпение и самомнение.

– Ларри Уолл
«Программирование на языке Perl»,
1-е издание

Ну, вот мы и здесь. Несколько сотен страниц и более 3000 диаграмм – мы рассказали вам (почти) все, что знаем о квантовой теории и диаграммных рассуждениях. И что дальше? Уже пора покрывать доски и заполнять листы бумаги диаграммами? Конечно!

А еще лучше, если бы кто-то занялся доказыванием на диаграммах вместо вас, а вы бы сидели, откинувшись на спинку кресла, и потягивали пиво, правда? Ну, точно, это куда лучше! Диаграммы, по существу, состоят из конечного числа ингредиентов (если точнее, пауков), а это значит, что они отлично подходят для *автоматизированных рассуждений*. В этой области искусственного интеллекта разрабатывают программы, наделяющие компьютер способностью выполнять действия, которые обычно ассоциируются с работой математика: от простой проверки правильности математических доказательств до автоматического поиска новых доказательств или даже открытия новых интересных теорем, которые затем компьютер пытается доказать автоматически.

В прошлом автоматические рассуждения обычно касались традиционной математики на основе формул и базировались на формальной логике и основанных на множествах алгебраических структурах. И в этом направлении удалось добиться значительных успехов. Мы получили инструменты, называемые *доказывателями теорем*, которые умеют автоматически строить доказательства таких заумных результатов, как теоремы Гёделя о неполноте, и строго проверять доказательства, слишком длинные для полного восприятия математиком-человеком, например: гипотезы Кеплера, теоремы о четырех красках и теоремы Фейта–Томпсона (самые знаменитые длинные доказательства в геометрии, теории графов и теории групп соответственно).

Помимо исполнения роли «робота-помощника», который неустанно проверяет работу математиков, различные техники автоматизированного рассуждения помогают открывать новые факты с помощью *синтеза гипотез*. Математик-человек изучает свойства и поведение незнакомых математических объектов «методом тыка» (формулируя предположения и пытаясь их доказать). Существуют автома-

тизированные методы, которые делают то же самое, но очень быстро. Если удастся найти доказательство, то мы получаем свежее испеченную теорему, которую ни один человек не видел и даже не обдумывал.

Вообще, если вы не можете придумать, что подарить на Рождество, можете купить такие теоремы на сайте theorymine.co.uk (и назвать их в честь одаряемого).

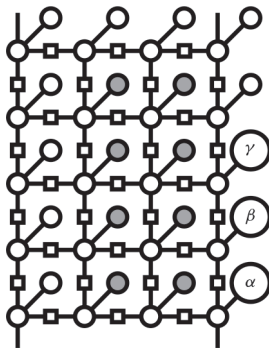
«Хорошо, хорошо, – слышу я, – но какое отношение все это имеет к диаграммам?» В этой главе мы поговорим о том, как автоматизированные рассуждения проникли на территорию диаграмм и как их можно применить к тому, чем мы занимались в этой книге с помощью диаграммного доказывателя теорем Quantomatic. Эта программа позволяет создавать струнные диаграммы и равенства между ними, а затем применять эти равенства для доказательства теорем. Это можно делать в пошаговом режиме, как мы делали все это время, или в автоматическом – с помощью *стратегий доказывания*. В последнем случае легко удастся справляться со струнными диаграммами и диаграммными доказательствами, слишком большими для работы вручную. Мы также увидим, как начинают давать отдачу такие мощные результаты, как теорема о полноте для ZX-исчисления из раздела 9.4.5, поскольку их можно преобразовать в стратегии, которые полностью автоматизируют графические доказательства.

Диаграммы особенно хорошо подходят для синтеза гипотез, поскольку зачастую у нас имеется набор базовых «генераторов» (например, пауков), и мы хотим понять, как выглядит графическое исчисление для них. В конце главы мы обсудим, как работает синтез гипотез в Quantomatic, и посмотрим, какой прогресс достигнут на пути автоматического открытия новых теорем, касающихся физических теорий.

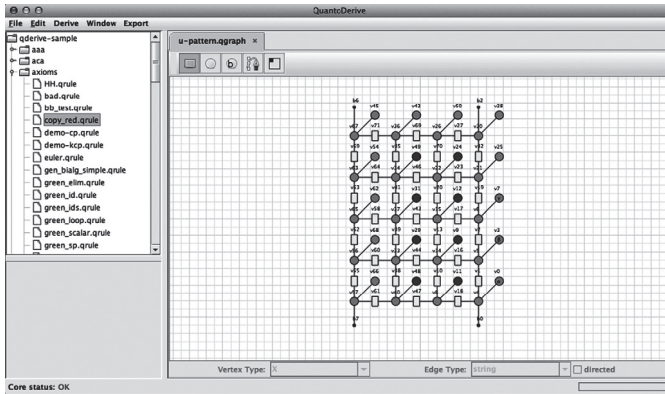
14.1. ПРОВЕРКА QUANTOMATIC В ДЕЛЕ

Сейчас вы составите представление о том, как работать с Quantomatic и какого рода вычисления она умеет делать. Мы не будем глубоко вдаваться в детали, поскольку они неизбежно устареют, т. к. программа постоянно развивается. Конечно, будет лучше всего, если вы скачаете последнюю версию с сайта quantomatic.github.io и поэкспериментируете с ней самостоятельно. На сайте имеются демонстрационные проекты и пособия.

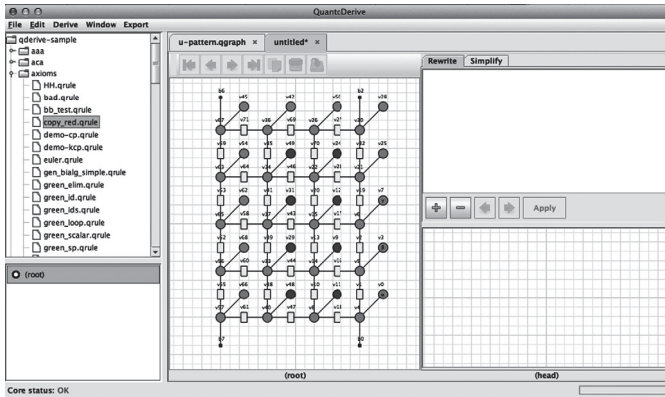
Хорошим кандидатом для автоматизации являются MBQC-вычисления, поскольку диаграммы могут расти довольно быстро. Рассмотрим такое вычисление:



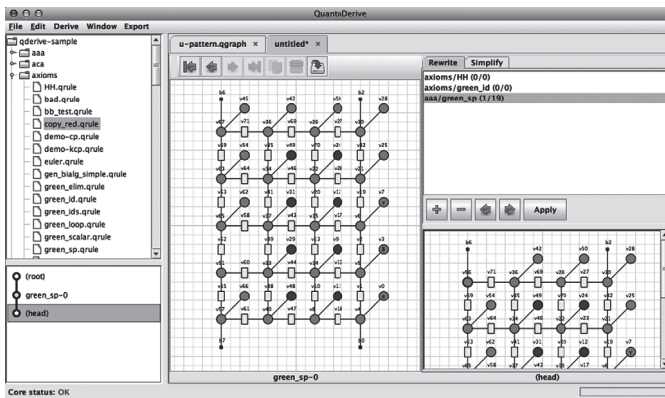
Вот как выглядит эта диаграмма в Quantomatic:



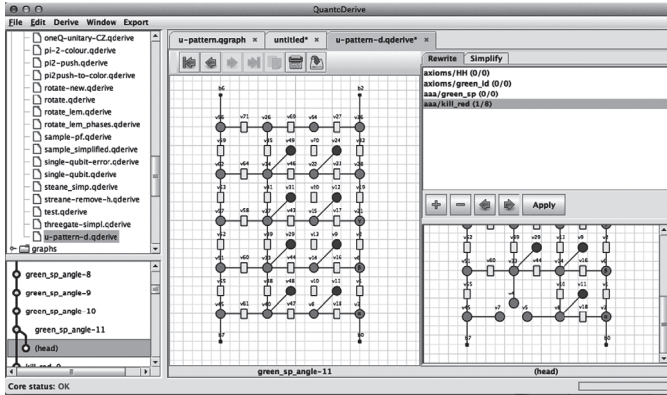
Теперь посмотрим, как можно ее упростить, и для этого начнем вывод:



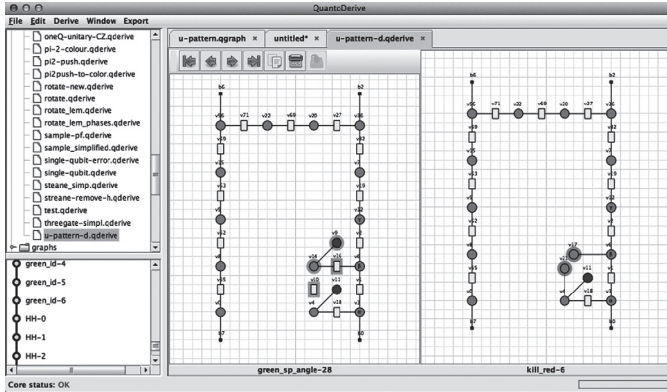
Добавим несколько правил и начнем преобразования:



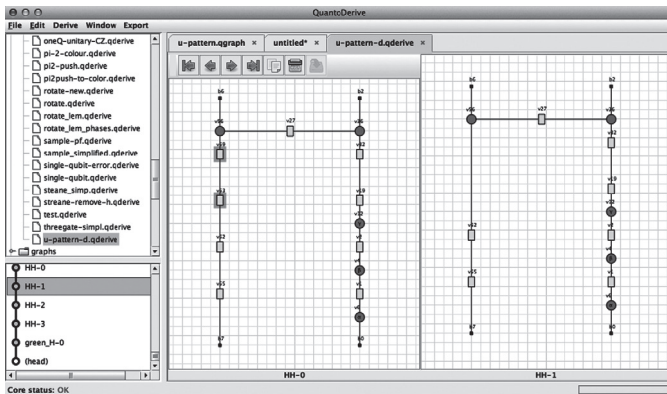
...еще преобразования...



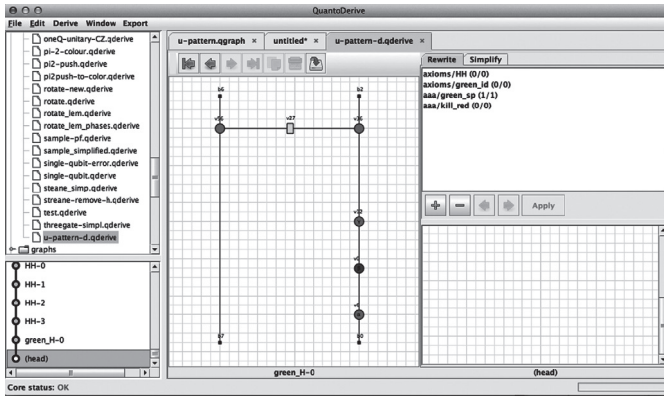
...и еще...



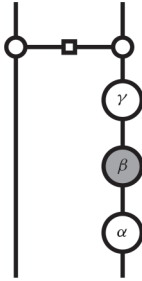
...почти у цели...



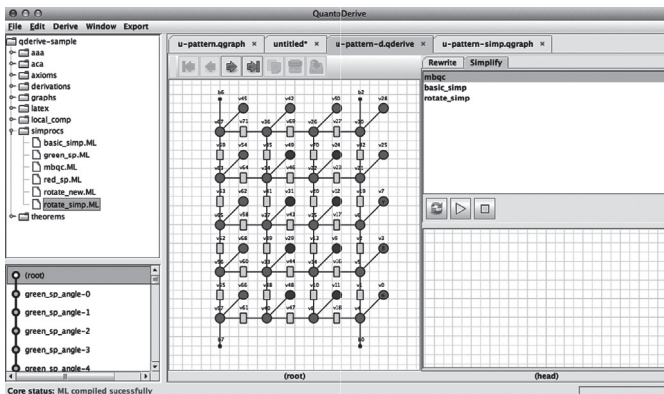
...и наконец-то:



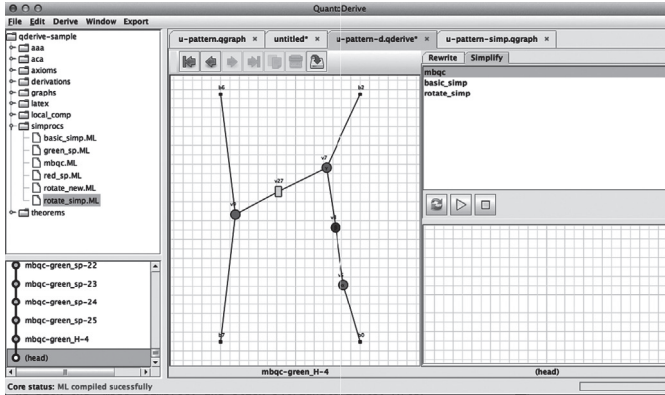
Чуть больше 50 шагов – и мы пришли к фазовым вентилям и CZ-вентилю:



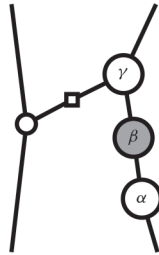
Однако! Работы-то сколько! Вообще-то, в Quantomatic это заняло примерно 15 минут. Но хотелось бы уложиться в 15 секунд, поэтому перейдем в режим *упростителя*:



Упрощатель в Quantomatic производит преобразования автоматически, применяя одну или несколько программируемых стратегий доказывания. Это небольшие программки, которые подсказывают Quantomatic, каким должно быть следующее применяемое правило. Выберите стратегию `mbqc` и нажмите \triangleright . 15 секунд психоделического светового шоу – и мы получаем результат:

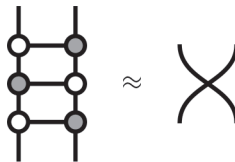


совпадающий с тем, что мы ожидали, с точностью до дополнительного слияния пауков:

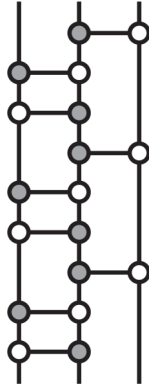


Несмотря на большое количество шагов, это вычисление было довольно простым. После ряда слияния пауков нужно было лишь устранить \bullet -пауков, появляющихся в результате Z -измерений, как описано в разделе 12.3.2, а оставшиеся N -вентили исключить с помощью правила изменения цвета.

