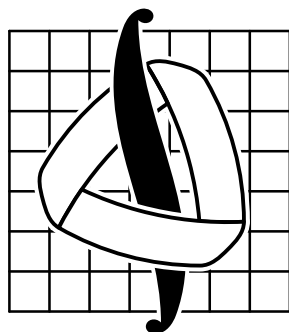


МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Курс лекций по логике и теории алгоритмов

Лектор — Валентин Борисович Шехтман

IV курс, 8 семестр, поток математиков

Москва, 2006 г.

Оглавление

1. Логика высказываний	4
1.1. Высказывания, формулы и правила вывода	4
1.1.1. Высказывания	4
1.1.2. Формулы	5
1.1.3. Аксиомы логики высказываний	5
1.1.4. Правило вывода	6
1.2. Корректность и полнота ИВ	6
1.2.1. Теорема корректности	6
1.2.2. Отступление об интуиционистской логике	6
1.2.3. Выводимость формулы. Подготовка к доказательству теоремы полноты	7
1.2.4. Путь к теореме полноты	8
1.2.5. Семантическая полнота и непротиворечивость теорий	8
1.2.6. Доказательство теоремы полноты CL	10
1.3. Интуиционистская логика	10
2. Логика предикатов	12
2.1. Построение языка первого порядка	12
2.1.1. Введение	12
2.1.2. Определения	12
2.1.3. Интерпретация сигнатуры. Модель. Оценки	13
2.1.4. Правила логики предикатов	15
2.1.5. Теорема корректности исчисления предикатов	17
2.1.6. Теорема корректности и теорема непротиворечивости для теорий первого порядка	18
2.1.7. Теории с равенством	19
2.2. Теории Хенкина	19
2.2.1. Экзистенциальная полнота	19
2.2.2. Свойство Хенкина	19
2.2.3. Вложение непротиворечивых теорий в полные теории Хенкина	19
2.3. Существование модели	21
2.3.1. Случай теории без равенства	21
2.3.2. Случай теории с равенством	22
2.4. Изоморфизм и элементарная эквивалентность интерпретаций	23
2.4.1. Определения и основные свойства	23
2.4.2. Сильная категоричность и счётная категоричность	24
3. Теория алгоритмов	25
3.1. Введение в системы Поста	25
3.1.1. Построение и примеры систем Поста	25
3.1.2. Подстановки и правила	26

Предисловие

Порядок изложения материала наиболее соответствует курсу 2006 г.
Фактических изменений начиная с 27 мая в тексте не было.

Благодарности

Огромное спасибо . . .

За поиск лажи выносятся благодарности . . .

Обозначения

- $A @ B$ — формулы, связанные любой из логических связок \vee , $\&$, \rightarrow .
- Если имеется k различных величин, обозначаемых, скажем, p_1, \dots, p_k , мы будем иногда использовать сокращенную запись \bar{p} , подразумевая всё множество $\{p_1, \dots, p_k\}$.

Последняя компиляция: 31 мая 2006 г.

Обновления документа — на сайтах <http://dmvn.mexmat.net>,

<http://dmvn.mexmat.ru>.

Об опечатках и неточностях пишите на dmvn@mccme.ru.

Литература

- [1] Н. К. Верещагин, А. Шень. *Лекции по математической логике и теории алгоритмов. Начала теории множеств*. М.: МЦНМО, 2000.
- [2] Н. К. Верещагин, А. Шень. *Лекции по математической логике и теории алгоритмов. Языки и исчисления*. М.: МЦНМО, 2000.
- [3] Н. К. Верещагин, А. Шень. *Лекции по математической логике и теории алгоритмов. Вычислимые функции*. М.: МЦНМО, 2000.
- [4] В. А. Успенский, Н. К. Верещагин, В. Е. Плиско. *Вводный курс математической логики*. М.: ФИЗМАТЛИТ, 2004

Введение: математика и компьютер

Из лжи следует истина.

Народная мудрость

В 30-е годы XX века была создана аксиоматика теории множеств Цермело–Френкеля (ZF). Когда стало ясно, что все математические доказательства можно записать с помощью формальных значков, а следствия из набора аксиом получать с помощью достаточно простых алгоритмических операций (которые легко можно поручить компьютеру), возник вопрос: а нельзя ли всю математику свести к компьютерным доказательствам?

Как выяснилось, на этом пути есть большая проблема. Компьютер способен получить миллионы правильных утверждений, но они будут нам совершенно неинтересны (когда мы сами пытаемся доказать теорему, мы уже знаем, что она нам интересна). А задача отделения полезных утверждений от миллионов правильных утверждений уже не является алгоритмической.

Ну ладно, допустим, что для этой цели компьютер (пока) непригоден. Предположим, однако, что мы хотим доказать какую-то теорему, но пока не умеем этого делать. Поручим компьютеру это задание, и он рано или поздно с этой задачей справится. Однако и здесь есть неприятности: мы получим формальный вывод, но он будет столь длинен, что мы не усвоим ничего полезного из этого доказательства. Хуже того, если теорема всё-таки неверна, то мы никогда этого не узнаем (ибо не существует алгоритма, который по формуле устанавливает, выводима она в данной аксиоматике или нет).

Ну хорошо, в таком случае остаётся надежда только на то, что компьютер можно использовать для проверки доказательств, написанных человеком. Это представляется наиболее реалистичным, однако пока не удалось найти разумного способа записывать доказательства на языке, понятном одновременно и человеку, и компьютеру.

1. Логика высказываний

Мы начнём с маленького фрагмента аксиоматической теории, а именно с исчисления высказываний (ИВ).

1.1. Высказывания, формулы и правила вывода

1.1.1. ВЫСКАЗЫВАНИЯ

Высказывание относится к одному из неопределяемых понятий и задаётся аксиоматически: это утверждение, которое может быть либо истинно, либо ложно.

Пример 1.1.

- «Число $2\sqrt{3}$ является иррациональным.» является истинным высказыванием.
- «Число x делится на 2.» не является высказыванием в полном смысле этого слова, потому что содержит свободную переменную x . Про него мы не можем сказать, истинно оно или ложно. Это так называемая высказывательная форма.
- «Верно ли, что сегодня очень холодно?» не является высказыванием.

Мы не будем интересоваться смыслом самих высказываний, нам будет важно только их истинностное значение. Мы будем обозначать высказывания латинскими буквами, например, p, p_2, \dots . Это так называемые пропозициональные переменные (от англ. *proposition* — высказывание).

Как и в русском языке, из нескольких высказываний можно образовывать более сложные высказывания. Например, можно объединять их союзами «И», «ИЛИ», «НЕ» и так далее. Так и для высказываний существуют логические связи.

Мы будем использовать символ «1» для обозначения того, что данное высказывание истинно, и символ «0» для обозначения ложных высказываний.

Если p — высказывание, то через $\neg p$ будем обозначать отрицание этого высказывания. Зададим его таблицей:

p	$\neg p$
0	1
1	0

Для отрицания ещё используется черта сверху: $\bar{p} = \neg p$.

Определим теперь значения логических связок «И» (называется конъюнкцией и обозначается & или \wedge), «ИЛИ» (называется дизъюнкцией и обозначается \vee). и «ЕСЛИ, ТО» (обозначается \rightarrow и называется импликацией).

p	q	$p \& q$	$p \vee q$	$p \rightarrow q$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

1.1.2. ФОРМУЛЫ

Конечно, одних только переменных нам будет мало. Мы будем из высказываний с помощью связок и скобок строить формулы. Определение даётся индуктивно:

Определение.

- Все высказывательные переменные являются формулами.
- Если P и Q — формулы, то $(P \& Q)$, $(P \vee Q)$, $(P \rightarrow Q)$ являются формулами.
- Если P — формула, то $\neg P$ — тоже формула.

Пример 1.2. Выражение $(\neg(P \& Q) \rightarrow R)$ является формулой, а $P \& Q$ — нет, потому что всякая формула, содержащая хотя бы одну конъюнкцию, содержит хотя бы пару скобок, а в этом выражении скобок нет совсем.

Замечание. Мы часто будем опускать внешние скобки. Кроме того, чтобы не писать лишних скобок, часто используется приоритетность выполнения операций: самой сильной является отрицание, затем следует конъюнкция, затем дизъюнкция и лишь потом — импликация.

Замечание. На первый взгляд не совсем понятно, почему импликация имеет такую таблицу истинности. Однако рассмотрим такое утверждение: «если x делится на 4, то x делится на 2». Оно истинно при всех значениях x . Рассмотрим два высказывания: пусть p обозначает высказывание « x делится на 4», а q обозначает « x делится на 2». Тогда наше тождественно истинное утверждение записывается как $p \rightarrow q$.

Рассмотрим различные значения x . Возьмём $x = 4$. Для него истинна и левая, и правая часть, стало быть, получается, что $1 \rightarrow 1 = 1$. Теперь возьмём x , равное 2. Для него истинна только правая часть, значит, $0 \rightarrow 1 = 1$. Теперь рассмотрим $x = 1$. Для него ложна и правая, и левая часть, значит, $0 \rightarrow 0 = 1$. Тем самым мы поняли, что хоть в каком-то смысле импликация определена «логично» и согласуется с интуитивными представлениями. Для полноты картины рассмотрим ложное высказывание «если x делится на 2, то x делится на 4». Подставляя $x = 2$, получаем, что $1 \rightarrow 0 = 0$, то есть из истины не следует ложь.

Замечание. Совершенно неочевидным фактом является то, что всякую формулу в ИВ можно однозначно «разобрать» на подформулы (теорема корректности, или, как её ещё называют, теорема о главном знаке).

Итак, у нас есть переменные, связки и формулы. Некоторые формулы замечательны тем, что они истинны при любых значениях переменных, входящих в них. Такие формулы называются тавтологиями. Они замечательны тем, что выражают законы логики. Введём для удобства ещё одну логическую связку, соответствующую языковой конструкции «РАВНОСИЛЬНО» или «ТОГДА И ТОЛЬКО ТОГДА». Она обозначается $p \leftrightarrow q$ и является сокращением для следующей формулы: $p \leftrightarrow q = (p \rightarrow q) \& (q \rightarrow p)$.

Пример 1.3. Это самый простой пример тавтологии: $p \rightarrow p$.

Пример 1.4. Законы де Моргана:

- 1) $((p \& q) \vee (p \& r)) \leftrightarrow (p \& (q \vee r))$;
- 2) $((p \vee q) \& (p \vee r)) \leftrightarrow (p \vee (q \& r))$.

Пример 1.5. Закон контрапозиции: $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$.

Пример 1.6. Законы поглощения:

- 1) $p \vee (p \& q) \leftrightarrow p$;
- 2) $p \& (p \vee q) \leftrightarrow p$.

Пример 1.7. Законы дистрибутивности:

- $$p \& (q \vee r) \leftrightarrow (p \& q) \vee (p \& r);$$
- $$p \vee (q \& r) \leftrightarrow (p \vee q) \& (p \vee r).$$

1.1.3. АКСИОМЫ ЛОГИКИ ВЫСКАЗЫВАНИЙ

Чтобы построить исчисление, нужно всегда задать набор аксиом.

Вот набор аксиом исчисления высказываний (ИВ):

1. $A \rightarrow (B \rightarrow A)$.
2. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.
3. $A \& B \rightarrow A$.
4. $A \& B \rightarrow B$.

5. $A \rightarrow (B \rightarrow A \& B)$.
6. $A \rightarrow (A \vee B)$.
7. $B \rightarrow (A \vee B)$.
8. $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$.
9. $\neg A \rightarrow (A \rightarrow B)$.
10. $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$.
11. $A \vee \neg A$.

На месте переменных A, B, C в этих аксиомах могут стоять любые формулы логики высказываний. Таким образом, у нас на самом деле имеется счётный набор аксиом, а здесь заданы фактически только их шаблоны.

1.1.4. ПРАВИЛО ВЫВОДА

Определение. Правило вывода (*modus ponens*, MP для краткости) — это правило $\frac{A, A \rightarrow B}{B}$, которое говорит, что если истинны формулы A и $A \rightarrow B$, то B тоже истинна.

Определение. Говорят, что формула A выводима в ИВ, если существует конечная последовательность формул A_1, \dots, A_n таких, что при всех i формула A_i либо является аксиомой, либо получена из каких-то предыдущих формул $\{A_1, \dots, A_{i-1}\}$ по правилу вывода (MP), и $A = A_n$.

Пример 1.8. Выведем формулу $(p \rightarrow p) \rightarrow (p \rightarrow p)$:

- Пишем аксиому 1, получаем $A_1 := p \rightarrow (p \rightarrow p)$.
- Пишем аксиому 2, получаем $A_2 := (p \rightarrow (p \rightarrow p)) \rightarrow ((p \rightarrow p) \rightarrow (p \rightarrow p))$.
- Выводим из A_1 и A_2 по правилу MP требуемую формулу.

1.2. Корректность и полнота ИВ

ИВ замечательно именно тем, что в нём все выводимые формулы истинны, и наоборот, любую истинную формулу можно вывести из аксиом. Сейчас мы приступим к доказательству этого факта. Сначала реализуем простую часть, а именно докажем теорему корректности вывода.

1.2.1. ТЕОРЕМА КОРРЕКТНОСТИ

Теорема 1.1 (Теорема о корректности вывода). *Все выводимые в ИВ формулы являются тавтологиями.*

□ Как это часто бывает в этой науке, доказательство похоже на доказательство по индукции. Сначала проверим базу.

1°. Нужно показать, что все аксиомы 1–11 являются тавтологиями. Это тривиальная, но довольно утомительная проверка, поэтому здесь мы не будем этого проделывать. Однако в этом рекомендуется убедиться самостоятельно¹.

2°. Пусть A — тавтология и $(A \rightarrow B)$ — тавтология. Допустим, что B не является тавтологией. Тогда существует такой набор переменных, что B ложна. Но A истинна всегда, поэтому мы получили такой набор переменных, что посылка A истинна, а заключение B ложно. Но тогда $A \rightarrow B$ ложно. Противоречие.

Поскольку мы можем получать новые формулы вывода только подстановкой выражений в аксиомы и по правилу вывода, то, отправляясь от тавтологий, вновь будем получать только тавтологии. ■

1.2.2. ОТСТУПЛЕНИЕ ОБ ИНТУИЦИОНИСТСКОЙ ЛОГИКЕ

Прежде, чем двигаться дальше, нужно сделать важное замечание об интуиционистской логике. Тот набор из 11 аксиом, который мы выписали, называется аксиомами классического исчисления высказываний, для которого мы будем использовать обозначение CL (*classic logic*).

Если отбросить самую последнюю аксиому, то мы получим исчисление ИЛ (*intuitive logic*). В нём предполагается, что когда мы говорим «верно A или верно B », то *знаем* про истинность и A , и B по отдельности.

Пример 2.1. Пусть A = «Гипотеза Римана верна». Мы ничего не знаем про то, верна ли гипотеза Римана, поэтому не знаем, истинно ли высказывание A . Однако в классической логике высказывание $A \vee \neg A$ является истинным (как говорят, третьего не дано — *tertium non datur* (TND) — либо верна, либо не верна). А вот в ИЛ, чтобы считать $A \vee \neg A$ истинным, нужно сначала установить истинность A или его отрицания.

Мы ещё вернёмся к интуиционистской логике, хотя и не будем забираться в неё очень глубоко.

¹Никто не запрещает для этой цели использовать компьютер, ему это вполне по силам! — *Прим. наб.*

1.2.3. ВЫВОДИМОСТЬ ФОРМУЛЫ. ПОДГОТОВКА К ДОКАЗАТЕЛЬСТВУ ТЕОРЕМЫ ПОЛНОТЫ

Обозначения. Для обозначения выводимости формулы A в исчислении Ω мы будем использовать значок $\vdash_{\Omega} A$. Значок $\vDash A$ означает, что формула A является тавтологией.

Замечание. Набор аксиом CL, оказывается, нельзя «проредить», то есть он обладает свойством минимальности. Здесь мы не будем этого доказывать.

В этом параграфе Ω будет обозначать одно из исчислений — CL или PL, поскольку мы не будем затрагивать последней аксиомы. Мы будем писать просто значок выводимости, не указывая всякий раз исчисление.

Определение. Пусть Γ — некоторое множество формул. Будем говорить, что формула выводима из множества Γ в исчислении Ω , если существует конечная последовательность формул A_1, \dots, A_n таких, что при всех i формула A_i либо является аксиомой, либо $A_i \in \Gamma$, либо получена из каких-то предыдущих формул $\{A_1, \dots, A_{i-1}\}$ по правилу вывода (MP), и $A = A_n$. Обозначение: $\Gamma \vdash_{\Omega} A$.

Лемма 1.2. $\vdash A \rightarrow A$.

□ Предъявим нужный нам вывод. Для краткости обозначим $B := A \rightarrow A$.

- 1) Аксиома 2: $[A \rightarrow (B \rightarrow A)] \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow A)]$.
- 2) Аксиома 1: $A \rightarrow (B \rightarrow A)$.
- 3) Из 1) и 2) выводим $(A \rightarrow B) \rightarrow (A \rightarrow A)$.
- 4) Аксиома 1: $A \rightarrow B = A \rightarrow (A \rightarrow A)$.
- 5) Из 3) и 4) выводим $B = A \rightarrow A$. ■

Теорема 1.3 (Теорема дедукции). Пусть Γ — множество формул. Тогда $\Gamma \cup \{A\} \vdash B$ тогда и только тогда, когда $\Gamma \vdash A \rightarrow B$.

□ Докажем сначала обратное утверждение, потому что оно проще. Допустим, что $A \rightarrow B$ выводима в Γ . Напишем этот вывод \mathcal{D} . Ясно, что он будет выводом и в $\Gamma \cup \{A\}$. Допишем к \mathcal{D} последовательно ещё две формулы: A и B . Это будет вывод формулы B в $\Gamma \cup \{A\}$, потому что B получается из двух предыдущих формул по правилу MP.

Теперь докажем прямое утверждение. Допустим, что $\Gamma, A \vdash B$. Докажем, что $\Gamma \vdash A \rightarrow B$. Будем вести индукцию по длине вывода формулы B из $\Gamma \cup \{A\}$.

0°. В случае, когда $B = A$, утверждение совпадает с утверждением предыдущей леммы.

1°. Пусть теперь B — аксиома Ω . У нас есть аксиомы $B \rightarrow (A \rightarrow B)$ и аксиома B . Из них по правилу MP выводим $A \rightarrow B$. Совершенно аналогично доказывается в том случае, когда $B \in \Gamma$ — в этом случае полученный вывод, конечно, будет выводом из Γ .

2°. Напишем вывод \mathcal{D} для B в системе $\Gamma \cup \{A\}$. Если B — не аксиома и не совпадает с A , то формула B получена из каких-то двух предыдущих формул в \mathcal{D} по правилу MP. Они, ясное дело, имеют вид C и $C \rightarrow B$, и выводы для них уже более короткие. Значит, к ним применимо предположение индукции. Получаем, что формулы $A \rightarrow C$ и $A \rightarrow (C \rightarrow B)$ выводимы в Γ . А коли так, напишем вывод в Γ для формулы B :

$$\begin{aligned} & \left. \begin{array}{c} \vdots \\ A \rightarrow C \end{array} \right\} \text{— вывод } A \rightarrow C, \\ & \left. \begin{array}{c} \vdots \\ A \rightarrow (C \rightarrow B) \end{array} \right\} \text{— вывод } A \rightarrow (C \rightarrow B), \\ & [A \rightarrow (C \rightarrow B)] \rightarrow [(A \rightarrow C) \rightarrow (A \rightarrow B)] \text{— аксиома 2,} \\ & (A \rightarrow C) \rightarrow (A \rightarrow B) \text{— MP,} \\ & A \rightarrow B \text{— MP.} \end{aligned} \tag{1}$$

Вот и всё. ■

Лемма 1.4 (Метод «От противного»). Если $\Gamma, A \vdash B$ и $\Gamma, A \vdash \neg B$, то $\Gamma \vdash \neg A$.

□ Напишем требуемый вывод в Γ :

$$\begin{aligned} & \left. \begin{array}{c} \vdots \\ A \rightarrow B \end{array} \right\} \text{— существует по теореме дедукции,} \\ & \left. \begin{array}{c} \vdots \\ A \rightarrow \neg B \end{array} \right\} \text{— существует по теореме дедукции,} \\ & (A \rightarrow B) \rightarrow [(A \rightarrow \neg B) \rightarrow \neg A] \text{— аксиома 10,} \\ & (A \rightarrow \neg B) \rightarrow \neg A \text{— MP,} \\ & \neg A \text{— MP,} \end{aligned} \tag{2}$$

и мы победили. ■

Лемма 1.5 (Метод разбора случаев). Если $\Gamma, A \vdash C$ и $\Gamma, B \vdash C$, то $\Gamma, A \vee B \vdash C$.

□ Напишем требуемый вывод в Γ :

$$\left. \begin{array}{c} \vdots \\ A \rightarrow C \end{array} \right\} \text{— существует по теореме дедукции,}$$

$$\left. \begin{array}{c} \vdots \\ B \rightarrow C \end{array} \right\} \text{— существует по теореме дедукции,} \quad (3)$$

$$(A \rightarrow C) \rightarrow [(B \rightarrow C) \rightarrow (A \vee B \rightarrow C)] \text{— аксиома 8,}$$

$$(B \rightarrow C) \rightarrow (A \vee B \rightarrow C) \text{— МР,}$$

$$A \vee B \rightarrow C \text{— МР,}$$

а теперь осталось применить теорему дедукции в обратную сторону. ■

Лемма 1.6. Имеют место утверждения

$$A, \neg B \vdash \neg(A \rightarrow B), \quad (4)$$

$$\neg A, \neg B \vdash \neg(A \vee B). \quad (5)$$

□ Очевидно, что $A, \neg B, A \rightarrow B \vdash B$ — достаточно одного МР. Ещё более очевидно, что $A, \neg B, A \rightarrow B \vdash \neg B$ — и выводить-то нечего. Применим метод «от противного» для полученных выводов, получим, что $A, \neg B \vdash \neg(A \rightarrow B)$, что и требовалось доказать.