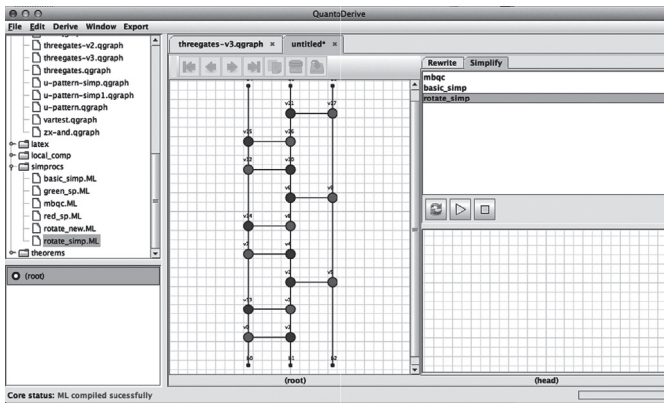
Теперь попробуем кое-что не столь очевидное, взятое из схемной модели. Мы уже видели, что три вентили CNOT равны перекмутации:



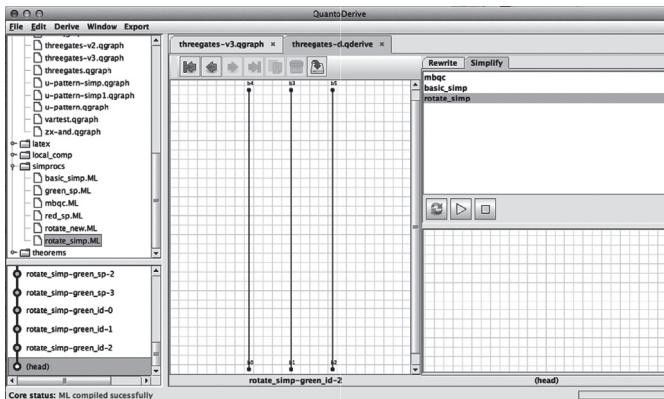
А как насчет такой, куда более сложной, конфигурации вентилей CNOT?



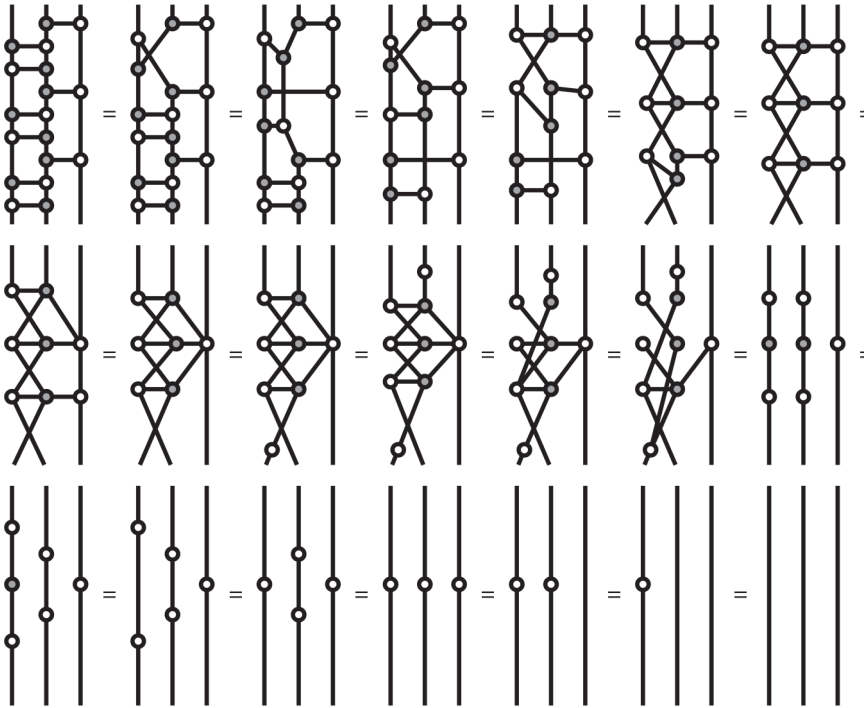
Можно, конечно, начать сливать пауков или, быть может, воспользоваться сильной дополнительностью, чтобы избавиться от 4-циклов, но даже после того как мы это сделаем, совершенно не понятно, куда двигаться дальше. А давайте скормим эту диаграмму упростилю Quantomatic:



На этот раз выберем стратегию доказывания `rotate simp`, которая приводит любую ZX-диаграмму к канонической форме:



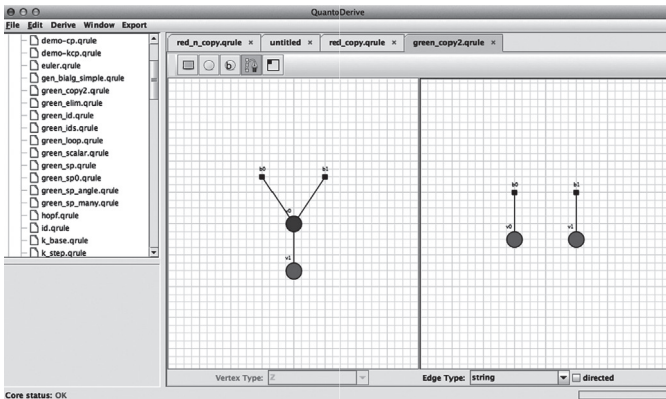
Оказывается, что это просто тождество. Чтобы понять, как Quantomatic пришла к этому выводу, мы можем экспортировать доказательство, найденное упростителем:



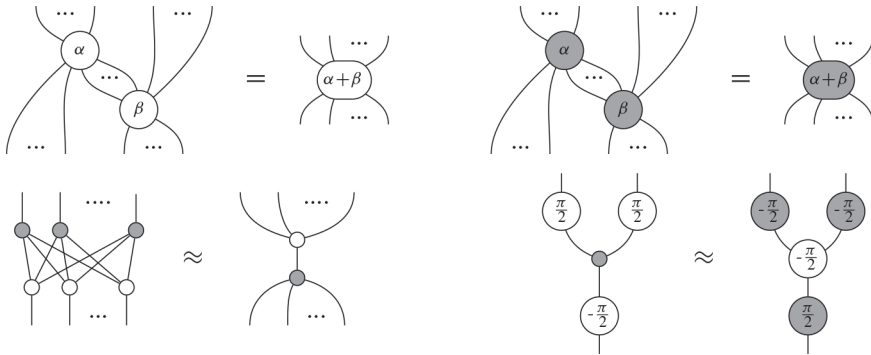
Как видим, мы оказались в затруднении, а Quantomatic радостно свела диаграмму к тождеству. А слава и почет – нам!

14.2. !-блоки: ЗАМЕНА МНОГОТОЧИЮ

До сих пор мы обходили молчанием вопрос о том, как в Quantomatic выглядят правила. С простыми правилами все понятно: два графа с одинаковыми входами и выходами в каждой части:

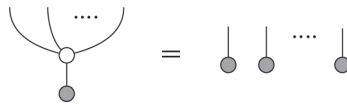


но если взглянуть на ZX-исчисление:

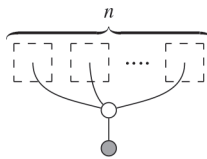


то окажется, что три из четырех правил на самом деле представляют собой семейства правил, о чем свидетельствует многоточие «...» в левой и правой частях. Записывая такое правило, мы неявно рассчитываем, что его будет читать человек, которому понятно, что мы имеем в виду, или можно легко объяснить наши намерения словами.

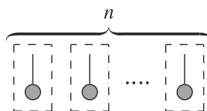
Очевидно, что с Quantomatic это не пройдет, так что придется формализовать идею многоточия, так чтобы она стала понятной машине. Чтобы понять, как это делается, начнем с несколько более простого правила n -кратного копирования, которое тоже содержит многоточие:



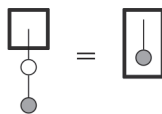
В левой и правой частях имеется некоторая поддиаграмма, повторенная n раз. В левой части она содержит всего один выходной провод:



где каждая копия соединена с одним и тем же \circ -пауком, тогда как правая часть содержит n копий целого \bullet -паука с одним выходом:



Мы можем обозначить такое повторение, заключив часть диаграммы в $!$ -блок:



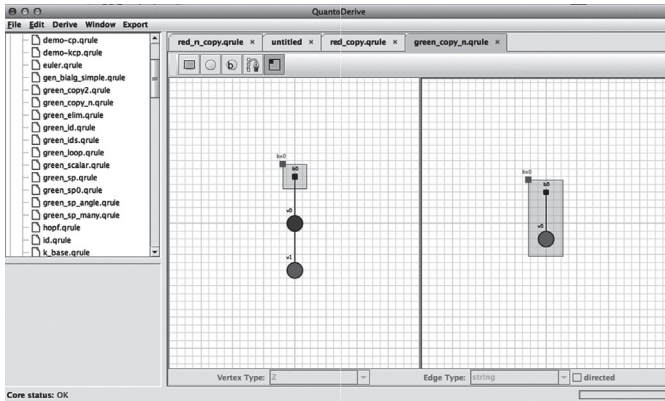
(произносится «бэнг-блок»). Диаграмма с !-блоками интерпретируется как семейство диаграмм, полученное путем копирования диаграммы внутри !-блока n раз с сохранением всех проводов, входящих в !-блок и исходящих из него:

$$\left[\left[\begin{array}{c} \square \\ \circ \\ \bullet \end{array} \right] \right] := \left\{ \begin{array}{c} \circ \\ \bullet \end{array}, \begin{array}{c} | \\ \bullet \end{array}, \begin{array}{c} \diagup \\ \circ \\ \diagdown \\ \bullet \end{array}, \begin{array}{c} \diagup \diagdown \\ \circ \\ \bullet \end{array}, \dots \right\}$$

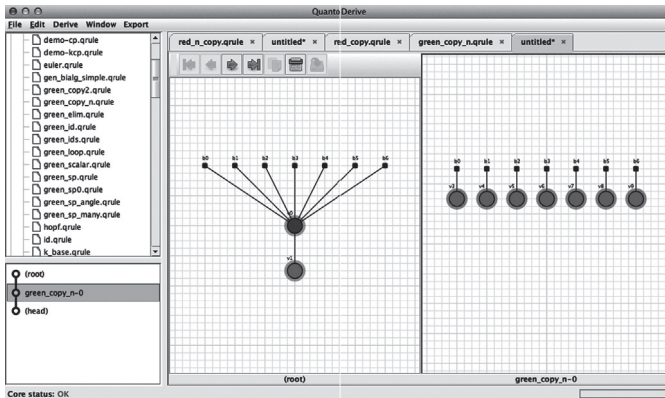
Таким образом, равенство между диаграммами с !-блоками дает целое семейство диаграммных равенств, в котором каждый !-блок в левой части и соответствующий ему !-блок в правой части копируются n раз:

$$\left[\left[\begin{array}{c} \square \\ \circ \\ \bullet \end{array} \right] = \begin{array}{c} \square \\ \bullet \end{array} \right] := \left\{ \begin{array}{c} \circ \\ \bullet \end{array} = \square, \begin{array}{c} | \\ \bullet \end{array} = \bullet, \begin{array}{c} \diagup \\ \circ \\ \diagdown \\ \bullet \end{array} = \bullet \bullet, \dots \right\}$$

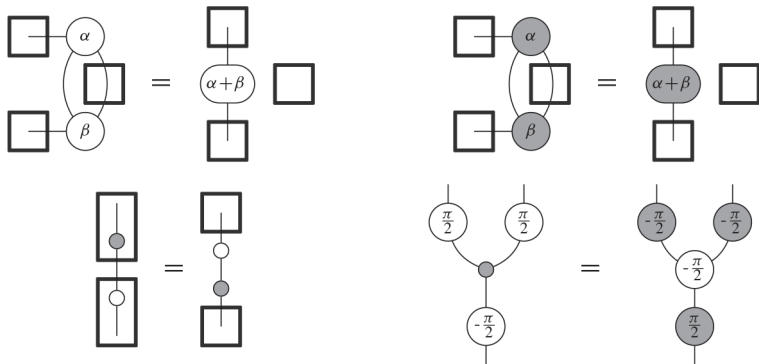
В Quantomatic это правило !-блока выглядит так:



Его можно применить, чтобы породить, например:



Применяя правила !-блока, мы можем выразить ZX-исчисление в Quantomatic следующим образом:

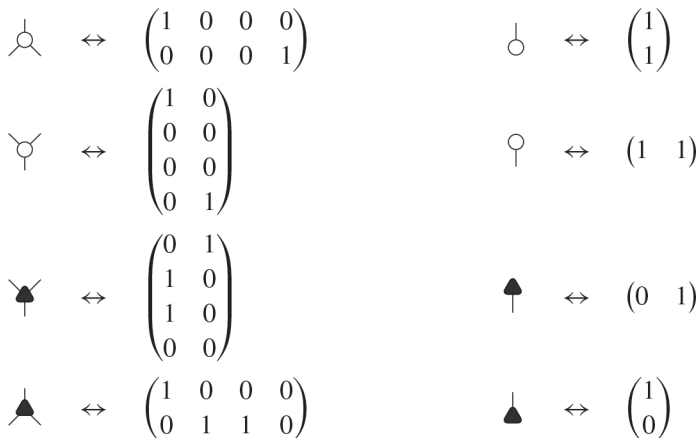


Удивительно, но совершенно общее правило сильной дополненности, которое непросто описать словами, очень легко записывается с помощью !-блоков.