Докажем второе утверждение. Очевидно, что $A, \neg B, A \vee B \vdash \neg B$ — выводить опять-таки нечего. Хотелось бы вывести отсюда же саму формулу B . Воспользуемся методом разбора случаев.

Ясно, что $\neg A, \neg B, B \vdash B$ — выводить снова нечего. Напишем теперь вывод для B из системы $\neg A, \neg B, A$.

$$\neg A,$$

$$A,$$

$$\neg A \rightarrow (A \rightarrow B) \text{— аксиома 9,} \quad (6)$$

$$A \rightarrow B \text{— МР,}$$

$$B \text{— МР,}$$

и дело в шляпе: применяем теперь метод разбора случаев к полученным выводам и получаем требуемое. ■

1.2.4. ПУТЬ К ТЕОРЕМЕ ПОЛНОТЫ

Мы постепенно переходим к доказательству теоремы полноты. Как и у всякой хорошей теоремы, у неё есть несколько различных доказательств.

Первый способ состоит в том, что сначала для каждой тавтологии A строится вывод $\vdash A \leftrightarrow A'$, где A' — СДНФ формулы A . Тавтологичность формулы A означает, что в СДНФ будут присутствовать все конъюнкции. Именно их-то мы и будем выводить.

Однако мы пойдём другим путём, а по дороге докажем кучу других полезных вещей. Для этого нам потребуются ввести несколько новых понятий.

1.2.5. СЕМАНТИЧЕСКАЯ ПОЛНОТА И НЕПРОТИВОРЕЧИВОСТЬ ТЕОРИЙ

Определение. Пропозициональная теория — произвольное множество пропозициональных формул.

Определение. Теория Γ называется противоречивой, если в ней можно вывести A и $\neg A$ одновременно. Если так сделать нельзя, то теория называется непротиворечивой.

Пример 2.2. Теория ИВ непротиворечива в силу теоремы корректности. Мы доказали, что из аксиом 1–11 можно выводить лишь тавтологии. А если A — тавтология, то $\neg A$ уж никак не может быть тавтологией, значит, её вывести нельзя.

Определение. Теория называется синтаксически полной, если для всякой формулы выводится либо A , либо $\neg A$.

Определение. Теория называется семантически полной, если в ней всякая тавтология выводима.

Лемма 1.7 (Свойства непротиворечивых синтаксически полных теорий). Пусть Γ — непротиворечивая синтаксически полная теория. Тогда

- 1°. $\Gamma \vdash \neg A$ тогда и только тогда, когда $\Gamma \not\vdash A$.
 2°. $\Gamma \vdash A \& B$ тогда и только тогда, когда $\Gamma \vdash A$ и $\Gamma \vdash B$.
 3°. $\Gamma \vdash A \vee B$ тогда и только тогда, когда $\Gamma \vdash A$ или $\Gamma \vdash B$.
 4°. $\Gamma \vdash A \rightarrow B$ тогда и только тогда, когда $\Gamma \not\vdash A$ или $\Gamma \vdash B$.

□ Ну что же, давайте доказывать по порядку. . .

1°. Сразу следует из определения непротиворечивой синтаксически полной теории.

2°. Пусть $A \& B$ выводима из Γ . Присоединим к этому выводу две аксиомы $A \& B \rightarrow A$ и $A \& B \rightarrow B$ и применим два раза МР.

Обратно, пусть у нас есть выводы для A и для B в отдельности. Тогда напомним аксиому $A \rightarrow (B \rightarrow A \& B)$. Из неё и формулы A выводим по правилу МР формулу $B \rightarrow A \& B$. Применяя МР второй раз, получаем вывод формулы $A \& B$, что и требовалось.

3°. Будем доказывать от противного. Допустим, что $\Gamma \not\vdash A$ и $\Gamma \not\vdash B$. Докажем, что $\Gamma \not\vdash A \vee B$. В самом деле, в силу полноты теории Γ , в ней выводимы $\neg A$ и $\neg B$. А из этих двух формул, как мы знаем, выводима формула $\neg(A \vee B)$ (лемма 1.6). А если она выводима, то, в силу непротиворечивости, $A \vee B$ не выводима, что и требуется.

Обратно, пусть выводима хотя бы одна из формул A или B . Напишем аксиому $A \rightarrow (A \vee B)$ и $B \rightarrow (A \vee B)$, после чего получим вывод для $A \vee B$ по правилу МР.

4°. Пусть сначала $\Gamma \not\vdash A$. Докажем, что $\Gamma \vdash A \rightarrow B$. Из полноты следует, что $\Gamma \vdash \neg A$, после чего, используя аксиому 9 ($\neg A \rightarrow (A \rightarrow B)$), получим $A \rightarrow B$ по правилу МР.

Если же $\Gamma \vdash B$, то $A \rightarrow B$ сразу выводится из B и аксиомы 1.

Прямое утверждение будем доказывать от противного. Допустим, что $\Gamma \vdash A$ и $\Gamma \not\vdash B$. Докажем, что $\Gamma \not\vdash A \rightarrow B$. В силу синтаксической полноты имеем $\Gamma \vdash \neg A$ и $\Gamma \vdash \neg B$. А мы знаем, что из этих двух формул по лемме 1.6 выводима формула $\neg(A \rightarrow B)$. Осталось воспользоваться непротиворечивостью теории. ■

Лемма 1.8 (Свойство противоречивых теорий). *Если теория противоречива, то в ней можно вывести всё, что угодно.*

□ Пусть $\Gamma \vdash A$ и $\Gamma \vdash \neg A$. Построим вывод для произвольной формулы B . Напишем аксиому 9: $\neg A \rightarrow (A \rightarrow B)$, из неё сразу выводим $A \rightarrow B$, а поскольку A тоже выведено, то по правилу МР получаем вывод для B . ■

Лемма 1.9 (Лемма Линденбаума). *Пусть Γ_0 — непротиворечивая теория. Тогда эту теорию можно синтаксически пополнить, то есть существует непротиворечивая синтаксически полная теория $\Gamma \supset \Gamma_0$.*

□ Перенумеруем все формулы: A_0, A_1, A_2, \dots . Это можно сделать, так как всякую формулу можно записать в $\text{T}\text{E}\text{X}^2$, используя конечный алфавит (если договориться, что имя переменной — это выделенный символ, снабжённый индексом, например, $P_{\{2147483647\}}$), а в конечном алфавите количество формул ограниченной длины конечно, поэтому всего их счётное множество.

Пусть теория Γ_n уже построена (и непротиворечива). Построим теорию $\Gamma_{n+1} \supset \Gamma_n$. Именно, положим

$$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{A_n\}, & \text{если эта теория непротиворечива;} \\ \Gamma_n \cup \{\neg A_n\} & \text{иначе.} \end{cases} \quad (7)$$

Покажем, что Γ_{n+1} непротиворечива. Допустим, что нам не повезло, и обе теории оказались противоречивыми. Как мы знаем из предыдущей леммы, в противоречивой теории можно вывести что угодно. Обозначим это «что угодно» через X . Тогда имеем $\Gamma_n, A_n \vdash X$ и $\Gamma_n, \neg A_n \vdash X$. Применяя лемму о разборе случаев, получаем, что $\Gamma_n, A_n \vee \neg A_n \vdash X$. Но $A_n \vee \neg A_n$ — вообще аксиома, поэтому её можно выкинуть. Значит, что угодно можно было вывести уже в Γ_n , это странно, потому что она была непротиворечива.

Итак, Γ_{n+1} непротиворечива. Теперь положим

$$\Gamma := \bigcup_{n=0}^{\infty} \Gamma_n. \quad (8)$$

Очевидно, что это синтаксически полная теория, потому что для каждой формулы в ней содержится либо она сама, либо её отрицание. Осталось доказать непротиворечивость Γ . Допустим, что нам опять не повезло, и Γ противоречива. Значит, есть вывод \mathcal{D}_1 в Γ для некоторой формулы X и вывод \mathcal{D}_2 в Γ для формулы $\neg X$. Заметим, что эти выводы содержат лишь конечное число формул, поэтому найдётся такое n , что $\mathcal{D}_1, \mathcal{D}_2 \subset \Gamma_n$. Но это означает, что Γ_n противоречива, а мы знаем, что все теории Γ_k непротиворечивы. Полученное противоречие доказывает теорему. ■

Замечание. Лемма Линденбаума — первое утверждение, в которой мы воспользовались последней аксиомой (TND), поэтому в $\mathbb{I}\mathbb{L}$ это доказательство не пройдёт.

²Как вы понимаете, про TEX лектор, конечно, не говорил, но подразумевал нечто в таком духе. — *Прим. наб.*

Лемма 1.10. $\vdash_{\text{CL}} \neg\neg A \rightarrow A$.

□ Очевидно, что $\neg\neg A, A \vdash A$. Далее, поскольку из противоречивой теории выводимо всё, что угодно, в частности, получаем, что $\neg\neg A, \neg A \vdash A$. В силу леммы о разборе случаев получаем $\neg\neg A, A \vee \neg A \vdash A$. Но формула $A \vee \neg A$ является аксиомой, и её можно убрать из вывода. Значит, $\neg\neg A \vdash A$. ■

1.2.6. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ПОЛНОТЫ CL

Теорема 1.11 (Теорема полноты CL). *Всякую тавтологию A можно вывести в CL.*

□ Будем доказывать от противного. Допустим, что $\not\vdash A$. Тогда теория $\Gamma_0 := \{\neg A\}$ непротиворечива. В самом деле, допустим, что $\neg A \vdash B$ и $\neg A \vdash \neg B$. Применяя лемму о методе «от противного», получаем $\vdash \neg\neg A$. По лемме 1.10 у нас есть вывод для $\neg\neg A \rightarrow A$. Применив МР, получаем вывод для A . Противоречие.

Итак, Γ_0 непротиворечива. Построим по лемме Линденбаума синтаксически полную непротиворечивую теорию $\Gamma \supset \Gamma_0$. Пусть p_1, p_2, \dots — все переменные. Зафиксируем значения переменных следующим образом: $|p_k| = 1$ тогда и только тогда, когда $\Gamma \vdash p_k$.

Докажем, что при такой оценке $|A| = 0$. Для этого докажем, что $|B| = 1$ тогда и только тогда, когда $\Gamma \vdash B$. Доказываем индукцией по длине B . Как обычно, рассматриваем несколько случаев:

0°. Если $B = p_k$, то доказывать нечего.

1°. Пусть $B = C \& D$. Мы знаем, что $|B| = 1$ тогда и только тогда, когда $|C| = 1$ и $|D| = 1$. К формулам C и D уже применимо предположение индукции. Значит, $|B| = 1$ в точности тогда, когда $\Gamma \vdash C$ и $\Gamma \vdash D$. Осталось применить лемму о свойствах синтаксически полных непротиворечивых теорий. Совершенно аналогично разбираются случаи дизъюнкции и импликации.

Осталось заметить, что $\Gamma \vdash \neg A$ в силу полноты теории Γ . Значит, $|\neg A| = 1$, откуда следует, что $|A| = 0$, что и требовалось доказать.

Итак, мы построили некоторую оценку, при которой наша формула принимает значение «ложь». Стало быть, она не является тавтологией. Противоречие, следовательно, $\vdash A$. ■

1.3. Интуиционистская логика

Что такое семантика? Это определение истинности, то есть выводимости в данной теории. Ещё раз напомним, чем отличается классическая логика (CL) от интуиционистской (IL).

В интуиционистской логике истинность $A \& B$ означает, что мы **умеем доказывать** A и B по отдельности, истинность $A \vee B$ означает, что мы **умеем доказывать** либо A , либо B , истинность $\neg A$ означает умение из A вывести \perp , а истинность $A \rightarrow B$ трактуется как умение из истинности A вывести B .

Напомним, что отношение частичного порядка \prec на множестве M — это рефлексивное транзитивное антисимметричное бинарное отношение.

Напомним, что рефлексивность означает $x \prec x$, транзитивность — $(x \prec y) \& (y \prec z) \Rightarrow (x \prec z)$, а антисимметричность — что $(x \prec y) \& (y \prec x) \Rightarrow (x = y)$.

Определение. Шкала Крипке — это пара (W, \leq) , состоящая из непустого множества W и отношения частичного порядка \leq на W . Множество W называется множеством миров.

Определение. Будем говорить, что на шкале W задана оценка θ , если задано отображение $\theta: \text{Var} \times W \rightarrow \mathbb{B}$ оценки переменной в данном мире, удовлетворяющее следующему свойству: если $u \leq w$ и $\theta(p, u) = 1$, то и $\theta(p, w) = 1$.

Определение. Шкала Крипке вместе с оценкой θ называется моделью Крипке: (W, \leq, θ) .

После того, как мы определили истинность переменных в каждом мире (то есть по сути зафиксировали некоторую модель), не грех будет сказать о том, как вычисляется значение формулы в мире. Будем использовать следующие правила:

- 1) $u \vDash B \& C$ тогда и только тогда, когда $u \vDash B$ и $u \vDash C$.
- 2) $u \vDash B \vee C$ тогда и только тогда, когда $u \vDash B$ или $u \vDash C$.
- 3) $u \vDash \neg B$ тогда и только тогда, когда для всех $v \geq u$ имеем $v \not\vdash B$.
- 4) $u \vDash B \rightarrow C$ тогда и только тогда, когда для всех $v \geq u$ выполнено условие: если $v \vDash B$, то $v \vDash C$.

Обозначение. Мы будем писать $M, u \vDash A$, если формула A истинна в мире u .

Лемма 1.12 (Принцип сохранности). *Пусть $M, u \vDash A$ и $u \leq v$. Тогда $M, v \vDash A$.*

□ Доказательство сводится к разбору случаев. Поскольку модель везде одна и та же, не будем её указывать.

0°. Если A — пропозициональная переменная, то доказывать нечего.

1°. Пусть $A = B \& C$. По определению истинности, в этом случае имеем $u \vDash B$ и $u \vDash C$. Поскольку $v \geq u$, получаем $v \vDash B$ и $v \vDash C$. Значит, $v \vDash B \& C$.

2°. Пусть $A = B \vee C$. Этот случай полностью аналогичен 1°.

3°. Пусть $A = \neg B$. Значит, для всех $w \geq u$ имеем $w \neq B$. А нам нужно, чтобы для всех $x \geq v$ имеем $x \neq B$. Но так оно и будет, поскольку отношение \leq транзитивно, и потому $\{x: x \geq v\} \subset \{w: w \geq u\}$.

4°. Пусть $A = B \rightarrow C$. Мы знаем, что $v \models B \rightarrow C$ тогда и только тогда, когда для всех $w \geq v$ выполнено $w \models B \Rightarrow w \models C$. А мы знаем, что $u \models B \rightarrow C$ тогда и только тогда, когда для всех $x \geq u$ выполнено $x \models B \Rightarrow x \models C$. Опять-таки, в силу транзитивности получаем требуемое. ■

Замечание. Этот принцип допускает полезную переформулировку: если формула A ложна в каком-то мире, то она ложна и во всех «предыдущих» мирах.

Определение. Формула истинна в модели, если она истинна в любом мире.

Определение. Формула общезначима, если она истинна в любой модели (то есть при любых оценках). Обозначение: $\models_{\text{IL}} A$.

Теорема 1.13 (Теорема корректности для IL). Если $\vdash_{\text{IL}} X$, то $\models_{\text{IL}} X$.

□ Будем вести индукцию по длине вывода.

0°. Для начала нужно проверить, что это справедливо для аксиом.

1) $X = A \rightarrow (B \rightarrow A)$. По определению имеем $u \models A \rightarrow (B \rightarrow A)$ тогда и только тогда, когда для всех $v \geq u$ выполнено $v \models A \Rightarrow v \models B \rightarrow A$. Докажем более общий факт: из истинности посылки следует истинность заключения. Именно, докажем, что для всех v имеем $v \models A \Rightarrow v \models B \rightarrow A$. Как мы знаем, $v \models B \rightarrow A$ — это то же самое, что для всех $w \geq v$ имеем $w \models B \Rightarrow w \models A$. Но это утверждение всегда истинно, потому что заключение истинно во всех мирах, которые старше v (а значит, и в мире w !).

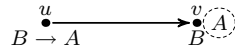


Рис. 1. К доказательству аксиомы 1

2) Пусть $X = (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$. Докажем, что $u \models X$. Это означает, что для всех $v \geq u$ выполнено $v \models A \rightarrow (B \rightarrow C) \Rightarrow v \models (A \rightarrow B) \rightarrow (A \rightarrow C)$. Пусть посылка истинна (ведь только в этом случае импликация может быть ложной). Тогда для всех $w \geq v$ имеем $w \models A \Rightarrow w \models B \rightarrow C$, то есть для всех $x \geq w$ при условии $w \models A$ имеем $x \models B \Rightarrow x \models C$. А нам нужно, чтобы для всех $w \geq v$ было выполнено $w \models (A \rightarrow B) \Rightarrow w \models (A \rightarrow C)$. Опять-таки, допустим, что $w \models A \rightarrow B$. Это значит, что для всех $x \geq w$ имеем $x \models A \Rightarrow x \models B$. Нам нужно доказать, что для всех $x \geq w$ имеем $x \models A \Rightarrow x \models C$. Пусть посылка истинна. Значит, верно и $x \models B$. А отсюда необходимым образом уже следует, что $x \models C$, что и требуется.

Для краткости мы не будем проверять все аксиомы, проверим только наиболее интересные.

8) $X = (A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B) \rightarrow C)$. Как обычно, чтобы «обломать» импликацию, нужна истинность посылок. Пусть $u \leq v \leq w$. Достаточно доказать, что $u \models A \rightarrow C \Rightarrow u \models (B \rightarrow C) \rightarrow (A \vee B) \rightarrow C$. Допустим, что $u \models A \rightarrow C$. Это означает, что для всех $v \geq u$ имеем $v \models A \Rightarrow v \models C$. А доказать нужно, что для всех $v \geq u$ имеем $v \models B \rightarrow C \Rightarrow v \models A \vee B \rightarrow C$. Допустим, что $v \models B \rightarrow C$. Это значит, что для всех $w \geq v$ имеем $w \models B \Rightarrow w \models C$. А мы хотим, чтобы $v \models A \vee B \rightarrow C$. Покажем, что и правда для всех $w \geq v$ имеем $w \models A \vee B \Rightarrow w \models C$. Применим уже знакомую схему:

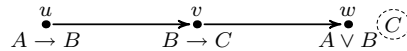


Рис. 2. К доказательству аксиомы 8

Если в мире w истинна формула A , то работает композиция первой и второй стрелки, а если истинна B , то работает вторая стрелка (это в точности копия рассуждения для первой аксиомы).

10) $X = (A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$. Допустим, что $u \models A \rightarrow B$. Нужно доказать, что $u \models (A \rightarrow \neg B) \rightarrow \neg A$, то есть для всех $v \geq u$ имеем $v \models (A \rightarrow \neg B) \Rightarrow v \models \neg A$. Допустим, что $v \models A \rightarrow \neg B$. Нужно получить, что для всех $w \geq v$ имеем $w \models A \Rightarrow w \models \neg B$. Достаточно показать, что $w \neq A$. В самом деле, допустим противное. Тогда имеем такую картину, изображённую на рис. 3.

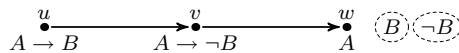


Рис. 3. К доказательству аксиомы 10

Отсюда с помощью первых двух стрелок получаем, что $w \models B$, а с помощью второй стрелки — что $v \models \neg B$. Противоречие, значит, посылка $w \models A$ не может быть истинной, и всё доказано.

1°. Проверим, что правило вывода (MP) тоже ничего не портит. Пусть $\vdash_{\text{IL}} Y, Y \rightarrow X$, и это более короткие доказательства. Имеем $u \models Y \rightarrow X$ и $u \models Y$. Тогда для всех $v \geq u$ (в частности, для $v = u$) имеем $v \models Y \Rightarrow v \models X$. Но у нас $u \models Y$, поэтому $u \models X$, что и требовалось доказать.

Отсюда следует, что все выводимые формулы будут тавтологиями. Теорема доказана. ■

Следствие 1.1 (Недоказуемость TND). Аксиома TND не является тавтологией в IL.

□ Построим модель Крипке, в которой эта аксиома будет нарушена. Возьмём два мира u и v , соединённые так, как показано на рис. 4. Оценим переменные так: пусть p истинна в v , но ложна в u . Тогда ясно, что $v \models p$, но $u \not\models p$.

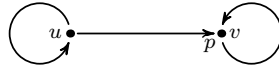


Рис. 4. Модель Крипке, опровергающая TND в IL

Однако не менее ясно, что $u \not\models \neg p$, иначе бы p была бы ложна и в v , что неверно. Итак, в мире u не является тавтологией ни переменная p , ни её отрицание. Значит, $u \not\models p \vee \neg p$, что и требовалось показать. ■

Задача 1.1. Докажите, что $A \rightarrow \neg\neg A$ выводима в IL.

Решение. Нам необходимо доказать, что, как только в некотором мире $u \models A$, то $u \models \neg\neg A$: из этого уже будет следовать, что $v \models \neg\neg A$ для всех более поздних миров v , а значит и $u \models \neg\neg A$. Так мы докажем выполнение требуемого тождества во всех мирах, где выводится A , из чего, очевидно, будет следовать его выполнимость во всех остальных мирах.

Итак, пусть $u \models A$. Тогда, как несложно заметить, $u \models \neg A \rightarrow \neg A$ (очевидно) и $u \models \neg A \rightarrow A$ (потому что A там и так выводится). Остается воспользоваться 10й аксиомой: $(\neg A \rightarrow A) \rightarrow ((\neg A \rightarrow \neg A) \rightarrow \neg\neg A)$. ■

2. Логика предикатов

2.1. Построение языка первого порядка

2.1.1. ВВЕДЕНИЕ

Мы уже много знаем про исчисление высказываний. Проблема в том, что в логике нулевого порядка формулы имеют довольно простой вид. В логике высказываний нас не интересует смысл самих высказываний. Это довольно плохо, поэтому мы сейчас построим более «выразительный» язык.