14.3. СИНТЕЗ ФИЗИЧЕСКИХ ТЕОРИЙ

Может ли машина придумать новые интересные теоремы в области физики? Точнее, может ли она, соединяя ингредиенты диаграммной теории (например, пауков и антипауков), автоматически определить, как они взаимодействуют? Именно в этом состоит назначение второго компонента Quantomatic – синтеза гипотез.

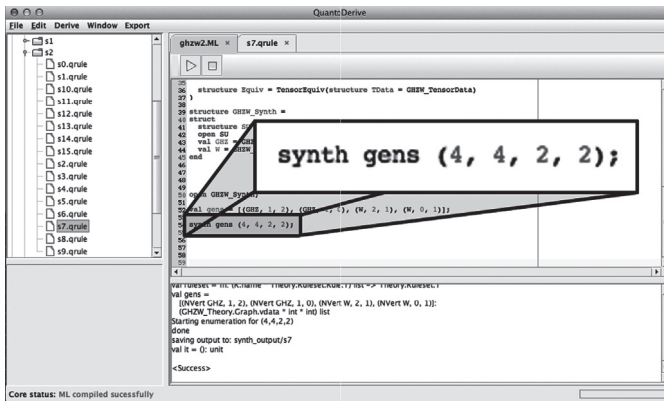
Вместо того чтобы, начав с фиксированного набора правил переписывания диаграмм, пытаться вывести новые правила, этот компонент начинает с конкретной модели и пытается выявить правила, которые должны выполняться. Иными словами, предположим, что имеется набор генераторов, заданных в конкретном виде, например в виде матриц:



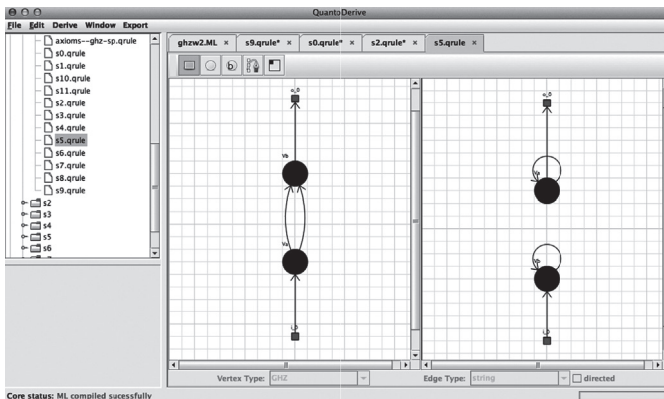
но мы понятия не имеем, какого сорта равенства имеют место между диаграммами этих генераторов. Являются ли они пауками? Удовлетворяют ли чему-то вроде правил сильной дополнителности? Или это что-то совсем другое?

Чтобы попытаться выяснить это, ученые (вроде нас с вами) просто начали бы соединять объекты между собой и смотреть, какие равенства при этом получаются. Это вполне алгоритмизируемый процесс, так что, в принципе, машина могла бы с ним справиться. К тому же машина сделает это гораздо быстрее и более систематически.

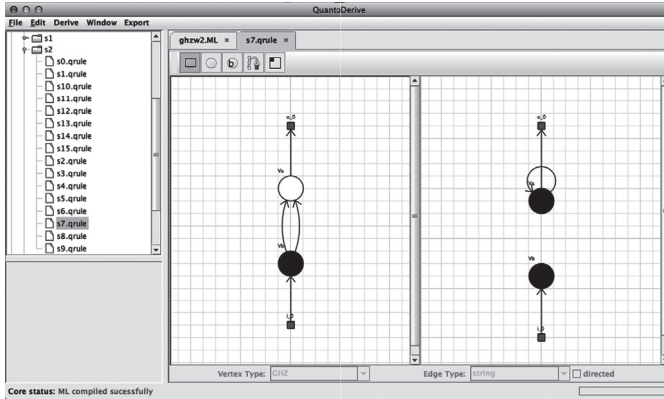
Тут-то и вступает в игру синтез гипотез. Это процедура эффективного перечисления диаграмм вплоть до заданного размера с использованием попутно обнаруженных правил для устранения избыточности и ускорения поиска новых интересных правил. После задания списка генераторов (ниже он называется «gens») нужно вызвать эту процедуру в Quantomatic таким заклинанием:



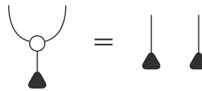
которое выполняет синтез вплоть до размера (4, 4, 2, 2), т. е. генерирует правила, содержащие не более четырех генераторов, четырех соединяющих их проводов, двух входов и двух выходов. Правил с такими параметрами существует 170. Среди них множество вариантов правила слияния пауков, наши друзья – взрывающиеся антипауки (показаны черным цветом):



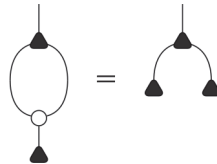
а также вариант ГХЦ-паука вверху:



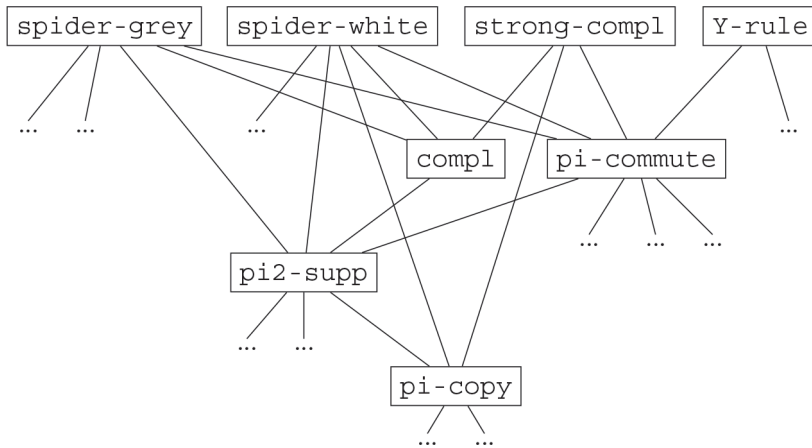
Конечно, 170 разрозненных правил – еще не графическое исчисление. И вот тут-то начинается самое интересное – мы пытаемся выявить соотношения между этими правилами. Какие правила самые важные? Какие обладают наибольшей «доказательной силой»? Процедура поиска спроектирована так, чтобы исключить правила, которые «очевидно» выводятся из других. Например, если нам известно правило



то «умный» синтезатор гипотез не станет проверять, выполняется ли правило:



Но как насчет менее очевидных вещей? Для них можно использовать стратегии автоматизированного доказывания типа описанных в разделе 14.1 и попытаться выстроить зависимости между правилами, т. е. граф, показывающий, какие правила можно доказать с помощью других. Например, для ZX-исчисления будет построен примерно такой граф:



из которого легко вывести наиболее интересные базовые правила и нетривиальные теоремы, существующие в этой теории. Высшим достижением, конечно, было бы открытие теорем, которые интересны сами по себе вне зависимости от того, как были найдены. Разумеется, у такого развития событий есть нежелательный побочный эффект – мы, ученые, оказываемся не у дел!

14.4. ИСТОРИЧЕСКИЕ ЗАМЕЧАНИЯ И ССЫЛКИ

Теория, стоящая за программой *Quantomatic*, описанной в работе Kissinger and Zamdzhiev (2015), разработана в статье Dixon and Kissinger (2013) по следам более ранних результатов из работ Dixon and Duncan (2010) и Dixon et al. (2010). $!$ -блоки впервые предложены в работе Dixon and Duncan (2009) и формализованы в работе Kissinger et al. (2014).

Один из первых интерактивных доказывателей теорем, Stanford LCF, разработан Робинот Милнером (Robin Milner, 1972) и назван по первым буквам названия «logic of computable functions» (логика вычислимых функций) в работе Dana Scott (1993). За ним последовал Edinburgh LCF (Gordon et al., 1979), который заложил основы *парадигмы LCF*, состоящей из логического «ядра», управляемого различными (полу)автоматизированными «тактиками». Краткую историю можно прочитать в работе Gordon (2000). Из других известных доказывателей, воспринявших эту парадигму, отметим Isabelle (Paulson et al., 1986) и Coq (Coquand et al., 1984). Последний недавно привлек особенное внимание благодаря использованию в гомотопической теории типов и унивалентных основаниях математики (Shulman et al., 2013).

В последние годы с помощью доказывателей теорем было полностью формализовано несколько гигантских доказательств. Проект *Flyspeck*, возглавляемый Хейлсом (Hales et al. 2015), в 2015 году добился успеха в формальном доказательстве гипотезы Кеплера. Формальное доказательство теоремы о четырех красках было дано в работе Gonthier (2008), а теоремы Фейта–Томпсона – в работе Gonthier et al. (2013).

Метод синтеза диаграммных теорий предложен в работе Kissinger (2012b) и основан на технике, разработанной в статье Johansson et al. (2011). Последняя была применена (среди прочего!) к автоматическому доказательству простых теорем, которые можно купить в качестве подарков (Bundy et al., без даты).

Второй пример в разделе 14.1 эквивалентен правилу (C14) из работы (Selinger, 2015) – одному из 15 правил, использованных при построении полного исчисления для схем Клиффорда.

Приложение

Некоторые обозначения

В книге применяются следующие обозначения.

Общие

- $X := Y$ означает, что X по определению является (или интерпретируется как) Y
- $X \leftrightarrow Y$ означает, что X соответствует Y
- $X \Leftrightarrow Y$ означает, что X тогда и только тогда, когда Y
- \exists – существует
- \forall – для любого
- \checkmark означает «хорошо»
- \otimes означает «плохо»


Множества

- \emptyset – пустое множество
- \mathbb{R} – множество всех вещественных чисел
- \mathbb{R}^+ – множество всех положительных вещественных чисел
- $[0, 1]$ – множество вещественных чисел от 0 до 1 (включительно)
- $x \in X$ означает, что x является элементом X
- $X \subseteq Y$ означает, что X является подмножеством Y
- $X - Y$ – множество элементов X , не являющихся элементами Y
- $X \cong Y$ означает, что X изоморфно Y
- $\{X \mid Y\}$ – множество всех таких X , для которых выполняется Y

Функции и отношения

- $x \mapsto y$ означает, что x отображается в y
- $f: X \rightarrow Y$ означает, что f – функция из множества X в множество Y
- $f :: x \mapsto y$ означает, что функция или отношение f отображает x в y
- $f :: \begin{cases} x_1 \mapsto y_1 \\ x_2 \mapsto y_2 \\ \vdots \\ x_n \mapsto y_n \end{cases}$ означает, что функция (или отношение) f отображает ..., x_i в y_i , ...
- $R :: \begin{cases} x_1 \mapsto Y_1 \\ x_2 \mapsto Y_2 \\ \vdots \\ x_n \mapsto Y_n \end{cases}$ означает, что отношение R отображает ..., x_i во все $y_i \in Y_i$, ...
- $f(a)$ означает те элементы, в которые функция (или отношение) f отображает a

Диаграммы

-  – пустая диаграмма
- 0 – любая нулевая диаграмма

Библиография

Abramsky S. 2010. No-cloning in categorical quantum mechanics. Pages 1–28 of: Gay, S., and Mackie, I. (eds), *Semantic Techniques in Quantum Computation*. Cambridge University Press. Arxiv preprint arXiv:0910.2401.

Abramsky S. and Coecke B. 2004. A categorical semantics of quantum protocols. Pages 415–425 of: *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LICS)*. arXiv:quant-ph/0402130.

Abramsky S. and Coecke B. 2005. Abstract physical traces. *Theory and Applications of Categories*, **14** (6), 111–124. arXiv:0910.3144.

Abramsky S. and Heunen C. 2012. Operational theories and categorical quantum mechanics. In: *Logic and Algebraic Structures in Quantum Computing*. Cambridge University Press. arXiv:1206.0921.

Abramsky S. and Jagadeesan R. 1994. New foundations for the geometry of interaction. *Information and Computation*, **111**, 53–119.

Abramsky S. and Tzevelekos N. 2011. Introduction to categories and categorical logic. Pages 3–94 of: Coecke, B. (ed), *New Structures for Physics*. Lecture Notes in Physics. Springer-Verlag.

Alberti P. M. and Uhlmann A. 1982. Stochasticity and Partial Order. *Mathematics and Its Applications*, vol. 9. Reidel.

Ambainis A. 2010. New developments in quantum algorithms. arXiv:1006.4014.

Aspect A., Grangier P. and Roger G. 1981. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, **47** (7), 460.

Aspect A., Dalibard J. and Roger G. 1982. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, **49** (25), 1804.

Awodey S. 2010. *Category Theory*. Oxford University Press.

Backens M. 2014a. The ZX-calculus is complete for the single-qubit Clifford+T group. Pages 293–303 of: Coecke, B., Hasuo, I. and Panangaden, P. (eds), *Proceedings of the 11th Workshop on Quantum Physics and Logic*. Electronic Proceedings in Theoretical Computer Science, vol. 172. Open Publishing Association.

Backens M. 2014b. The ZX-calculus is complete for the single-qubit Clifford+T group. arXiv:1412.8553.

Backens M. and Nabi Duman A. 2015. A complete graphical calculus for Spekkens' toy bit theory. *Foundations of Physics*. arXiv:1411.1618.