Например, высказывание «Существует число, большее ста.» хотелось бы раздробить на более мелкие части, чтобы можно было анализировать его смысл.

Так появляются атомарные формулы (строгое определение мы дадим позже), а пока приведём некоторые примеры. $x \cdot x < 2$, $1 + 3 = 4$, «Новгород старше Москвы» — это примеры атомарных формул.

Как мы знаем, некоторые высказывания нельзя оценить. Это связано с тем, что в них есть свободные переменные. Однако, если связать их кванторами, то они превращаются в обычные высказывания. Например, $x \cdot x < 2$ нельзя оценить, пока не указано, чему равен x . А вот высказывание $\exists x \exists y (x^2 + y^2 = 84)$ уже можно оценивать, если определить, по какому множеству бегают переменные x и y . Так, если $x, y \in \mathbb{N}$, то это высказывание ложно, а если $x, y \in \mathbb{R}$, то оно истинно.

Итак, мы видим, что нам нужна «область определения» и атомарные формулы, кроме того, мы захотим использовать в формулах кванторы. Этих мотивировок нам хватит для того, чтобы начать строить языки первого порядка.

2.1.2. ОПРЕДЕЛЕНИЯ

Зафиксируем некоторое множество Ω исходных символов, называемое сигнатурой. Сигнатура — это четвёрка $\Omega = (\text{Cnst}, \text{Fn}, \text{Pr}, \gamma)$, где Cnst — множество константных символов, Fn — множество функциональных символов, Pr — множество предикатных символов, а $\gamma: \text{Fn} \cup \text{Pr} \rightarrow \mathbb{N}_+$ — отображение, которое каждому функциональному символу и каждому предикатному символу ставит в соответствие натуральное число, называемое валентностью (или арностью — от англ. *arity*). Говоря простым языком, арность — это количество аргументов предиката или функционального символа. Валентность символа мы будем указывать верхним индексом.

Чтобы всё было хорошо, нужно потребовать, чтобы $\text{Pr} \neq \emptyset$.

Ещё нужно определить множество индивидуальных переменных $\text{Var} := \{v_0, v_1, v_2, \dots\}$.

Замечание. Задание сигнатуры — это совершенно символическая операция. Никакого смысла в значках сигнатуры изначально не предполагается. Мы «вдохнём в неё жизнь» чуть позже, когда определим модель.

Определение. Терм сигнатуры Ω определяется индуктивно:

- 1) Всякая константа является термом.
- 2) Всякая переменная является термом.
- 3) Если $f^k \in \text{Fn}$, а t_1, \dots, t_k — термы, то $f^k(t_1, \dots, t_k)$ — терм.

Определение. Атомарная формула — это выражение такого вида: $P^k(t_1, \dots, t_k)$, где t_i — термы, а P — k -местный предикатный символ. Множество атомарных формул сигнатуры Ω мы будем обозначать AF_Ω .

Пример 1.1. Пусть $\cdot^2, +^2$ — функциональные символы, $=^2, <^2$ — предикатные символы. Тогда привычная нам запись $1 + 3 = 2 \cdot 2$ записывается так: $(+(1, 3), \cdot(2, 2))$.

Формулы строятся, начиная с атомарных формул, индуктивным образом:

Определение.

- 1) Всякая атомарная формула является формулой.
- 2) Если φ и ψ — формулы, то $\neg\varphi, (\varphi \vee \psi), (\varphi \& \psi), (\varphi \rightarrow \psi)$ — тоже формулы.
- 3) Если φ — формула, а v — переменная, то $\exists v \varphi$ и $\forall v \varphi$ — тоже формулы.

В логике первого порядка появляется то, чего не было в логике нулевого порядка. В ИВ вместо любой переменной в формулу можно безболезненно подставить константу, от этого смысл не потеряется. Однако подставлять в формулу $\forall x (x^2 = 2)$ вместо x константу по меньшей мере нелепо: $\forall 5 (5^2 = 2)$. Дело в том, что кванторы связывают некоторые переменные, значит, нужно научиться определять все связанные вхождения переменной.

Определим индуктивно множество $FV(\varphi)$ свободных переменных формулы φ .

- 1) Если φ — атомарная формула, то в ней все переменные свободны.
- 2) При навешивании \neg ничего не меняется.
- 3) При навешивании $\&, \vee, \rightarrow$ множества свободных переменных объединяются. Например, $FV(\alpha \& \beta) = FV(\alpha) \cup FV(\beta)$.
- 4) При навешивании квантора все свободные вхождения переменной, по которой берётся квантор, объявляются связанными.

Определение. Если $FV(\alpha) = \emptyset$, то формула называется замкнутой.

2.1.3. ИНТЕРПРЕТАЦИЯ СИГНАТУРЫ. МОДЕЛЬ. ОЦЕНКИ

Пусть M — непустое множество. Интерпретация сигнатуры Ω — это пара (M, I) , где I — интерпретирующая функция. Её область определения — множество $\text{Cnst} \cup \text{Fn} \cup \text{Pr}$. При этом всякому константному символу эта функция сопоставляет некоторый элемент множества M , всякому k -местному функциональному символу — функцию $M^k \rightarrow M$, а всякому k -местному предикатному символу — отображение $M^k \rightarrow \mathbb{B}$, то есть k -местный предикат на множестве M .

Итак, всё достаточно естественно. Интерпретация просто назначает значкам их «реальный смысл».

Для дальнейшего нам потребуется расширить сигнатуру, чтобы иметь возможность определить оценку формулы.

Определение. Пусть фиксирована модель M . Расширенной сигнатурой называется множество $\tilde{\Omega} := \Omega \cup M$.

Замечание. Естественно, чтобы не вышло неприятности, нужно, чтобы M не пересекалось с Ω . Но это несложно обеспечить.

Определение. Значение оценки t^M замкнутого термина t определяется опять-таки индуктивно:

- 1) оценка константы $a \in \text{Cnst}$ — это просто $I(c)$.
- 2) оценка элемента носителя — это он сам.
- 3) оценка функционального символа $f: |f(t_1, \dots, t_k)| := I(f)(t_1^M, \dots, t_k^M)$.

Для краткости будем писать f^M вместо $I(f)$ для функциональных символов и P^M вместо $I(P)$ для предикатных символов.

Определение. Совершенно аналогично определяется оценка для формулы.

- 1) $|P(t_1, \dots, t_k)| := P^M(t_1^M, \dots, t_k^M)$.
- 2) Оценки для формул $\varphi @ \psi, \neg\varphi$ определяются естественным образом.
- 3) $|\exists v \varphi| = 1$ тогда и только тогда, когда найдётся $a \in M$ такое, что $|[a/v]\varphi| = 1$.
- 4) $|\forall v \varphi| = 1$ тогда и только тогда, когда для всех $a \in M$ имеем $|[a/v]\varphi| = 1$.

Определение. Формула называется истинной в модели, если её оценка в этой модели истинна. В этом случае пишут $M \models \varphi$. Формула называется общезначимой, если она истинна в любой модели. Формула называется выполнимой, если существует модель M , для которой $M \models \varphi$.

Определение. Пусть $FV(\varphi) = \{x_1, \dots, x_n\}$. Тогда универсальным замыканием $\bar{\forall} \varphi$ формулы φ называется формула $\forall x_1 \forall x_2 \dots \forall x_n \varphi$.

Определение. Пусть φ — любая формула (не обязательно замкнутая). Будем говорить, что $M \models \varphi$, если $M \models \bar{\forall} \varphi$. Аналогично определяются общезначимые незамкнутые формулы.

Лемма 2.1. Если $\exists x (\varphi \& \psi)$, то $\exists x \varphi \& \exists x \psi$.

□ Рассмотрим интерпретацию M . По определению, найдётся $a \in M$ такое, что $|[a/x]\varphi \& [a/x]\psi| = 1$. Тогда $|[a/x]\varphi| = 1$ и $|[a/x]\psi| = 1$. Значит $|\exists x \varphi| = 1$ и $|\exists x \psi| = 1$, и всё доказано. ■

Пример 1.2. Обратное неверно, как показывает следующий пример. Рассмотрим $M := \mathbb{N}$, а предикат P определим так: $P(x) = 1$ тогда и только тогда, когда x чётно. Рассмотрим $\varphi := P(x)$ и $\psi := \neg P(x)$. Тогда, очевидно, $M \models \exists x \varphi$ и $M \models \exists x \psi$, но формула $\varphi \& \psi$ является тождественно ложной.

Определение. Формулы φ и ψ называются эквивалентными, если $\models \varphi \leftrightarrow \psi$. При этом пишут $\varphi \sim \psi$.

Пример 1.3. Если $x \notin FV(\varphi)$, то формулы φ , $\exists x \varphi$ и $\forall x \varphi$ обозначают одно и то же (эквивалентны), потому что при подстановке ничего не поменяется.

Определение. Теория первого порядка — произвольное подмножество замкнутых формул сигнатуры Ω . Элементы теории называются аксиомами.

Определение. Будем говорить, что M — модель теории T , если $M \models T$, то есть для всех $\varphi \in T$ имеем $M \models \varphi$. Будем говорить, что теория T выполнима, если существует модель M , для которой $M \models T$.

Пример 1.4. Построим теорию графов (наши графы не будут содержать петель). Сигнатура будет состоять только из одного двуместного предиката P^2 . Зададим аксиомы:

- 1) $\forall x \neg P(x, x)$ — иррефлексивность.
- 2) $\forall x \forall y P(x, y) \rightarrow P(y, x)$ — симметричность.

Предикат P задаёт отношение « x и y связаны ребром».

Казалось бы, язык первого порядка уже довольно богат. Однако можно показать, на нём нельзя записать, например, такое утверждение: «В графе существует цикл». «Бедность» нашего языка в том, что кванторы могут применяться только к переменным, принимающим значения в носителе. Мы не можем, например, пробежаться по всем предикатам или по всем функциям; мы умеем бегать только по всему множеству M .

Определение. Будем называть интерпретацию нормальной, если в ней знак равенства ($=$) означает совпадение объектов.

Пример 1.5. Построим теорию полугрупп. Имеем $\text{Fn} := \{\circ^2\}$, $\text{Pr} := \{=^2\}$. Единственной аксиомой будет требование ассоциативности: $(x \circ y) \circ z = x \circ (y \circ z)$.

Пример 1.6. Приведём пример выполнимой теории, не имеющей конечных интерпретаций. Рассмотрим такую систему аксиом:

- 1) $\forall x \neg P(x, x)$ — иррефлексивность.
- 2) $\forall x \forall y \forall z (P(x, y) \& P(y, z) \rightarrow P(x, z))$ — транзитивность.
- 3) $\forall x \exists y P(x, y)$ — аксиома следования.

Модель такой теории очевидна: множество натуральных чисел, предикат P символизирует отношение «меньше». Очевидно, что у такой теории не может быть конечной модели: если M конечно, то рассмотрим произвольный элемент x_0 носителя и построим следующий элемент x_1 , такой что $P(x_0, x_1)$. Далее повторяем то же для x_1 , получаем x_2 , и так далее. Следовательно, получим последовательность $\{x_i\}$. В силу конечности множества, найдутся два одинаковых элемента: $x_i = x_k$. Тогда в силу транзитивности имеем $P(x_i, x_k)$, что невозможно в силу иррефлексивности.