Backens M., Perdrix S. and Wang Q. 2016. A simplified stabilizer ZX-calculus. In: *Proceedings of the 13th International Conference on Quantum Physics and Logic*. arXiv:1602.04744.

Baez J. C. 1993–2010. This week's finds in mathematical physics. math.ucr.edu/home/baez/TWF.html.

Baez J. C. 2006. Quantum quandaries: a category-theoretic perspective. Pages 240–266 of: Rickles, D., French, S., and Saatsi, J.T. (eds), *The Structural Foundations of Quantum Gravity*. Oxford University Press. arXiv:quant-ph/0404040.

Baez J. C. and Dolan J. 1995. Higher-dimensional algebra and topological quantum field theory. *Journal of Mathematical Physics*, **36**, 6073. arXiv:q-alg/9503002.

- Baez J. C. and Erbele J. Categories in control. arXiv:1405.6881.
- Baez J. C. and Fong B. 2015. A compositional framework for passive linear networks. arXiv:1504.05625.
- Baez J. C. and Lauda A. 2011. A prehistory of n-categorical physics. Pages 13–128 of: Halvorson, H. (ed), *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*. Cambridge University Press.
- Baez J. C. and Stay M. 2011. Physics, topology, logic and computation: a Rosetta Stone. Pages 95–172 of: Coecke, B. (ed), *New Structures for Physics*. Lecture Notes in Physics. Springer.
- Balkir E., Sadrzadeh M. and Coecke B. 2016. Distributional Sentence Entailment Using Density Matrices. Cham: Springer International Publishing. Pages 1–22.
- Ballance C. J., Harty T. P., Linke N. M., Sepiol M. A. and Lucas D. M. 2016. High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits. *Physical Review Letters*, **117** (6), 060504.
- Baltag A. and Smets S. 2005. Complete axiomatizations for quantum actions. *International Journal of Theoretical Physics*, **44**, 2267–2282.
- Bankova D., Coecke B., Lewis M. and Marsden D. 2016. Graded entailment for compositional distributional semantics. In: Proceedings of the 13th International Conference on Quantum Physics and Logic. arXiv:1601.04908.
- Barenco A., Bennett C. H., Cleve R., DiVincenzo D. P., Margolus N., Shor P. W., Sleator T., Smolin J. A. and Weinfurter H. 1995. Elementary gates for quantum computation. *Physical Review A*, **52**, 3457–3467.
- Barnum H., Caves C. M., Fuchs C. A., Jozsa R. and Schumacher B. 1996. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, **76**, 2818.
- Barnum H., Barrett J., Leifer M. and Wilce A. 2007. A generalized no-broadcasting theorem. *Physical Review Letters*, **99** (24), 240501.
- Barr M. and Wells C. 1990. *Category Theory for Computing Science*. New York: Prentice Hall.
- Barrett J. 2007. Information processing in generalized probabilistic theories. *Physical Review A*, **75**, 032304.
- Belinfante F. J. 1973. *Survey of Hidden-Variables Theories*. Pergamon Press.
- Bell J. S. 1964. On the Einstein–Podolsky–Rosen paradox. *Physics*, **1** (3), 195–200.
- Benabou J. 1963. Categories avec multiplication. *Comptes Rendus des Séances de l'Académie des Sciences. Paris*, **256**, 1887–1890.
- Benioff P. 1980. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, **22**, 563–591.
- Bennett C. H. and Brassard G. 1984. Quantum cryptography: public key distribution and coin tossing. Pages 175–179 of: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. IEEE.
- Bennett C. H. and Wiesner S. 1992. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Physical Review Letters*, **69**, 2881–2884.
- Bennett C. H., Brassard G., Crepeau C., Jozsa R., Peres A. and Wootters W. K. 1993. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters*, **70** (13), 1895–1899.
- Birkhoff G. and von Neumann J. 1936. The logic of quantum mechanics. *Annals of Mathematics*, **37**, 823–843.

- Bloch F. 1946. Nuclear induction. *Physical Review*, **70**, 460–474.
- Blute R. F., Ivanov I. T. and Panangaden P. 2003. Discrete quantum causal dynamics. *International Journal of Theoretical Physics*, **42** (9), 2025–2041.
- Bohm D. 1952a. A suggested interpretation of the quantum theory in terms of «hidden» variables. I. *Physical Review*, **85** (2), 166.
- Bohm D. 1952b. A suggested interpretation of the quantum theory in terms of «hidden» variables. II. *Physical Review*, **85** (2), 180.
- Bohm D. 1986. Time, the implicate order and pre-space. Pages 172–208 of: Griffin, D. R. (ed), *Physics and the Ultimate Significance of Time*. SUNY Press.
- Bohm D. and Peat F. D. 1987. *Science, Order, and Creativity*. Routledge.
- Bohr N. 1931. *Atomtheorie und Naturbeschreibung*. Springer.
- Bohr N. 1935. Quantum mechanics and physical reality. *Nature*, **136**, 65.
- Bohr N. 1961. *Atomic Physics and Human Knowledge*. Science Editions.
- Boixo S. and Heunen C. 2012. Entangled and sequential quantum protocols with dephasing. *Physical Review Letters*, **108**, 120402. arXiv:1108.3569.
- Bonchi F., Sobocinski P. and Zanasi F. 2014a. A categorical semantics of signal flow graphs. Pages 435–450 of: CONCUR'14: Concurrency Theory. Lecture Notes in Computer Science, vol. 8704. Springer.
- Bonchi F., Sobocinski P. and Zanasi F. 2014b. Interacting bialgebras are Frobenius. Pages 351–365 of: 17th International Conference on Foundations of Software Science and Computation Structures (FOSSACS).
- Borceux F. 1994a. *Handbook of Categorical Algebra: Basic Category Theory*. Cambridge University Press.
- Borceux F. 1994b. *Handbook of Categorical Algebra: Categories and Structures*. Cambridge University Press.
- Born M. 1926. Quantenmechanik der stoßvorgänge. *Zeitschrift für Physik*, **38** (11–12), 803–827.
- Born M. and Jordan P. 1925. Zur Quantenmechanik. *Zeitschrift für Physik*, **34**, 858–888.
- Bourbaki N. 1959–2004. *Éléments de mathématique*. CCLS & Editions Masson.
- Bourbaki N. 1981. *Espaces vectoriels topologiques*. Springer.
- Bourbaki N. 1987. *Topological Vector Spaces*. Springer.
- Bouwmeester D., Pan J.-W., Mattle K., Eibl M., Weinfurter H. and Zeilinger A. 1997. Experimental quantum teleportation. *Nature*, **390** (6660), 575–579.
- Brandão F. G. S. L., Horodecki M., Oppenheim J., Renes J. M. and Spekkens R. W. 2013. The resource theory of quantum states out of thermal equilibrium. *Physical Review Letters*, **111**, 250404.
- Brauer R. and Nesbitt C. 1937. On the regular representations of algebras. *Proceedings of the National Academy of Sciences of the United States of America*, **23** (4), 236.
- Bub J. 1999. *Interpreting the Quantum World*. Cambridge University Press.
- Buchsbaum D. 1955. Exact categories and duality. *Transactions of the American Mathematical Society*, **80**, 1–34.
- Bundy A., Cavallo F., Dixon L., Johansson M. and McCasland R. N.d. 2015. The theory behind TheoryMine. *IEEE Intelligent Systems*, **30** (4), 64–69.
- Carboni A. and Walters R. F. C. 1987. Cartesian bicategories I. *Journal of Pure and Applied Algebra*, **49**, 11–32.
- Carroll L. 1942. *Alice in Wonderland*. Pelangi Publishing Group Bhd.
- Chiribella G. 2014. Distinguishability and copiability of programs in general process theories. arXiv:1411.3035.

Chiribella G. and Scandolo C. M. 2015. Entanglement and thermodynamics in general probabilistic theories. *New Journal of Physics*, **17**, 103027.

Chiribella G., D'Ariano G. M. and Perinotti P. 2010. Probabilistic theories with purification. *Physical Review A*, **81** (6), 062348.

Chiribella G., D'Ariano G. M. and Perinotti P. 2011. Informational derivation of quantum theory. *Physical Review A*, **84** (1), 012311.

Choi M.-D. 1975. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, **10**, 285–290.

Clark S., Coecke B., Grefenstette E., Pulman S. and Sadrzadeh M. 2014. A quantum teleportation inspired algorithm produces sentence meaning from word meaning and grammatical structure. *Malaysian Journal of Mathematical Sciences*, **8**, 15–25. arXiv:1305.0556.

Clifton R., Bub J. and Halvorson H. 2003. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, **33**, 1561–1591.

Coecke B. 2000. Structural characterization of compoundness. *International Journal of Theoretical Physics*, **39**, 585–594.

Coecke B. 2003. The logic of entanglement. An invitation. Tech. rept. RR-03-12. Department of Computer Science, Oxford University.

Coecke B. 2005. Kindergarten quantum mechanics. Pages 81–98 of: Khrennikov, A. (ed), *Quantum Theory: Reconsiderations of the Foundations III*. AIP Press. arXiv: quant-ph/0510032.

Coecke B. 2007. De-linearizing linearity: projective quantum axiomatics from strong compact closure. *Electronic Notes in Theoretical Computer Science*, **170**, 49–72. arXiv: quant-ph/0506134.

Coecke, B. 2008. Axiomatic description of mixed states from Selinger's CPM-construction. *Electronic Notes in Theoretical Computer Science*, **210**, 3–13.

Coecke B. 2009. Quantum picturalism. *Contemporary Physics*, **51**, 59–83. arXiv: 0908.1787.

Coecke B. 2011. A universe of processes and some of its guises. Pages 129–186 of: Halvorson, H. (ed), *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*. Cambridge University Press. arXiv:1009.3786.

Coecke B. 2013. An alternative Gospel of structure: order, composition, processes. Pages 1–22 of: Heunen, C., Sadrzadeh, M., and Grefenstette, E. (eds), *Quantum Physics and Linguistics: A Compositional, Diagrammatic Discourse*. Oxford University Press. arXiv:1307.4038.

Coecke B. 2014a. *The Logic of Entanglement*. Cham: Springer International Publishing. Pages 250–267.

Coecke B. 2014b. Terminality implies non-signalling. arXiv:1405.3681.

Coecke B. 2016. The logic of quantum mechanics – take II. Pages 174–198 of: Chubb, J., Eskandarian, A., and Harizanov, V. (eds), *Logic and Algebraic Structures in Quantum Computing*. Cambridge University Press. arXiv:1204.3458.

Coecke B. and Duncan R. 2008. Interacting quantum observables. In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP)*. Lecture Notes in Computer Science.

Coecke B., and Duncan R. 2011. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, **13**, 043016. arXiv:quant-ph/09064725.

Coecke B., and Edwards B. 2010. Three qubit entanglement within graphical Z/Xcalculus. *Electronic Proceedings in Theoretical Computer Science*, **52**, 22–33.

Coecke B. and Edwards B. 2011. Toy quantum categories. *Electronic Notes in Theoretical Computer Science*, **270** (1), 29–40. arXiv:0808.1037.

Coecke B. and Edwards B. 2012. Spekkens's toy theory as a category of processes. In: Abramsky S. and Mislove M. (eds), *Mathematical Foundations of Information Flow*.

Proceedings of symposia in applied mathematics. American Mathematical Society. arXiv:1108.1978.

Coecke B. and Heunen C. 2011. Pictures of complete positivity in arbitrary dimension. *Quantum Physics and Logic, Electronic Proceedings in Theoretical Computer Science*, **95**, 27–35. arXiv:1210.0298.

Coecke B. and Kissinger A. 2010. The compositional structure of multipartite quantum entanglement. Pages 297–308 of: *Automata, Languages and Programming. Lecture Notes in Computer Science*. Springer. arXiv:1002.2540.

Coecke B. and Lal R. 2013. Causal categories: relativistically interacting processes. *Foundations of Physics*, **43**, 458–501. arXiv:1107.6019.

Coecke B. and Paquette É. O. 2008. POVMs and Naimark's theorem without sums. *Electronic Notes in Theoretical Computer Science*, **210**, 15–31. arXiv:quant-ph/0608072.

Coecke B. and Paquette É. O. 2011. Categories for the practicing physicist. Pages 167–271 of: Coecke, B. (ed), *New Structures for Physics. Lecture Notes in Physics*. Springer. arXiv:0905.3010.

Coecke B. and Pavlovic D. 2007. Quantum measurements without sums. Pages 567–604 of: Chen G., Kauffman L. and Lamonaco S. (eds), *Mathematics of Quantum Computing and Technology*. Taylor and Francis. arXiv:quant-ph/0608035.

Coecke B. and Perdrix S. 2010. Environment and classical channels in categorical quantum mechanics. Pages 230–244 of: *Proceedings of the 19th EACSL Annual Conference on Computer Science Logic (CSL). Lecture Notes in Computer Science*, vol. 6247. Extended version: arXiv:1004.1598.

Coecke B. and Smets S. 2004. The Sasaki hook is not a [static] implicative connective but induces a backward [in time] dynamic one that assigns causes. *International Journal of Theoretical Physics*, **43**, 1705–1736.

Coecke B. and Spekkens R. W. 2012. Picturing classical and quantum Bayesian inference. *Synthese*, **186**, 651–696. arXiv:1102.2368.

Coecke B., Moore D. J. and Wilce A. 2000. Operational quantum logic: an overview. Pages 1–36 of: Coecke B., Moore D. J. and Wilce A. (eds), *Current Research in Operational Quantum Logic: Algebras, Categories and Languages. Fundamental Theories of Physics*, vol. 111. Springer-Verlag. arXiv:quant-ph/0008019.

Coecke B., Moore D. J. and Stubbe I. 2001. Quantaloids describing causation and propagation of physical properties. *Foundations of Physics Letters*, **14**, 133–146. arXiv:quant-ph/0009100.

Coecke B., Paquette É. O. and Perdrix S. 2008a. Bases in diagrammatic quantum protocols. *Electronic Notes in Theoretical Computer Science*, **218**, 131–152. arXiv:0808.1029.

Coecke B., Paquette É. O. and Pavlović D. 2008b. Classical and quantum structures. Tech. rept. RR-08-02. Department of Computer Science, Oxford University.

Coecke B., Paquette É. O. and Pavlović D. 2010a. Classical and quantum structuralism. Pages 29–69 of: Gay S. and Mackie I. (eds), *Semantic Techniques in Quantum Computation*. Cambridge University Press. arXiv:0904.1997.

Coecke B., Kissinger A., Merry A. and Roy S. 2010b. The GHZ/W-calculus contains rational arithmetic. *Electronic Proceedings in Theoretical Computer Science*, **52**, 34–48.

Coecke B., Sadrzadeh M. and Clark S. 2010c. Mathematical foundations for a compositional distributional model of meaning. Pages 345–384 of: van Benthem J., Moortgat M. and Buszkowski W. (eds), *A Festschrift for Jim Lambek*. *Linguistic Analysis*, vol. 36. arxiv:1003.4394.

Coecke B., Wang Q., Wang B., Wang Y. and Zhang Q. 2011a. Graphical calculus for quantum key distribution (extended abstract). *Electronic Notes in Theoretical Computer Science*, **270** (2), 231–249.

Coecke B., Edwards B. and Spekkens R. W. 2011b. Phase groups and the origin of non-locality for qubits. *Electronic Notes in Theoretical Computer Science*, **270** (2), 15–36. arXiv:1003.5005.

Coecke B., Duncan R., Kissinger A. and Wang Q. 2012. Strong complementarity and non-locality in categorical quantum mechanics. In: *Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science (LICS)*. arXiv:1203.4988.

Coecke B., Heunen C. and Kissinger A. 2013a. Categories of quantum and classical channels. arXiv:1305.3821.

Coecke B., Heunen C. and Kissinger A. 2013b. Compositional quantum logic. Pages 21–36 of: *Computation, Logic, Games, and Quantum Foundations: The Many Facets of Samson Abramsky*. Springer.

Coecke B., Pavlović D. and Vicary J. 2013c. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, **23**, 555–567. arXiv:quant-ph/0810.1037.

Coecke B., Fritz T. and Spekkens R. W. 2016. A mathematical theory of resources. *Information and Computation*.

Coecke B., Duncan R., Kissinger A. and Wang Q. 2016. Generalised compositional theories and diagrammatic reasoning. In: Chiribella G. and Spekkens R. W. (eds), *Quantum Theory: Informational Foundations and Foils*. *Fundamental Theories of Physics*. Springer. arXiv:1203.4988.

Coqand T., Heut G., et al. 1984. Coq theorem prover. <https://coq.inria.fr/>.

Cunningham O. and Heunen C. 2015. Axiomatizing complete positivity. Pages 148–157 of: Heunen C., Selinger P. and Vicary J. (eds), *Proceedings of the 12th International Workshop on Quantum Physics and Logic*. *Electronic Proceedings in Theoretical Computer Science*, vol. 195. Open Publishing Association.

Davies E. B. 1976. *Quantum Theory of Open Systems*. Academic Press.

Davies E. B. and Lewis J. T. 1970. An operational approach to quantum probability. *Communications in Mathematical Physics*, **17**, 239–260.

Deutsch D. 1985. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, **400** (1818), 97–117.

Deutsch D. 1989. Quantum computational networks. *Proceedings of the Royal Society of London*, **425**.

Deutsch D. 1991. Quantum mechanics near closed timelike lines. *Physical Review D*, **44**, 3197.

Deutsch D. and Jozsa R. 1992. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, **439** (1907), 553–558.

Dieks D. G. B. J. 1982. Communication by EPR devices. *Physics Letters A*, **92** (6), 271–272.

Dijkstra E. W. 1968. A constructive approach to the problem of program correctness. *BIT Numerical Mathematics*, **8**, 174–186.

Dirac P. A. M. 1926. On the theory of quantum mechanics. *Proceedings of the Royal Society A*, **112**, 661–677.

Dirac P. A. M. 1939. A new notation for quantum mechanics. Pages 416–418 of: *Proceedings of the Cambridge Philosophical Society*, vol. 35. Cambridge University Press.

Dixon L. and Duncan R. 2009. Graphical reasoning in compact closed categories for quantum computation. *Annals of Mathematics and Artificial Intelligence*, **56** (1), 23–42.

Dixon L. and Duncan R. 2010. Extending graphical representations for compact closed categories with applications to symbolic quantum computation. *Intelligent Computer Mathematics*, 77–92.

Dixon L. and Kissinger A. 2013. Open-graphs and monoidal theories. *Mathematical Structures in Computer Science*, **23** (2), 308–359.

Dixon L., Duncan R. and Kissinger A. 2010. Open graphs and computational reasoning. Pages 169–180 of: Cooper, S. B., Panangaden, P. and Kashefi, E. (eds), *Proceedings of the Sixth Workshop on Developments in Computational Models: Causality, Computation, and Physics*. Electronic Proceedings in Theoretical Computer Science, vol. 26. Open Publishing Association.

Dixon L., Duncan R., Merry A., Kissinger A., Soloviev M. and Zamzhev V. 2011. *quantomatic*. <http://quantomatic.github.io>.

Duncan R. 2006. Types for quantum computation. DPhil Thesis, Oxford University.

Duncan R. 2012. A graphical approach to measurement-based quantum computing. arXiv:1203.6242.

Duncan R. and Lucas M. 2013. Verifying the Steane code with *Quantomatic*. In: *Proceedings of the 10th International Workshop on Quantum Physics and Logic*. arXiv:1306.4532.

Duncan R. and Perdrix S. 2009. Graph states and the necessity of Euler decomposition. *Mathematical Theory and Computational Practice*, 167–177.

Duncan R. and Perdrix S. 2010. Rewriting measurement-based quantum computations with generalised flow. Pages 285–296 of: *Proceedings of ICALP*. Lecture Notes in Computer Science. Springer.

Duncan R. and Perdrix S. 2013. Pivoting makes the ZX-calculus complete for real stabilizers. In: *Proceedings of the 10th International Workshop on Quantum Physics and Logic*. arXiv:1307.7048.

Dür W., Vidal G. and Cirac J. I. 2000. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, **62** (062314).

Durt T., Englert B.-G., Bengtsson I. and Życzkowski K. 2010. On mutually unbiased bases. *International Journal of Quantum Information*, **8**, 535–640.

Eckmann B. and Hilton P. J. 1962. Group-like structures in general categories. I. Multiplications and comultiplications. *Mathematische Annalen*, **145** (3).

Edwards B. 2009. Non-locality in categorical quantum mechanics. PhD thesis, University of Oxford.

Eilenberg S. and Mac Lane S. 1945. General theory of natural equivalences. *Transactions of the American Mathematical Society*, **58** (2), 231.

Einstein A. 1936. Physics and reality. *Journal of the Franklin Institute*, **221** (3), 349–382.

Einstein A., Podolsky B. and Rosen N. 1935. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, **47** (10), 777.

Ekert A. K. 1991. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, **67** (6), 661–663.

- Evans J., Duncan R., Lang, A. and Panangaden P. 2009. Classifying all mutually unbiased bases in Rel. arXiv:0909.4453.
- Everett H. III. 1957. «Relative state» formulation of quantum mechanics. *Reviews of Modern Physics*, **29** (3), 454.
- Faure C.-A., Moore D. J. and Piron C. 1995. Deterministic evolutions and Schrödinger flows. *Helvetica Physica Acta*, **68** (2), 150–157.
- Fausser B. 2013. Some graphical aspects of Frobenius structures. Pages 23–48 of: Heunen C., Sadrzadeh M. and Grefenstette E. (eds), *Quantum Physics and Linguistics: A Compositional, Diagrammatic Discourse*. Oxford University Press. arXiv:1202.6380.
- Feynman R. P. 1982. Simulating physics with computers. *International Journal of Theoretical Physics*, **21**, 467–488.
- Fong B. and Nava-Kopp H. 2015. Additive monotones for resource theories of parallel-combinable processes with discarding. *Electronic Proceedings in Theoretical Computer Science*, **195**, 170–178. arXiv:1505.02651.
- Fort C. 1931. Lo! Cosimo Books.
- Foulis D. J. and Randall C. H. 1972. Operational statistics. I. Basic concepts. *Journal of Mathematical Physics*, **13** (11), 1667–1675.
- Freyd P. 1964. *Abelian Categories*. New York: Harper and Row.
- Freyd P. and Yetter D. 1989. Braided compact closed categories with applications to lowdimensional topology. *Advances in Mathematics*, **77**, 156–182.
- Fritz T. 2014. Beyond Bell's theorem II: scenarios with arbitrary causal structure. arXiv: 1404.4812.
- Fritz T. 2015. Resource convertibility and ordered commutative monoids. *Mathematical Structures in Computer Science*, **10**, 1–89.
- Fuchs C. A. 2002. Quantum mechanics as quantum information (and only a little more). arXiv: quant-ph/0205039.
- Fuchs C. A., Mermin N. D. and Schack R. 2014. An introduction to QBism with an application to the locality of quantum mechanics. *American Journal of Physics*, **82**, 749–754. arXiv:1311.5253.
- Ghirardi G.-C., Rimini A. and Weber T. 1980. A general argument against superluminal transmission through the quantum mechanical measurement process. *Lettere Al Nuovo Cimento*, **27** (10), 293–298.
- Gilbreth F. B. and Gilbreth L. M. 1922. Process charts and their place in management. *Mechanical engineering*, **70**, 38–41.
- Girard J.-Y. 1989. Towards a geometry of interaction. *Contemporary Mathematics*, **92**, 69–108.
- Gleason A. M. 1957. Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics*, **6**, 885–893.
- Gogioso S. 2015a. A bestiary of sets and relations. arXiv:1506.05025.
- Gogioso S. 2015b. Categorical semantics for Schrödinger's equation. arXiv:1501.06489.
- Gogioso S. 2015c. Monadic dynamics. arXiv:1501.04921.
- Gogioso S. and Genovese F. 2016. Infinite-dimensional categorical quantum mechanics. In: *Proceedings of QPL*. arXiv:1605.04305.
- Gogioso S. and Kissinger A. 2016. Fully graphical treatment of the Hidden Subgroup Problem. Unpublished.
- Gogioso S. and Zeng W. 2015. Mermin non-locality in abstract process theories. arXiv: 1506.02675.

Gonthier G. 2008. The Four Colour Theorem: Engineering of a Formal Proof. Berlin and Heidelberg: Springer. Page 333.

Gonthier G., Asperti A., Avigad J., Bertot Y., Cohen C., Garillot F., Le Roux S., Mahboubi, A., O'Connor R., Biha S. O., et al. 2013. A machine-checked proof of the odd order theorem. Pages 163–179 of: Interactive Theorem Proving. Springer.

Gordon M. 2000. From LCF to HOL: a short history. Pages 169–186 of: Proof, Language, and Interaction.

Gordon M. J., Milner A. J. and Wadsworth C. P. 1979. Lecture Notes in Computer Science. Vol. 78. Berlin: Springer-Verlag.

Gottesman D. and Chuang I. L. 1999. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, **402** (6760), 390–393.

Gour G. and Spekkens R. W. 2008. The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics*, **10**, 033023.

Gour G., Müller M. P., Narasimhachar V., Spekkens R. W. and Younger Halpern N. 2013. The resource theory of informational nonequilibrium in thermodynamics. arXiv:1309.6586.

Greenberger D. M., Horne M. A., Shimony A. and Zeilinger A. 1990. Bell's theorem without inequalities. *American Journal of Physics*, **58**, 1131–1143.

Grefenstette E. and Sadrzadeh M. 2011. Experimental support for a categorical compositional distributional model of meaning. Pages 1394–1404 of: The 2014 Conference on Empirical Methods on Natural Language Processing. arXiv:1106.4058.

Gröblacher S., Paterek T., Kaltenbaek R. R., Brukner C., Żukowski M., Aspelmeyer M., and Zeilinger A. 2007. An experimental test of non-local realism. *Nature*, **446**, 871–875.

Grothendieck A. 1957. Sur quelques points d'algèbre homologique. *Tohoku Math J.*, 119–221.

Grover L. K. 1996. A fast quantum mechanical algorithm for database search. Pages 212–219 of: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. STOC '96. New York: ACM.

Hadzihanovic A. 2015. A diagrammatic axiomatisation for qubit entanglement. In: Proceedings of the 30th Annual IEEE Symposium on Logic in Computer Science (LICS). arXiv:1501.07082.

Hales T., Adams M., Bauer G., Dang D. T., Harrison J., Hoang T. L., Kaliszky C., Magron V., McLaughlin S., Nguyen T. T., et al. 2015. A formal proof of the Kepler conjecture. arXiv preprint arXiv:1501.02155.

Harding J. 2009. A link between quantum logic and categorical quantum mechanics. *International Journal of Theoretical Physics*, **48** (3), 769–802.

Hardy L. N.d. Disentangling nonlocality and teleportation. arXiv:quant-ph/9906123.

Hardy L. 2001. Quantum theory from five reasonable axioms. arXiv:quant-ph/0101012.

Hardy L. 2011. Foliabile operational structures for general probabilistic theories. Pages 409–442 of: Halvorson, H. (ed), Deep Beauty: Understanding the Quantum World through Mathematical Innovation. Cambridge University Press. arXiv:0912.4740.