Подстановка терма вместо переменной в формулу — это, грубо говоря, замена всех свободных вхождений переменной данным термом. Однако, как будет видно из следующего примера, не все подстановки являются хорошими.

Пример 1.7. Рассмотрим формулу $\varphi := P(x) \& \exists x P(x)$. Тут всё хорошо: подстановка t вместо x ничего не портит, получаем $[t/x]\varphi = P(t) \& \exists x P(x)$. Теперь возьмём формулу $\psi := \exists y (P(y) \& \neg P(x))$. Попробуем подставить y вместо x : $[y/x]\psi = \exists y (P(y) \& \neg P(y))$. Получилось совсем не то, что мы хотели. А почему? А потому что у нас подставленная переменная y попала в область действия квантора и стала связанной.

Определение. Терм t называется свободным для x в формуле φ , если никакое свободное вхождение x в φ не находится в области действия квантора по свободным переменным терма t .

Итак, теперь надлежит строго определить, что такое подстановка.

Определение. Подстановка $s := [t/x]r$ терма t вместо x в терм r определяется, как водится, индуктивно.

- 1) Если $r = v \in \text{Var}$, то $[t/x]r = \begin{cases} v, & v \neq x, \\ t, & v = x. \end{cases}$
- 2) Если $r = c \in \text{Cnst}$, то $[t/x]c := c$.
- 3) Если $r = f(t_1, \dots, t_k)$, то $[t/x]f(t_1, \dots, t_k) := f([t/x]t_1, \dots, [t/x]t_k)$.

Определение. Подстановка в формулы с кванторами делается так: $[t/x]\exists v \psi := \begin{cases} \exists v [t/x]\psi, & v \neq x, \\ \exists x \psi, & v = x. \end{cases}$

Мы будем использовать одно соглашение, касающееся обозначения подстановки переменных в формулы. Зависимость формулы от параметра x мы не будем обозначать никак, то есть просто будем писать φ . А вот подстановку $[t/x]\varphi$ будем обозначать через $\varphi(t)$.

Обозначение. Исчисление предикатов сигнатуры Ω мы будем обозначать PC_{Ω} . Мы не будем этого явно указывать, но всегда подразумевать, что имеется в виду классическое исчисление.

Определим аксиоматику исчисления предикатов.

1–11) Аксиомы 1–11 переносятся без изменений из классического ИВ.

Кроме них добавляется ещё 4 шаблона:

$$12) \forall x \varphi(x) \rightarrow \varphi(t).$$

$$13) \varphi(t) \rightarrow \exists x \varphi(x).$$

$$14) \forall x (\varphi(x) \rightarrow \psi) \rightarrow (\exists x \varphi(x) \rightarrow \psi).$$

$$15) \forall x (\psi \rightarrow \varphi(x)) \rightarrow (\psi \rightarrow \forall x \varphi(x)).$$

Дополнительно существует уже знакомое нам правило вывода (не будем здесь напоминать его определение) и правило обобщения (Gen), устроенное так: $\frac{\varphi}{\forall x \varphi}$.

2.1.4. ПРАВИЛА ЛОГИКИ ПРЕДИКАТОВ

Теорема 2.2 (Теорема дедукции).

$$\Gamma \vdash (\varphi \rightarrow \psi) \Leftrightarrow \Gamma, \varphi \vdash \psi,$$

причём предполагается, что правило обобщения не применяется к параметрам формулы φ .

Замечание наборщика. Без этой говорки теорема не выполняется. Пример:

$$P(x) \vdash \forall x P(x), \quad \not\vdash P(x) \rightarrow \forall x P(x).$$

□ Доказывать будем, как всегда, индукцией по длине вывода формулы ψ . Нас интересует лишь случай, когда ψ получается по правилу обобщения, так как остальные уже были рассмотрены при доказательстве теоремы дедукции логики высказываний. Итак, пусть $\psi = \forall x \eta(x)$. По предположению индукции

$$\Gamma, \varphi \vdash \eta(x) \Rightarrow \Gamma \vdash \varphi \rightarrow \eta(x).$$

Применяя правило обобщения, получим

$$\Gamma \vdash \forall x (\varphi \rightarrow \eta(x)).$$

Осталось лишь записать 15ю аксиому:

$$\forall x (\varphi \rightarrow \eta(x)) \rightarrow (\varphi \rightarrow \forall x \eta(x))$$

и воспользоваться правилом МР. ■

Утверждение 2.3. Если $\varphi \vdash \psi$, то $\frac{\varphi}{\psi}$ — допустимое правило.

□ Смысл этого утверждения состоит в том, что если мы сначала получили доказательство какой — то формулы, то потом можем просто пользоваться готовым доказательством, заменяя посылку на утверждение. На формальном уровне это означает, что мы всякий раз подставляем доказательство формулы ψ в вывод. ■

Утверждение 2.4 (Правила Бернайса).

$$1) \alpha \rightarrow \beta(x) \vdash (\alpha \rightarrow \forall x \beta(x)).$$

$$2) \beta(x) \rightarrow \alpha \vdash \exists x \beta(x) \rightarrow \alpha, \text{ если } x \notin FV(\alpha).$$

□ Для доказательства 1го пункта следует применить правило обобщения, потом 15ю аксиому и правило вывода (всё аналогично доказательству теоремы дедукции). То же самое касается и 2го пункта, только там нужна 14я аксиома. ■

Утверждение 2.5. $\neg \exists x \varphi \rightarrow \forall x \neg \varphi$.

□ Напишем вывод из наших аксиом и правил:

$$1) \varphi \rightarrow \exists x \varphi \text{ — это аксиома 13 при } t = x.$$

$$2) \neg \exists x \varphi \rightarrow \neg \varphi \text{ — правило контрапозиции.}$$

$$3) \neg \exists x \varphi \rightarrow \forall x \neg \varphi \text{ — правило Бернайса, вот и всё.}$$

$(\varphi \rightarrow \psi) \rightarrow (\neg \psi \rightarrow \neg \varphi)$ — тавтология языка нулевого порядка. Она истинна в CL , поэтому выводима в CL (по теореме полноты для CL), следовательно, выводима и тут.

Замечание наборщика. На всякий случай приведу вывод:

$$1. \text{ 10я аксиома для } \varphi \text{ и } \psi$$

$$2. \varphi \rightarrow \psi$$

$$3. (\varphi \rightarrow \neg \psi) \rightarrow \neg \varphi \text{ — получается по МР из 2х предыдущих}$$

$$4. \neg \psi$$

$$5. \neg \psi \rightarrow (\varphi \rightarrow \neg \psi) \text{ — первая аксиома}$$

6. $\varphi \rightarrow \neg\psi$ — получается по МР из 2х предыдущих

7. $\neg\varphi$ — получается по МР из 3 и 6

Таким образом, мы доказали, что $\varphi \rightarrow \psi, \neg\psi \vdash \neg\varphi$. Осталось воспользоваться правилом дедукции.

Утверждение 2.6. *Монотонность импликации:*

1) $\varphi \rightarrow \psi \vdash \forall x \varphi \rightarrow \forall x \psi$.

2) $\varphi \rightarrow \psi \vdash \exists x \varphi \rightarrow \exists x \psi$.

□ Доказательство для 1го пункта.

1. $\varphi \rightarrow \psi$

2. $\forall x \varphi \rightarrow \varphi$ — это 12я аксиома

3. $\forall x \varphi \rightarrow \psi$

4. $\forall x \varphi \rightarrow \forall x \psi$ — правило Бернаиса

Доказательство для 2го пункта.

1. $\varphi \rightarrow \psi$

2. $\psi \rightarrow \exists x \psi$ — это 13я аксиома

3. $\varphi \rightarrow \exists x \psi$

4. $\exists x \varphi \rightarrow \exists x \psi$ — правило Бернаиса

■

Утверждение 2.7.

1) $\exists x \varphi(x) \rightarrow \exists y \varphi(y), \quad x \notin \text{FV}(\exists y \varphi(y))$

2) $\forall x \varphi(x) \rightarrow \forall y \varphi(y), \quad y \notin \text{FV}(\forall x \varphi(x))$

□ Эти правила становятся совсем уж очевидными, если переписать их в несколько ином виде:

$$\exists y [y/z]\varphi(z) \rightarrow \exists x [x/z]\varphi(z), \quad x, y \notin \text{FV}(\varphi)$$

$$\forall y [y/z]\varphi(z) \rightarrow \forall x [x/z]\varphi(z), \quad x, y \notin \text{FV}(\varphi)$$

■

Лемма 2.8.

1) $\neg\exists x \varphi \leftrightarrow \forall x \neg\varphi$

2) $\neg\forall x \varphi \leftrightarrow \exists x \neg\varphi$

□ Первый пункт.

1. $\forall x \varphi \rightarrow \varphi$ — аксиома 12

2. $\neg\varphi \rightarrow \neg\forall x \varphi$ — правило контрапозиции

3. $\neg\exists x \varphi \rightarrow \forall x \neg\varphi$ — правило Бернаиса

Теперь докажем, что

$$\forall x \neg\varphi \rightarrow \neg\exists x \varphi,$$

что, очевидно, эквивалентно тому, что $\neg\forall x \varphi \leftarrow \exists x \neg\varphi$ (достаточно заменить φ на $\neg\varphi$ и применить правило контрапозиции).

1. $\forall x \neg\varphi \rightarrow \neg\varphi$ — аксиома 12

2. $\varphi \rightarrow \neg\forall x \neg\varphi$ — правило контрапозиции

3. $\exists x \varphi \rightarrow \neg\forall x \neg\varphi$ — правило Бернаиса

4. $\forall x \neg\varphi \rightarrow \neg\exists x \varphi$ — правило контрапозиции

Осталось доказать, что $\neg\forall x \varphi \rightarrow \exists x \neg\varphi$.

1. $\neg\exists x \neg\varphi \rightarrow \forall x \neg\neg\varphi$ — по уже доказанному

2. $\neg\neg\varphi \rightarrow \varphi$

3. $\forall x \neg \varphi \rightarrow \forall x \varphi$ — монотонность
4. $\neg \exists x \neg \varphi \rightarrow \forall x \varphi$ — два раза МР
5. $\neg \forall x \varphi \rightarrow \exists x \neg \varphi$ — правило контрапозиции

Теперь лемма доказана полностью. ■

2.1.5. ТЕОРЕМА КОРРЕКТНОСТИ ИСЧИСЛЕНИЯ ПРЕДИКАТОВ

В этом разделе нашей основной целью будет доказательство теоремы корректности для исчисления предикатов, а именно,

$$\vdash_{\text{PC}\Omega} \varphi \Rightarrow \models \varphi.$$

Доказательство мы разобьём на много-много промежуточных лемм. Итак, вперёд.