Hardy L. 2012. The operator tensor formulation of quantum theory. arXiv:1201.4390.

Hardy L. 2013a. A formalism-local framework for general probabilistic theories, including quantum theory. *Mathematical Structures in Computer Science*, **23** (2), 339–440.

Hardy L. 2013b. On the theory of composition in physics. Pages 83–106 of: Computation, Logic, Games, and Quantum Foundations: The Many Facets of Samson Abramsky. Springer. arXiv:1303.1537.

Hardy L. and Spekkens R. W. 2010. Why physics needs quantum foundations. *Physics in Canada*, **66**, 73–76.

Hardy L. and Spekkens R. W. 2010. Einstein, incompleteness, and the epistemic view of quantum states. *Foundations of Physics*, **40**, 125–157.

Hasegawa M., Hofmann M., and Plotkin G. D. 2008. Finite dimensional vector spaces are complete for traced symmetric monoidal categories. Pages 367–385 of: Avron, A., Dershowitz N. and Rabinovich A. (eds), *Pillars of Computer Science. Lecture Notes in Computer Science*, vol. 4800. Springer.

Hedges J., Shpirts E., Winschel V. and Zahn P. 2016. Compositionality and string diagrams for game theory. arXiv:1604.06061.

Hein M., Eisert J. and Briegel H. J. 2004. Multiparty entanglement in graph states. *Physical Review A*, **69**, 062311.

Heisenberg W. 1925. Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen. Heisenberg (1925), **33**, 879–893.

Heisenberg W. 1930. *Die physikalischen Prinzipien der Quantentheorie*. Leipzig: S. Hirzel.

Hensen B., Bernien H., Dreau A. E., Reiserer A., Kalb N., Blok M. S., Ruitenberg J., Vermeulen R. F. L., Schouten R. N., Abellan C., Amaya W., Pruneri V., Mitchell M. W., Markham M., Twitchen D. J., Elkouss D., Wehner S., Taminiau T. H. and Hanson R. 2015. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, **526** (10), 682–686.

Henson J., Lal R. and Pusey M. F. 2014. Theory-independent limits on correlations from generalised Bayesian networks. arXiv:1405.2572.

Herrmann M. 2010. Models of multipartite entanglement. MSc Thesis, Oxford University.

Heunen C. and Jacobs B. 2010. Quantum logic in dagger kernel categories. *Order*, **27** (2), 177–212.

Heunen C. and Kissinger A. 2016. Can quantum theory be characterized in information-theoretic terms? arXiv:1604.05948.

Heunen C., Contreras I. and Cattaneo A. o S. 2012b. Relative Frobenius algebras are groupoids. *Journal of Pure and Applied Algebra*, **217**, 114–124.

Heunen C., Sadrzadeh M. and Grefenstette E. (eds). 2012a. *Quantum Physics and Linguistics: A Compositional, Diagrammatic Discourse*. Oxford University Press.

Hinze R. and Marsden D. 2016. Equational reasoning with lollipops, forks, cups, caps, snakes, and speedometers. *Journal of Logical and Algebraic Methods in Programming*.

Hoare C. A. R. and He J. 1987. The weakest prespecification. *Information Processing Letters*, **24**, 127–132.

Honda K. 2012. Graphical classification of entangled qutrits. *Electronic Proceedings in Theoretical Computer Science*, **95**, 123–141.

Horodecki M., Oppenheim J. and Horodecki R. 2002. Are the laws of entanglement theory thermodynamical? *Physical Review Letters*, **89**, 240403.

Horodecki M., Horodecki P. and Oppenheim J. 2003. Reversible transformations from pure to mixed states and the unique measure of information. *Physical Review A*, **67**, 062104.

Horodecki R., Horodecki P., Horodecki M. and Horodecki K. 2009. Quantum entanglement. *Reviews of Modern Physics*, **81**, 865–942. arXiv:quant-ph/0702225.

Horsman C. 2011. Quantum picturalism for topological cluster-state computing. *New Journal of Physics*, **13**, 095011. arXiv:1101.4722.

- Jacobs B. 2010. Orthomodular lattices, Foulis semigroups and Dagger kernel categories. *Logical Methods in Computer Science*, **6** (2), 1.
- Jamiołkowski A. 1972. Linear transformations which preserve trace and positive semi-definiteness of operators. *Reports on Mathematical Physics*, **3**, 275–278.
- Jammer M. 1974. *The Philosophy of Quantum Mechanics*. John Wiley & Sons.
- Jauch J. M. 1968. *Mathematical Foundations of Quantum Mechanics*. Addison-Wesley.
- Jauch J. M. and Piron C. 1963. Can hidden variables be excluded in quantum mechanics? *Helvetica Physics Acta*, **36**, 827–837.
- Johansson M., Dixon L. and Bundy A. 2011. Conjecture synthesis for inductive theories. *Journal of Automated Reasoning*, **47**, 251–289.
- Jones J. A., Mosca M. and Hansen R. H. 1998. Implementation of a quantum search algorithm on a quantum computer. *Nature*, **393** (6683), 344–346.
- Jones V. F. R. 1985. A polynomial invariant for knots via von Neumann algebras. *Bulletin of the American Mathematical Society*, **12**, 103–111.
- Joyal A. and Street R. 1991. The geometry of tensor calculus I. *Advances in Mathematics*, **88**, 55–112.
- Joyal A., Street R. and Verity D. 1996. Traced monoidal categories. Pages 447–468 of: *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 119. Cambridge University Press.
- Jozsa R. 1997. Quantum algorithms and the Fourier transform. In: *Proceedings of the Santa Barbara Conference on Coherence and Decoherence*. Proceedings of the Royal Society of London.
- Kartsaklis D. and Sadrzadeh M. 2013. Prior disambiguation of word tensors for constructing sentence vectors. Pages 1590–1601 of: *The 2013 Conference on Empirical Methods on Natural Language Processing*. ACL.
- Kassel C. 1995. *Quantum Groups*. Vol. 155. Springer.
- Kauffman L. H. 1987. State models and the Jones polynomial. *Topology*, **26**, 395–407.
- Kauffman L. H. 1991. *Knots and Physics*. World Scientific.
- Kauffman L. H. 2005. Teleportation topology. *Optics and Spectroscopy*, **99**, 227–232.
- Kelly G. M. 1972. Many-variable functorial calculus I. Pages 66–105 of: Kelly G. M., Laplaza M., Lewis G. and Mac Lane S. (eds), *Coherence in Categories*. Lecture Notes in Mathematics, vol. 281. Springer-Verlag.
- Kelly G. M. and Laplaza M. L. 1980. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, **19**, 193–213.
- Kissinger A. 2012a. Pictures of processes: automated graph rewriting for monoidal categories and applications to quantum computing. PhD thesis, University of Oxford.
- Kissinger A. 2012b. Synthesising graphical theories. arXiv:1202.6079.
- Kissinger A. 2014a. Abstract tensor systems as monoidal categories. In: Casadio C., Coecke B., Moortgat M. and Scott P. (eds), *Categories and Types in Logic, Language, and Physics: Festschrift on the Occasion of Jim Lambek's 90th Birthday*. Lecture Notes in Computer Science, vol. 8222. Springer. arXiv:1308.3586.
- Kissinger A. 2014b. Finite matrices are complete for (dagger-)hypergraph categories. arXiv:1406.5942 [math.CT].
- Kissinger A. and Zamdzhiev V. 2015. Quantomatic: a proof assistant for diagrammatic reasoning. arXiv:1503.01034.
- Kissinger A., Merry A. and Soloviev M. 2014. Pattern graph rewrite systems. Pages 54–66 of: Löwe B. and Winskel G. (eds), *Proceedings 8th International Workshop on De-*

velopments in Computational Models. Electronic Proceedings in Theoretical Computer Science, vol. 143. Open Publishing Association.

Kochen S. and Specker E. P. 1967. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, **17** (1), 59–87.

Kock J. 2004. Frobenius Algebras and 2D Topological Quantum Field Theories. Vol. 59. Cambridge University Press.

Kraus K. 1983. States, Effects and Operations. Springer.

Lack S. 2004. Composing PROPs. *Theory and Applications of Categories*, **13**, 147–163.

Laforest M., Baugh J. and Laflamme R. 2006. Time-reversal formalism applied to maximal bipartite entanglement: theoretical and experimental exploration. *Physical Review A*, **73** (3), 032323.

Lamata L., Léon J., Salgado D. and Solano E. 2007. Inductive entanglement classification of four qubits under stochastic local operations and classical communication. *Physical Review A*, **75**, 022318.

Lambek J. and Scott P. J. 1988. Introduction to Higher-Order Categorical Logic. Cambridge University Press.

Leinster T. 2004. Higher Operads, Higher Categories. Cambridge University Press.

Lemmens P. W. H. and Seidel J. J. 1973. Equiangular lines. *Journal of Algebra*, **24** (3), 494–512.

Lloyd S., Maccone L., Garcia-Patron R., Giovannetti V., Shikano Y., Pirandola S., Roze-ma L. A., Darabi A., Soudagar Y., Shalm L. K. and Steinberg A. M. 2011. Closed timelike curves via postselection: theory and experimental test of consistency. *Physical Review Letters*, **106** (4), 040403.

Lo H.-K. and Popescu S. 2001. Concentrating entanglement by local actions: beyond mean values. *Physical Review A*, **63**, 022301.

Ludwig G. 1985. An Axiomatic Basis of Quantum Mechanics, volume 1: *Derivation of Hilbert Space*. Springer-Verlag.

Mac Lane S. 1950. Duality for groups. *Bull. Am. Math. Soc.*, **56**, 485–516.

Mac Lane S. 1963. Natural associativity and commutativity. *The Rice University Studies*, **49** (4), 28–46.

Mac Lane S. 1998. Categories for the Working Mathematician. Springer-Verlag.

Mackey G. W. 1963. The Mathematical Foundations of Quantum Mechanics. New York: W. A. Benjamin.

Macrakis K. 1993. Surviving the Swastika: Scientific Research in Nazi Germany. Oxford University Press.

Majid S. 2000. Foundations of Quantum Group Theory. Cambridge University Press.

Manin Y. I. 1980. Vychislimoe i Nevychislimoe. Sovetskoye Radio.

Markopoulou F. 2000. Quantum causal histories. *Classical and Quantum Gravity*, **17** (10), 2059.

Marvian I. and Spekkens R. W. 2013. The theory of manipulations of pure state asymmetry: I. Basic tools, equivalence classes and single copy transformations. *New Journal of Physics*, **15** (3), 033001.

Mehra J. 1994. The Beat of a Different Drum: The Life and Science of Richard Feynman. Clarendon Press.

Mellies P.-A. 2012. Game semantics in string diagrams. Pages 481–490 of: Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science (LICS). IEEE Computer Society.

- Mermin N. D. 1990. Quantum mysteries revisited. *American Journal of Physics*, **58** (Aug.), 731–734.
- Mermin N. D. April 1989. What's wrong with this pillow? *Physics Today*.
- Mermin N. D. May 2004. Could Feynman have said this? *Physics Today*.
- Milner R. 1972. Logic for computable functions; description of a machine implementation. Tech. rept. STAN-CS-72-288. Stanford University.
- Montanaro A. 2015. Quantum algorithms: an overview. arXiv:1511.04206.
- Moore D. J. 1995. Categories of representations of physical systems. *Helvetica Physica Acta*, **68**, 658–678.
- Moore D. J. 1999. On state spaces and property lattices. *Studies in History and Philosophy of Modern Physics*, **30** (1), 61–83.
- Muirhead R. F. 1903. Some methods applicable to identities and inequalities of symmetric algebraic functions of n letters. *Proceedings of the Edinburgh Mathematical Society*, **21**, 144–157.
- Neumark M. A. 1943. On spectral functions of a symmetric operator. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, **7** (6), 285–296.
- Nielsen M. A. 1999. Conditions for a class of entanglement transformations. *Physical Review Letters*, **83** (2), 436–439.
- Nielsen M. A. and Chuang I. L. 2010. *Quantum Computation and Quantum Information*. Cambridge University Press.
- Ozawa M. 1984. Quantum measuring processes of continuous observables. *Journal of Mathematical Physics*, **25** (1), 79–87.
- Pan J.-W., Bouwmeester D., Daniell M., Weinfurter H. and Zeilinger A. 2000. Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. *Nature*, **403**, 515–519.
- Panangaden P. and Paquette É. O. 2011. A categorical presentation of quantum computation with anyons. Pages 983–1025 of: Coecke, B. (ed), *New Structures for Physics*. Lecture Notes in Physics. Springer.
- Paquette É. O. 2008. Categorical quantum computation. PhD thesis, University of Montreal.
- Paulsen V. 2002. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press.
- Paulson L., et al. 1986. Isabelle theorem prover. <https://isabelle.in.tum.de/>.
- Pavlovic D. 2009. Quantum and classical structures in nondeterministic computation. Pages 143–157 of: Proceedings of the 3rd International Symposium on Quantum Interaction. QI'09. Berlin and Heidelberg: Springer-Verlag.
- Pavlovic D. 2013. Monoidal computer I: basic computability by string diagrams. *Information and Computation*, **226**, 94–116.
- Pearl J. 2000. *Causality: Models, Reasoning and Inference*. Cambridge University Press.
- Penrose R. 1971. Applications of negative dimensional tensors. Pages 221–244 of: *Combinatorial Mathematics and Its Applications*. Academic Press.
- Penrose R. 1984. *Spinors and Spacetime*, vol. 1. Cambridge University Press.
- Penrose R. 2004. *The Road to Reality: A Complete Guide to the Physical Universe*. Jonathan Cape.
- Perdrix S. 2005. State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, **3** (1), 219–223.
- Perdrix S. and Wang Q. 2015. The ZX calculus is incomplete for Clifford+T quantum mechanics. arXiv:1506.03055.

- Piedeleu R., Kartsaklis D., Coecke B. and Sadrzadeh M. 2015. Open system categorical quantum semantics in natural language processing. In: CALCO 2015. arXiv:1502.00831.
- Pierce B. C. 1991. Basic Category Theory for Computer Scientists. MIT Press.
- Piron C. 1976. Foundations of Quantum Physics. W. A. Benjamin.
- Piron C. 1964. Axiomatique quantique. *Helvetica Physica Acta*, **37**, 439–468.
- Planck M. 1900. Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum. *Verhandlungen der Deutschen Physikalischen Gesellschaft*, **2**, 237–245.
- Poincaré H. 1902. La science et l'hypothèse. Flammarion.
- Pusey M. F., Barrett J. and Rudolph T. 2012. On the reality of the quantum state. *Nature Physics*, **8** (6), 475–478.
- Ranchin A. and Coecke B. 2014. Complete set of circuit equations for stabilizer quantum mechanics. *Physical Review A*, **90**, 012109.
- Rauch H., Zeilinger A., Badurek G., Wilfing A., Bauspiess W. and Bonse U. 1975. Verification of coherent spinor rotation of fermions. *Physics Letters A*, **54**, 425–427.
- Raussendorf R. and Briegel H. J. 2001. A one-way quantum computer. *Physical Review Letters*, **86**, 5188.
- Raussendorf R., Browne D. E. and Briegel H. J. 2003. Measurement-based quantum computation on cluster states. *Physical Review A*, **68** (2), 22312.
- Raussendorf R., Harrington J. and Goyal K. 2007. Topological fault-tolerance in cluster state quantum computation. *New Journal of Physics*, **9**, 199.
- Redei M. 1996. Why John von Neumann did not like the Hilbert space formalism of quantum mechanics (and what he liked instead). *Studies in History and Philosophy of Modern Physics*, **27** (4), 493–510.
- Redhead M. 1987. Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics. Clarendon Press.
- Rickles D. 2007. Symmetry, Structure, and Spacetime. Elsevier.
- Roddenberry G. 1966. Star Trek (television series). NBC.
- Rowe M. A., Kielpinski D., Meyer V., Sackett C. A., Itano W. M., Monroe C. and Wineland D. J. 2001. Experimental violation of a Bell's inequality with efficient detection. *Nature*, **409**, 791–794.
- Sadrzadeh M., Clark S. and Coecke B. 2013. The Frobenius anatomy of word meanings I: subject and object relative pronouns. *Journal of Logic and Computation*, **23**, 1293–1317. arXiv:1404.5278.
- Sadrzadeh M., Clark S. and Coecke B. 2014. The Frobenius anatomy of word meanings II: possessive relative pronouns. *Journal of Logic and Computation*, exu027.
- Schröder de Witt C. and Zamdzhiev V. 2014. The ZX calculus is incomplete for quantum mechanics. arXiv:1404.3633.
- Schrödinger E. 1926. An undulatory theory of the mechanics of atoms and molecules. *Physical Review Letters*, **28** (6), 1049–1070.
- Schrödinger E. 1935. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, **23**, 823–828.
- Schrödinger E. 1935. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, **31**, 555–563.
- Schumacher B. 1995. Quantum coding. *Physical Review A*, **51**, 2738.
- Schwinger J. 1960. Unitary operator bases. *Proceedings of the National Academy of Sciences of the U.S.A.*, **46**, 570–579.
- Scott D. S. 1993. A type-theoretical alternative to ISWIM, CUCH, OWHY. *Theoretical Computer Science*, **121** (1), 411–440.

Selinger P. 2007. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, **170**, 139–163.

Selinger P. 2011a. Finite dimensional Hilbert spaces are complete for dagger compact closed categories (extended abstract). *Electronic Notes in Theoretical Computer Science*, **270** (1), 113–119.

Selinger P. 2011b. A survey of graphical languages for monoidal categories. Pages 275–337 of: Coecke, B. (ed), *New Structures for Physics. Lecture Notes in Physics*. Springer-Verlag. arXiv:0908.3347.

Selinger P. 2015. Generators and relations for n-qubit Clifford operators. *Logical Methods in Computer Science*, **11**.

Shannon C. E. 1948. A mathematical theory of communication. *The Bell System Technical Journal*, **27**, 379–423.

Shende V. V., Bullock S. S. and Markov I. L. 2006. Synthesis of quantum-logic circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **25** (6), 1000–1010.

Shor P. W. 1994. Algorithms for quantum computation: discrete logarithms and factoring. Pages 124–134 of: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE.

Shor P. W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, **26** (5), 1484–1509.

Shulman M., et al. 2013. Homotopy type theory: univalent foundations of mathematics. <https://homotopytypetheory.org/book/>.

Simon D. R. 1997. On the power of quantum computation. *SIAM Journal on Computing*, **26** (5), 1474–1483.

Sobocinski P. 2015. Graphical linear algebra. <http://graphicallinearalgebra.net>.

Spekkens R. W. 2007. Evidence for the epistemic view of quantum states: a toy theory. *Physical Review A*, **75** (3), 032110.

Stay M. and Vicary J. 2013. Bicategorical semantics for nondeterministic computation. *Electronic Notes in Theoretical Computer Science*, **298**, 367–382. arXiv:1301.3393.

Stinespring W. F. 1955. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, **6** (2), 211–216.

Street R. 2007. *Quantum Groups: A Path to Current Algebra*. Cambridge University Press.

Stubbe I. and van Steirteghem B. 2007. Propositional systems, Hilbert lattices and generalized Hilbert spaces. Pages 477–524 of: Gabbay D., Lehmann D. and Engesser K. (eds), *Handbook Quantum Logic*. Elsevier Publ.

Sudarshan E. C. G., Mathews P. M. and Rau J. 1961. Stochastic dynamics of quantum-mechanical systems. *Physical Review*, **121** (3), 920.

Svetlichny G. 2009. Effective quantum time travel. arXiv:0902.4898.

Tull S. 2016. Operational theories of physics as categories. arXiv:1602.06284.

Turing A. M. 1937. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, **42**, 230–265.

Van den Nest M., Dehaene J. and De Moor B. 2004. Graphical description of the action of local Clifford transformations on graph states. *Physical Review A*, **69** (2), 9422.

Verstraete F., Dehaene J., De Moor B. and Verschelde H. 2002. Four qubits can be entangled in nine different ways. *Physical Review A*, **65** (052112). arXiv:quant-ph/0109033.

Vicary J. 2011. Categorical formulation of finite-dimensional quantum algebras. *Communications in Mathematical Physics*, **304** (3), 765–796.

Vicary J. 2013. The topology of quantum algorithms. Pages 93–102 of: *Proceedings of the 28th Annual IEEE Symposium on Logic in Computer Science (LICS)*. IEEE Computer Society.

Von Neumann J. 1927a. Thermodynamik quantenmechanischer Gesamtheiten. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, **1**, 273–291.

Von Neumann J. 1927b. Wahrscheinlichkeitstheoretischer aufbau der quantenmechanik. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, **1**, 245–272.

Von Neumann J. 1932. *Mathematische Grundlagen der quantenmechanik*. Springer-Verlag. Translation, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, 1955.

Walther P., Resch K. J., Rudolph T., Schenck E., Weinfurter H., Vedral V., Aspelmeyer M. and Zeilinger A. 2005. Experimental one-way quantum computing. *Nature*, **434**, 169–176.

Wedderburn J. H. M. 1906. On a theorem in hypercomplex numbers. *Proceedings of the Royal Society of Edinburgh*, **26**, 48–50.

Weih's G., Jennewein T., Simon C., Weinfurter H. and Zeilinger A. n. 1998. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, **81**, 5039.

Werner R. F. 2001. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, **34** (35), 7081.

Whitehead A. N. 1957. *Process and Reality*. Harper & Row.

Wigner E. P. 1931. *Gruppentheorie und ihre Anwendung auf die Quanten mechanik der Atomspektren*. Friedrich Vieweg und Sohn.

Wigner E. P. 1995a. *Remarks on the Mind-Body Question*. Springer. Pages 247–260.

Wigner E. P. 1995b. The unreasonable effectiveness of mathematics in the natural sciences. Pages 534–549 of: *Philosophical Reflections and Syntheses*. Springer.

Wilce A. 2000. Test spaces and orthoalgebras. Pages 81–114 of: Coecke B., Moore D. J. and Wilce A. (eds), *Current Research in Operational Quantum Logic: Algebras, Categories and Languages*. *Fundamental Theories of Physics*, vol. 111. Springer.

Wittgenstein L. 1953. *Philosophical Investigations*. Basil & Blackwell.

Wood C. J. and Spekkens R. W. 2012. The lesson of causal discovery algorithms for quantum correlations: causal explanations of Bell-inequality violations require fine-tuning. arXiv:1208.4119.

Wootters W. and Zurek W. 1982. A single quantum cannot be cloned. *Nature*, **299**, 802–803.

Zeilinger A. 1999. Experiment and the foundations of quantum physics. *Reviews of Modern Physics*, **71**, S288.

Zeng W. 2015. *The abstract structure of quantum algorithms*. PhD thesis, University of Oxford. arXiv:1512.08062.

Zeng W. and Vicary J. 2014. *Abstract structure of unitary oracles for quantum algorithms*. arXiv:1406.1278.

Zukowski M., Zeilinger A., Horne M. A. and Ekert A. K. 1993. «Event-ready-detectors» Bell experiment via entanglement swapping. *Physical Review Letters*, **71**, 4287–4290.

Предметный указатель

С

CP*, 544
CPM-построение, 373, 378
C*-алгебра, 542
 квантовая, 542

L

LOCC-максимальность, 151, 821

P

PROP, 667, 669

S

SIC-POVM-измерение, 425
SLOCC, 822
SLOCC-максимальность, 150

W

W-состояние, 826

X

X_α -измерение, 770
X-базис, 242

Z

ZX-диаграмма, 626
ZX-исчисление, 633
 Y-правило, 632
 л-коммутирование, 636
 л-копирование, 639
 изменение цвета, 645
 правило $\pi/2$ -дополнительности, 639
 правило локальной
 дополнительности, 650
 эквивалентное представление, 644
Z-базис, 238
Z-измерение, 771

A

Абстрактная тензорная система, 94, 169
Автоматизированные рассуждения, 842
 стратегия доказывания, 847
Адамара произведение, 471
Адьюнкция, 124
 интерпретация, 125
 линейно-алгебраическое сопряжение, 129
 матрица, 190
Аксиома локальной
 взаимозаменяемости, 840
Алгебра, 60, 471, 538
 ассоциативность, 471

 коммутативная, 541
 коммутативность, 471
 унитальность, 471
Алгебраический и диаграммный языки, 67
Алгоритм, 726
Ансамбли, 336
Антипаук, 829, 853
Антипод, 661
Антиунитарное отображение, 388

Б

Базис, 181
Базис произведения, 215
Байесовская инверсия, 474
Байесовский вывод, 399, 433
Белла базис, 246
 измерение, 365, 397
 невозмущающее, 402
 корректировка, 366
 матрицы, 248
 неравенство, 594
 отображения, 247
 состояние и эффект, 112, 503
Белла–Кохена–Спекера теорема, 434
Бесконтекстность, 434
Бесплатный процесс, 790
Биалгебра, 608, 661
 матрица путей, 665
Бит, 18, 481
Битовые строки, 71, 481
Блоки и провода, 46
Блокнот одноразового использования, 163
Блоха
 сфера, 289
 шар, 334
Борна правило, 80
 обобщенное, 80
Бэнг-блок, 851

В

Веддербёрна теорема, 541
Вентили
 AND, 238
 CNOT, 239, 295
 CX(α), 736
 CZ(α), 735
 NOT, 239, 294, 614
 T, 653
 XOR, 239
Адамара, 244, 295, 643

квантовый, 294
 Тоффоли, 739
 фазовый, 295, 566
 Вес, 314
 Взаимно несмещенные ОНБ, 577
 максимальные множества, 579
 Вигнера
 друг, 433
 теорема, 388
 Внутреннее произведение, 134
 Гильберта–Шмидта, 249
 Вполне положительное отображение, 323
 Вывод, 844
 Выполнимости проблема, 746
 Выпуклая комбинация. См. Смесь
 Высокоуровневый язык, 25
 Вычисление, 726
 Вычитание, 196

Г

Гейзенберга картина, 390
 Гильбертово пространство, 227
 бесконечномерное, 267
 теоретико-множественное
 определение, 254
 Глобальная фаза, 283, 287
 Грамматика, 376
 Графическое исчисление, 624
 Графовое состояние, 645, 767
 в спек-теории, 721
 квантовое, 769
 кирпичная кладка, 779
 кластерное состояние, 770
 Гровера алгоритм, 760
 Группа, 563
 генераторы, 765
 гомоморфизм, 617
 групповая операция, 563
 действие, 617
 единица, 563
 коммутативная, 563
 обратный элемент, 563
 циклическая, 623
 Группа круга $U(1)$, 565
 Групповая алгебра, 662
 Группоид, 544
 ГХЦ-состояние, 503
 обобщенное, 503

Д

Дважды стохастическое отображение, 801
 Двойственность процессов и состояний, 107
 Двойственный тип, 170

Двухкомпонентное состояние, 104
 Двухщелевой эксперимент, 394
 Де Бройля–Бома теория, 702
 Декартово произведение, 71
 Декогеренция, 404, 497
 время, 502
 декогерентное состояние, 499
 частичная, 501
 Декомпозиция, 65
 Деполяризующий канал, 798
 Диагонализация, 208
 Диаграмма, 47
 важны только соединения, 52
 подстановка, 59
 равенство, 55
 формула, 54
 Дилатация, теорема Наймарка, 361, 419
 Дирака нотация, 88
 Додо