Лемма 2.9. Пусть дана формула $\varphi \in \text{Fm}_\Omega$ и $\text{FV}(\varphi) \subseteq \{x_1, \dots, x_n\}$. Тогда в любой интерпретации M сигнатуры Ω

$$M \models \bar{\forall} \varphi \Leftrightarrow \text{для всех } a_1, \dots, a_n \in M \quad M \models [a_1, \dots, a_n/x_1, \dots, x_n] \varphi.$$

□ Индукцией по n :

$$|\forall x_1 \dots \forall x_n \varphi|_M = 1 \Leftrightarrow \text{для всех } a_1 \in M \quad |[a_1/x_1] \forall x_2 \dots \forall x_n \varphi|_M = 1.$$

■

Лемма 2.10. Пусть α — одна из первых 11ти аксиом. Тогда $\models \alpha$.

□ Почти очевидно. Берём произвольный набор переменных, подставляем в формулы, фигурирующие в аксиоме. Считаем их (формул) значения в интерпретации. Подставляем, получаем аксиому логики высказываний — а про них нам известно, что они все — тавтологии. ■

Лемма 2.11. Пусть α — 14я аксиома. Тогда $\models \alpha$.

□ Итак, есть утверждение вида

$$\forall x (\varphi(x) \rightarrow \psi) \rightarrow (\exists x \varphi(x) \rightarrow \psi), \quad x \notin \text{FV}(\psi).$$

Пусть $\text{FV}(\alpha) = \{y_1, \dots, y_n\}$. Ясно, что $x \notin \text{FV}(\alpha)$. Пусть ψ_1 и $\varphi_1(x)$ — формулы, полученные в результате подстановки в ψ и φ некоторых значений переменных y_i . Тогда

$$\alpha_1 = \forall x (\varphi_1(x) \rightarrow \psi_1) \rightarrow (\exists x \varphi_1(x) \rightarrow \psi_1).$$

Полагаем, что $|\forall x (\varphi_1(x) \rightarrow \psi_1)| = 1$ и $|\exists x \varphi_1(x)| = 1$, нужно доказать, что $|\psi_1| = 1$. То есть, мы знаем, что для некоторого $a \in M$ $|\varphi_1(a)| = 1$ и $|\varphi_1(a) \rightarrow \psi_1| = 1$. По МР (в рамках логики высказываний) получаем, что $|\psi_1| = 1$. ■

Следующая лемма доказывается полностью аналогично.

Лемма 2.12. Пусть α — 15я аксиома. Тогда $\models \alpha$.

А это и вовсе очевидно:

Лемма 2.13.

$$\models \alpha, \alpha \rightarrow \beta \Rightarrow \models \beta.$$

Лемма 2.14.

$$\models \varphi \Rightarrow \models \forall x \varphi.$$

□ По определению, $M \models \varphi \Leftrightarrow M \models \bar{\forall} \varphi$. ■

Лемма 2.15 (о двойной подстановке в терм). Даны термы $r \in \text{Tm}_{\Omega \cup M}$, $\text{FV}(r) \subseteq \{x\}$ и $t \in \text{Tm}_\Omega$, $\text{FV}(t) \subseteq \{z_1, \dots, z_n\}$ и элементы носителя $c_1, \dots, c_n \in M$. Обозначим $a = |t(\bar{c})|_M$. Тогда

$$|[\bar{c}/\bar{z}][t/x]r|_M = |[a/x]r|_M.$$

□ Очевидно (индукция по длине терма, то есть по числу функциональных символов в нём). ■

Лемма 2.16 (о двойной подстановке в формулу). Дана формула термы $\psi \in \text{Fm}_{\Omega \cup M}$, $\text{FV}(r) \subseteq \{x\}$ и терм $t \in \text{Tm}_\Omega$, $\text{FV}(t) \subseteq \{z_1, \dots, z_n\}$, а также элементы носителя $c_1, \dots, c_n \in M$, причём подстановка $[t/x]$ свободна в ψ . Обозначим $a = |t(\bar{c})|_M$. Тогда

$$|[\bar{c}/\bar{z}][t/x]\psi|_M = |[a/x]\psi|_M.$$

□ Опят-таки индукция по длине формулы. Здесь тоже всё достаточно очевидно, отдельного рассмотрения заслуживает лишь случай с квантором: $\psi(x) = \exists u \psi_1(u, x)$, $u \neq x$. Тогда $FV(\psi_1) = \{u, x\}$, причём $u \notin \bar{z}$ (по условию подстановка свободна). Нам нужно доказать равенство

$$|[\bar{c}/\bar{z}][t/x] \exists u \psi_1| = |[a/x] \exists u \psi_1|.$$

Пусть слева единица, докажем, что и справа получим один.

Итак, для некоторого $m \in M$ имеем:

$$|[\bar{c}/\bar{z}][t/x][m/u]\psi_1| = 1.$$

Обозначим $\psi_2 = [m/u]\psi_1$. ψ_2 короче, чем ψ , следовательно, к этой формуле можно применить предположение индукции:

$$1 = |[\bar{c}/\bar{z}][t/x][m/u]\psi_1| = |[\bar{c}/\bar{z}][t/x]\psi_2| = |[a/x]\psi_2| = |[a/x][m/u]\psi_1|,$$

а значит $|[a/x] \exists u \psi_1| = 1$, что и требовалось. Все рассуждения обратимы, поэтому окончательно получаем

$$|[\bar{c}/\bar{z}][t/x] \exists u \psi_1| = 1 \Leftrightarrow |[a/x] \exists u \psi_1| = 1.$$

Случай с квантором всеобщности разбирается полностью аналогично. Случай замкнутой формулы очевиден. Лемму можно считать доказанной. ■

Лемма 2.17. Пусть α — 13я аксиома. Тогда $\vDash \alpha$.

□ Нужно доказать, что

$$M \vDash \alpha = [t(\bar{z})/x] \varphi(x, \bar{y}) \rightarrow \exists x \varphi(x, \bar{y}).$$

По определению, для этого нужно доказать, что $M \vDash \bar{\forall} \alpha$, то есть $M \vDash [\bar{b}, \bar{c}/\bar{y}, \bar{z}] \alpha$ для произвольных элементов носителя \bar{b}, \bar{c} . При подстановке ещё надо учитывать, что наборы переменных \bar{y} и \bar{z} могут пересекаться, но мы не станем вдаваться в такие подробности. Итак, имеем

$$|[\bar{b}, \bar{c}/\bar{y}, \bar{z}] \alpha| = |[\bar{b}, \bar{c}/\bar{y}, \bar{z}][t, x] \varphi(x, \bar{y}) \rightarrow [\bar{b}/\bar{z}] \exists x \varphi(x, \bar{y})| = |\alpha_1 \rightarrow \alpha_2|,$$

то есть нужно доказать, что $|\alpha_1| = 1 \Rightarrow |\alpha_2| = 1$. Доказываем:

$$|\alpha_1| = |[\bar{c}/\bar{z}][t/x] \varphi(x, \bar{b})| = |[a/x] \varphi(x, \bar{b})| \Rightarrow |\exists x \varphi(x, \bar{b})| = 1,$$

где $a = |t(\bar{c})|$. Вот и всё. ■

Лемма 2.18. Пусть α — 12я аксиома. Тогда $\vDash \alpha$.

□ Полностью аналогично предыдущей лемме. ■

Тем самым, доказательство теоремы корректности для исчисления предикатов завершено.

2.1.6. ТЕОРЕМА КОРРЕКТНОСТИ И ТЕОРЕМА НЕПРОТИВОРЕЧИВОСТИ ДЛЯ ТЕОРИЙ ПЕРВОГО ПОРЯДКА

Определение. Будем говорить, что формула φ логически следует из теории T ($T \vDash \varphi$), если φ истинна в любой модели этой теории. Для незамкнутых формул, как обычно, речь идёт об их универсальном замыкании.

Теорема 2.19 (корректности для теорий первого порядка).

$$T \vdash \varphi \Rightarrow T \vDash \varphi.$$

□ Как обычно, индукция по длине вывода. База — очевидно. Шаг — теорема дедукции. ■

Определение. Теория T противоречива, если найдётся такая формула φ , что $T \vdash \varphi$ и $T \vdash \neg \varphi$.

Теорема 2.20 (о непротиворечивости для теорий первого порядка). Выполнимая теория непротиворечива.

□ Предположим обратное. Тогда в некоторой модели $M \vDash \varphi$ и $M \vDash \neg \varphi$, что невозможно (если φ незамкнута, берём $\bar{\forall} \varphi$ и приходим к такому же противоречию). ■

2.1.7. ТЕОРИИ С РАВЕНСТВОМ

В исчислении предикатов с равенством ($\text{PC}_{\Omega}^{\equiv}$) всякая сигнатура снабжается дополнительным предикатным символом « $=$ », а список аксиом пополняется следующими пятью:

- 16) $\forall x x = x$
- 17) $\forall x \forall y (x = y \rightarrow y = x)$
- 18) $\forall x \forall y \forall z (x = y \& y = z \rightarrow x = z)$
- 19) $\forall (x_1 = y_1 \& \dots \& x_n = y_n \rightarrow f^n(x_1, \dots, x_n) = f^n(y_1, \dots, y_n)), \quad f^n \in \text{Fn}$
- 20) $\forall (x_1 = y_1 \& \dots \& x_n = y_n \rightarrow P^n(x_1, \dots, x_n) = P^n(y_1, \dots, y_n)), \quad P^n \in \text{Pr}$

Понятия выводимости и логического следования вводятся аналогично обычному исчислению предикатов.

Определение. Интерпретация M теории с равенством нормальна, если

$$M \models a = b \Leftrightarrow a = b,$$

причём равенство справа понимается как совпадение соответствующих элементов носителя.

Лемма 2.21.

- 1) $\vdash_{\text{PC}_{\Omega}^{\equiv}} t_1 = r_1 \& \dots \& t_n = r_n \rightarrow f(t_1, \dots, t_n) = f(r_1, \dots, r_n)$
- 2) $\vdash_{\text{PC}_{\Omega}^{\equiv}} t_1 = r_1 \& \dots \& t_n = r_n \rightarrow P(t_1, \dots, t_n) = P(r_1, \dots, r_n)$

2.2. Теории Хенкина

2.2.1. ЭКЗИСТЕНЦИАЛЬНАЯ ПОЛНОТА

Определение. Теория T экзистенциально полна (\exists -полна) в сигнатуре Ω , если для любой формулы $\varphi(x) \in \text{Fm}_{\Omega}$ выполнено следующее следствие: если $T \vdash \exists x \varphi(x)$, то существует такой замкнутый терм $t \in \text{Tm}_{\Omega}$, что $T \vdash \varphi(t)$.

Замечание наборщика. Говоря неформально, это означает, что квантор существования всегда реализуется в теории T .

Пример 2.1. Пусть задана сигнатура $\Omega_1 = (\{0, 1\}, \{+\}, \emptyset, \gamma_1)$ со стандартной интерпретацией \mathbb{N}_1 (натуральные числа со сложением). В ней рассмотрим теорию $\text{Th}(\mathbb{N}_1)$, состоящую из множества всех формул, истинных в этой интерпретации (её элементарную теорию). Несложно понять, что эта теория экзистенциально полна. Действительно, по определению нашей теории имеем:

$$\text{Th}(\mathbb{N}_1) \vdash \exists x \varphi(x) \Leftrightarrow \mathbb{N}_1 \models \exists x \varphi(x),$$

а это означает, опять же, по определению, что найдётся натуральное число n , для которого $\mathbb{N}_1 \models \varphi(n)$.