квантовый, 18
 классический, 31
 Дойча–Йожи алгоритм, 750
 Доказыватель теорем, 842
 Дополнительные углы, 639
 Дополнительный паук, 571
 Дублирование, 283, 372

Е

Единичная матрица, 199
 Естественный изоморфизм, 274

З

Задача
 о скрытой подгруппе, 624, 760
 поиска, 756
 с предположением, 750
 Запутанное состояние, 296, 512
 Значения в контексте (Витгенштейн), 434

И

Измерение, 303
 POVM, 416
 возмущающие, 385
 исход, 385
 коллапс, 402
 коммутирующие фон Неймана, 415
 невозмущающие, 390
 обратное действие, 399
 ОНБ, 356, 385
 фон Неймана, 408
 Изометрия, 138
 Интерпретация квантовой теории, 433
 многомировая, 433
 Интерпретация $[[\]]$, 251, 443

К

Канонические соотношения
 коммутирования, 616
 Каузальность
 каузальное квантовое отображение, 324
 каузальное квантовое состояние, 314
 каузальное КК-отображение, 458
 квантовый процесс, 352
 Квадрат нормы, 135
 нечистота, 316
 Квант, 377
 Квантовая гравитация, 30
 Квантовая группа, 662
 Квантовая интерференция, 394
 Квантовая логика, 416, 435
 Квантовая машина Тьюринга, 786
 Квантовая нелокальность, 701
 Квантовая схема, 295
 Квантовая теория информации, 807
 Квантовое графовое состояние, 645
 Квантовое распределение ключей, 591
 Квантовое состояние, 311
 Квантовые отображения, 80, 319
 Квантовый байесианизм, 439
 Квантовый оракул, 585, 749
 опрос, 754
 Квантовый пикторализм, 30, 102
 Квантовый повторитель, 405
 Квантовый прибор, 378
 Квантовый процесс, 352, 365
 ветви и исходы, 352
 недетерминированный, 352
 управляемый, 363
 Квартеты блоков, 130
 Классическая корреляция, 511
 Классическая подгруппа, 611
 Классический провод, 283, 365
 Классический процесс, 461
 детерминированный, 463
 Классическое отображение, 461
 Классическое состояние
 возможность копирования, 464
 обратное, 473
 полный носитель, 474
 Клиффорда+Т диаграмма, 653
 приближительная универсальность, 653
 Клиффорда
 диаграмма, 630
 графовая форма, 647
 отображения, 624
 Коалгебра, 60, 539
 коассоциативная, 469
 коединица, 469

кокоммутативная, 469
 комоноидный гомоморфизм, 469
 коумножение, 469
 Кобордизм, 548
 Ковариантность, 349
 Коммутативная диаграмма, 274
 Комплексное число, 228
 комплексное сопряжение, 228
 положительная определенность, 230
 полярная форма, 229
 Композиция
 параллельная, 61
 последовательная, 62
 Копирование классических данных, 364
 Копирующий паук, 242
 Корреляция, 703
 Косинусно-синусное разложение, 744
 Крауса разложение, 331
 Кубит, 18, 237, 288
 Курс конвертации, 793

Л

Линейные отображения, 227
 Логика взаимодействия, 28
 Логический вентиль, 238
 Локальное дополнение, 647
 Локальные состояния, 349
 Локальные унитарные отображения
 Клиффорда, 646

М

Мажорирующий порядок, 800
 Максимально запутанное состояние, 151
 Маргинализация, 465
 Маргинальное распределение, 465
 Матрица, 188
 изометрического процесса, 204
 кронекеровское произведение, 218
 произведение, 213
 процессные теории матриц, 224
 смежности, 190
 столбцы, 203
 унитарного процесса, 205
 Матричное исчисление, 77, 213
 Мера
 аддитивная, 795
 супремальная, 796
 Множество, 70
 Модель
 квантовых вычислений, 727
 квантовых схем, 727
 универсальность, 738
 со скрытыми параметрами, 702

Модулярный закон, 440
 Моноидальная категория, 96
 инволютивная компактная замкнутая, 175
 когерентность, 98
 компактная замкнутая, 174
 симметричная, 97
 со следом, 99
 строгая, 96
 схемные диаграммы, 98

Н

Недетерминированность, 21
 Нелокальность, 23, 344, 702
 локальный реализм, 702
 сценарии ГХЦ–Мермина, 704
 Несигнальность, 345
 Несмещенное состояние, 552
 Несовместимое измерение, 589
 Нечистота, 312, 807
 Низкоуровневый язык, 25
 Нормальная форма, 601, 666
 Нормированное состояние ψ , 135
 Нулевое отношение, 85
 Нулевой процесс, 86

О

Обобщенная теория вероятностей, 708
 Обобщенное правило копирования, 477
 Обогащенная категория, 269
 Обращение времени, 156
 Огрубление, 409
 Односторонняя модель, 767
 Ожидаемое значение, 416
 Онтическое состояние, 722
 Онтологическая модель. См. Уточнение
 Оператор плотности, 287
 Операционный сценарий, 157
 Ориентированный ациклический граф, 65
 Ортонормированный базис, 183
 неединственность, 183
 самосопряженный, 190
 характеристика, 200
 Основанное на измерениях квантовое вычисление, 402, 645
 прямое распространение, 768, 772
 Отбрасывание, 283, 305, 307
 Отношения, 70
 неразделимость, 104
 нотация, 74
 параллельная композиция, 75
 последовательная композиция, 74
 состояния, эффекты и числа, 81
 сумма (объединение), 196

Отображение включения, 760
 Очищение, 320, 374
 совместное, 359

П

Парадигма LCF, 855
 Паук, 476
 гибридный, 504
 измеритель, 452
 изоморфизм, 833
 квантовый, 502
 классический, 502
 кодировщик, 452
 копирование, 475
 паучья диаграмма, 489
 слияние, 479
 сопоставление, 475
 удаление, 457, 475
 уравнения, 483
 фазовый, 558
 Паули матрицы. См. Белла матрицы
 Перекоммутация, 63
 Перекоммутация запутывания, 406, 525
 Перекрещенные чашки и крышки, 121
 Период функции, 766
 Планка
 постоянная, 377
 формула, 377
 Плотное кодирование, 524
 Подгруппа, аннулятор, 765
 Подсчет путей, 608
 Полная двудольная диаграмма, 606
 Полнота
 ZX-исчисления для спек-теории относительно спек-теории, 720
 ZX-исчисления относительно однокубитовых отображений Клиффорда+T, 654
 ZX-исчисления относительно отображений Клиффорда, 653
 паучьих диаграмм относительно линейных отображений, 491
 струнных диаграмм относительно линейных отображений, 251
 Полный порядок, 794
 Полный ранг (Шмидта), 150
 Положительное число, 230
 Положительность, 139
 \otimes -положительность, 142
 Положительный супероператор, 323
 Постоянная функция, 750
 Поток времени, 66
 Предпорядок, 791
 Предупорядоченный моноид, 792

- Причинно-следственная структура, 67
 Проблема измерения, 433
 Проектор, 143
 ортогональный, 409
 Простой провод, 63
 Пространственное разделение, 343
 Пространство-время, 342
 Процессная теория, 28, 49
 примеры, 50
 Процесс, определение, 46
 процессные равенства, 56
 Прямая сумма, 667
 Прямолинейная корреляция, 475
 Пустая система, 62
 Пуэзи–Барретта–Рудольфа теорема, 433
- Р**
 Разделимость, 104
 Размерность, 182
 теорема о, 182, 236
 это кружочек, 201
 Ранг, 824
 Распределение вероятностей, 202
 априорное, 472
 равномерное, 464
 совместное, 472
 точечное, 202
 условное, 472
 Распространение, 338, 470
 Распутанное состояние, 512
 Редуцированное отображение, 340, 496
 Редуцированное состояние, 308
 Рейхенбаха принцип, 703
 Реляционализм, 435
 Реляционное обращение, 128
 Ресурс, 787
 диаграмма конвертируемости, 825
 запутывания, 646
 класс эквивалентности, 825
 преобразование, 787
 Ресурсная теория, 337, 787
 количественно-подобная, 794
 невзаимодействующая, 794
 некаталитическая, 794
 Решетка, 435
 дистрибутивная, 435
 ортомодулярная, 437
- С**
 Самосопряженный процесс, 132
 Самотранспонированный процесс, 120
 Сбалансированная функция, 754
 Свертывание диаграмм, 504
 Световой конус, 344
- Свободная процессная теория, 56
 Семантика самого слабого
 предусловия, 440
 Сигнальность, 345
 Сильная дополнительность, 603
 обобщенное правило, 606, 852
 правило k - k' -коммутативности, 615
 правило k -исключения, 616
 правило k -копирования, 613
 правило k -копирования
 отображений, 614
 Симметричное информационно полное
 измерение, 424
 Сингулярное разложение, 486
 Синтез гипотез, 852
 Системный тип, 46
 Скрытые параметры, 434
 След, 122
 матрицы, 211
 цикличность, 123
 Слоение, 66, 349
 Смесь, 333
 Смешивание, 330, 333
 Собственное состояние, 208, 391
 Совместный системный тип, 62
 Сопряжение, 129
 Состояние, 78
 Спек-теория, 710
 ZX-исчисление, 718
 Спектр, 233
 Спектральная теорема, 231
 Спектральное разложение, 484
 Спин, 383
 Стохастическая матрица, 462
 Стохастическое отображение, 462
 С точностью до числа, \approx , 87
 Структура отбрасывания, 374
 Струнная диаграмма, 112
 логическое прочтение, 157
 Суммы, 192
 дистрибутивность, 193, 835
 замкнутость теории квантовых
 отображений, 332
 Суперпозиция, 302, 391
 Схемная диаграмма, 64
 характеристика, 65
 Схемная модель, 239
 Сценарии измерения, 703
 ГХЦ–Мермина, 704
- Т**
 Телепортация, 22
 квантовая, 361

классическая, 162
 с дополнительными измерениями, 594
 с классическими проводниками, 521
 со струнными диаграммами, 159
 Тензорная нотация, 189
 Теорема о невозможности, 147
 клонирования, 151, 154
 универсальной делимости, 147
 Теория
 относительности, 23, 342
 представлений, 483
 узлов, 271
 полиномом Джонса, 272
 Тип, 46
 Тожественность, 63
 Томография, 304, 421
 локальная, 426
 процессная, 427
 состояния, 421
 Транспонирование, 115
 алгебраическое, 122
 инволюция, 117
 матрицы, 190
 оператор, 172
 скользящие блоки, 118
 совместных систем, 120

У

Универсальное множество вентиляей, 566
 Унитарный процесс, 139
 мультиплексный, 738
 управляемый, 737
 Управляющий кубит, 731
 Упрощитель, 846
 Уравнения разгибания, 112
 Уточнение, 702

Ф

Фаза, 555
 Фазовое состояние, 554
 Фактор-группа, 761
 фактор-отображение, 761
 Фон Неймана
 алгебра, 440
 квантовый формализм, 413
 Фон Нейман, Джон, 22
 Фробениуса алгебра, 539
 бриджевая, 542
 инволютивная специальная, 539
 симметричная, 541
 Функции, 57, 70
 делимость, 104
 состояния, эффекты и числа, 81

Фурье базис, 557

Х

Хопфа алгебра, 661

Ч

Частичный порядок, 344, 791
 антисимметричность, 791
 Частичный след, 122
 Чашки и крышки, 110
 матричная форма, 221
 Четность
 нечетное состояние, 621
 обобщенное отображение четности, 622
 отображение, 620
 функция нечетности, 621
 функция четности, 620
 четное состояние, 620
 Число, 79
 коммутативный моноид, 80, 269
 Чистое квантовое отображение, 291
 Чистое квантовое состояние, 286
 Чистота, 807
 Чистый квантовый эффект, 286
 Чоя–Жамиловского изоморфизм, 110
 Чоя теорема, 360

Ш

Шмидта разложение. См. Сингулярное разложение
 Шмидта ранг. См. Ранг
 Шрёдингера
 картина, 390
 кот, 433
 Штерна–Герлаха прибор, 382
 Шумовое отображение, 336, 798
 Шура произведение, 471

Э

Эйлера углы, 627
 Эйлерово разложение, 627
 Эйнштейна, Подольского и Розена статья (ЭПР), 23
 Эквивалентность категорий, 226, 272
 Эквивалентные ресурсы, 791
 Экмана–Хилтона аргумент, 80
 Энтропия, 795
 фон Неймана, 806
 Шеннона, 806
 Эпистемическое состояние, 722
 Эффект, 78

Я

Язык спецификаций, 442

Книги издательства «ДМК Пресс» можно заказать в торгово-издательском холдинге «Планета Альянс» наложенным платежом, выслав открытку или письмо по почтовому адресу:
115487, г. Москва, 2-й Нагатинский пр-д, д. 6А.
При оформлении заказа следует указать адрес (полностью), по которому должны быть высланы книги; фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.
Эти книги вы можете заказать и в интернет-магазине: www.a-planeta.ru.
Оптовые закупки: тел. (499) 782-38-89.
Электронный адрес: books@alians-kniga.ru.

Боб Коке, Алекс Киссинджер

Изображение квантовых процессов

Начальный курс квантовой теории и рассуждений на диаграммах

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Перевод *Слинкина А. А.*
Корректор *Синяева Г. И.*
Верстка *Чаннова А. А.*
Дизайн обложки *Мовчан А. Г.*

Формат 70 × 100 1/16.

Гарнитура «PT Serif». Печать офсетная.

Усл. печ. л. 71,5. Тираж 200 экз.

Веб-сайт издательства: www.dmkpress.com