Пример 2.2. А вот обратный пример. Рассмотрим сигнатуру $\Omega_1 = (\emptyset, \emptyset, \{<\}, \gamma_1)$, интерпретируемую как натуральные числа со стандартным упорядочением (\mathbb{N}_2). В качестве теории вновь возьмём элементарную теорию данной интерпретации. Ясно, однако, что никакой экзистенциальной полноты здесь быть не может: так как множества констант и функциональных символов пусты, замкнутых термов в данной сигнатуре просто нет, и подставлять в формулу будет нечего.

2.2.2. СВОЙСТВО ХЕНКИНА

Определение. Будем говорить, что формула $\varphi(x)$ обладает свойством Хенкина относительно теории T , если существует такая константа данной сигнатуры $c \in \text{Cnst}$, что

$$T \vdash \exists x \varphi(x) \rightarrow \varphi(c).$$

Определение. Теория T является теорией Хенкина, если любая формула обладает одноимённым свойством относительно этой теории.

Лемма 2.22. Любая теория Хенкина экзистенциально полна.

□ Очевидно. ■

2.2.3. ВЛОЖЕНИЕ НЕПРОТИВОРЕЧИВЫХ ТЕОРИЙ В ПОЛНЫЕ ТЕОРИИ ХЕНКИНА

Лемма 2.23 (о свежих константах). Пусть дана формула $\varphi(x) \in \text{Fm}_{\Omega}$ и некоторая константа $c \in \text{Cnst}$, не входящая в эту формулу, причём $\vdash_{\text{PC}_{\Omega}^{(=)}} \varphi(c)$. Тогда $\vdash_{\text{PC}_{\Omega}^{(=)}} \varphi(x)$.

□ Пусть $\vdash \varphi(c)$, докажем, что $\vdash \varphi(z)$, где z — некоторая переменная, не встречающаяся в выводе $\varphi(c)$. Доказательство будем проводить по индукции по длине вывода $\varphi(c)$.

1. $\varphi(c)$ — аксиома. В таком случае $\varphi(z)$ — также аксиома.

2. $\varphi(c)$ получается по правилу МР:

$$\frac{\psi(c), \psi(c) \rightarrow \varphi(c)}{\varphi(c)}$$

и вывод формул $\psi(c)$ и $\psi(c) \rightarrow \varphi(c)$ короче, чем вывод $\varphi(c)$. Тогда по предположению индукции имеем $\vdash \psi(z)$ и $\vdash \psi(z) \rightarrow \varphi(z)$, откуда по МР получаем $\varphi(z)$.

3. $\varphi(c)$ получается по правилу обобщения: рассуждаем аналогично предыдущему случаю.

Итак, мы научились выводить $\varphi(z)$, а значит, по правилу обобщения, и $\vdash \forall z\varphi(z)$. По построению эта подстановка свободна, что даёт нам право воспользоваться 12й аксиомой:

$$\vdash \forall z\varphi(z) \rightarrow \varphi(x),$$

откуда по МР получаем требуемое. ■

Лемма 2.24. Пусть T — непротиворечивая теория в «счётной» (то есть не более чем счётной) сигнатуре Ω . Тогда существует такая сигнатура

$$\Omega' = \Omega \cup \{c_n | n \in \mathbb{N}\},$$

и непротиворечивая теория Хенкина T' в ней, что $T \subseteq T'$.

□ Пронумеруем все замкнутые формулы сигнатуры Ω' вида $\exists x_n \varphi_n(x_n)$. Построим индуктивно последовательность теорий T_n . Положим $T_0 = T$, $\Omega_0 = \Omega$ и

$$T_{n+1} = T_n \cup \{\exists x_n \varphi_n(x_n) \rightarrow \varphi_n(d_n)\},$$

где d_n — первая константа, не попавшая в Ω_n .

Замечание наборщика. Поясню идею этого построения (как я её понимаю). У нас есть теория T . Мы для каждой формулы вида $\exists x \varphi(x) \rightarrow \varphi(c)$ проверяем, выводима ли она из нашей теории хоть для какой-нибудь константы c . Если такой константы не нашлось, мы добавляем в сигнатуру новую константу (d_n) , а к теории — новую формулу $(\exists x_n \varphi_n(x_n) \rightarrow \varphi_n(d_n))$.

Убедимся (опять таки индуктивно), что построенные таким образом теории будут непротиворечивы. База у нас есть (исходная теория была непротиворечива по условию), будем доказывать шаг. Итак, считаем, что про теорию T_n известно, что она непротиворечива. Следует убедиться в непротиворечивости теории T_{n+1} . Предположим обратное (то есть противоречивость T_{n+1}). Мы знаем, что эта теория имеет вид $T_{n+1} = T_n, \alpha$, и её противоречивость означает, что

$$T_n, \alpha \vdash \psi, \quad T_n, \alpha \vdash \neg\psi.$$

По теореме дедукции получаем

$$T_n \vdash \alpha \rightarrow \psi, \quad T_n \vdash \alpha \rightarrow \neg\psi.$$

Теперь воспользуемся 10й аксиомой и получим $T_n \vdash \neg\alpha$. Это означает, что в теории T_n найдутся формулы r_1, \dots, r_k такие, что $r_1 \& \dots \& r_k \vdash \neg\alpha$. Вновь применим теорему дедукции:

$$\vdash r_1 \& \dots \& r_k \rightarrow \neg\alpha.$$

Вспомним, что $\alpha = \exists x_n \varphi_n(x_n) \rightarrow \varphi_n(d_n)$ и применим предыдущую лемму:

$$\vdash r_1 \& \dots \& r_k \rightarrow \neg(\exists x_n \varphi_n(x_n) \rightarrow \varphi_n(d_n)) \Rightarrow \vdash r_1 \& \dots \& r_k \rightarrow \neg(\exists x_n \varphi_n(x_n) \rightarrow \varphi_n(x)),$$

то есть

$$T_n \vdash \neg(\exists x_n \varphi_n(x_n) \rightarrow \varphi_n(x)).$$

Осталось понять, почему это невозможно. Нам известно, что

$$\neg(\alpha \rightarrow \beta) \rightarrow \alpha \& \neg\beta.$$

В нашем случае это означает следующее:

$$T_n \vdash \exists x \varphi(x) \& \neg\varphi(x).$$

Воспользуемся правилом обобщения:

$$T_n \vdash \forall x (\exists x \varphi(x) \& \neg\varphi(x)).$$

Теперь остаётся «раскрыть скобки». С одной стороны, получим

$$T_n \vdash \exists x \varphi(x),$$

так как

$$\forall x (\exists x \varphi(x) \& \neg \varphi(x)) \rightarrow \forall x \exists x \varphi(x), \quad \forall x \exists x \varphi(x) \rightarrow \exists x \varphi(x),$$

а с другой стороны, пользуясь тем, что $\forall x \neg \varphi(x) \rightarrow \neg \exists x \varphi(x)$, имеем

$$T_n \vdash \neg \exists x \varphi(x).$$

Это не согласуется с непротиворечивостью теории T_n , а значит, наше предположение о противоречивости T_{n+1} было ошибочным. Таким образом, все теории T_n будут непротиворечивы, а значит, непротиворечивой теорией будет и их объединение:

$$T' := \bigcup_n T_n.$$

По построению, эта теория будет содержать исходную и являться теорией Хенкина, что и требовалось. ■

Лемма 2.25. Пусть T — непротиворечивая теория в «счётной» (то есть не более чем счётной) сигнатуре Ω . Тогда существует такая сигнатура

$$\Omega' = \Omega \cup \{c_n | n \in \mathbb{N}\},$$

и полная непротиворечивая теория Хенкина S в ней, что $S \subseteq T'$.

□ Достаточно применить предыдущую лемму и лемму Линденбаума. ■

2.3. Существование модели

2.3.1. СЛУЧАЙ ТЕОРИИ БЕЗ РАВЕНСТВА

Лемма 2.26. Пусть T — непротиворечивая, полная, экзистенциально полная теория без равенства в не более чем счётной сигнатуре Ω . Тогда теория T имеет счётную модель.

□ Рассмотрим множество D всех замкнутых термов сигнатуры Ω (ясно, что оно не пусто, раз уж у нас нашлась экзистенциально полная теория, и не более чем счётно). Определим на это множестве модель:

$$M = (D, I).$$

Константы и функциональные символы I будет отображать в себя, а предикатные символы интерпретировать так:

$$P^M(t_1, \dots, t_n) := \begin{cases} 1, & T \vdash P(t_1, \dots, t_n) \\ 0, & \text{иначе.} \end{cases}$$

Покажем, что в такой интерпретации для любого терма имеем $t^M = t$. Проведём индукцию по числу функциональных символов, входящих в терм. Если их нет (база индукции), требование, очевидно, выполнено. Пусть теперь $t = f(t_1, \dots, t_k)$, тогда по предположению индукции

$$t^M = f^M(t_1^M, \dots, t_k^M) = f(t_1, \dots, t_k) = t,$$

что и требовалось.

Теперь осталось убедиться, что для любой замкнутой формулы φ

$$M \models \varphi \Leftrightarrow T \vdash \varphi.$$

Как обычно, используем индукцию, на этот раз — по числу логических связок, входящих в φ . Если их нет (атомарная формула), утверждение следует из определения оценки для предикатных символов. Для формул вида $\varphi \& \psi$, $\varphi \vee \psi$ и т. п. проверка тривиальна. Рассмотрим несколько более сложный случай формулы $\varphi = \exists x \psi(x)$. В силу экзистенциальной полноты $M \models \exists x \psi(x)$ тогда и только тогда, когда существует замкнутый терм t , такой что $M \models \psi(t)$, а по предположению индукции это возможно лишь в том случае, если $T \vdash \psi(t)$. Это доказывает шаг индукции, а вместе с ним и всю лемму, так как теперь уже ясно, что построенная модель является требуемой. ■

Теорема 2.27 (о существовании модели). Пусть T — непротиворечивая теория без равенства в не более чем счётной сигнатуре Ω . Тогда теория T имеет счётную модель.

□ Непротиворечивые теории мы умеем вкладывать в полные теории Хенкина, для которых можно применить только что доказанную лемму. ■

Теорема 2.28 (Гёделя о полноте).

$$\models \varphi \Rightarrow \vdash_{\text{PC}\Omega} \varphi.$$

□ Ясно, что формулу φ можно считать замкнутой. Пусть $\not\vdash \varphi$. Тогда теория $\{\neg\varphi\}$ непротиворечива, а значит, у неё существует счётная модель: $M \models \neg\varphi$. Следовательно, $\not\models \varphi$, что и требовалось доказать. ■

Следствие 2.1 (теорема Лёвенгейма–Сколема). Если теория 1го порядка без равенства имеет модель, то она имеет счётную модель.

2.3.2. СЛУЧАЙ ТЕОРИИ С РАВЕНСТВОМ

Пример 3.1. Рассмотрим теорию с равенством из одной формулы:

$$\forall x \forall y x = y.$$

Ясно, что модель этой теории не может состоять из более чем одного элемента. Этот пример показывает, что для теорий с равенством существование (нормальной) счётной модели не является обязательным.

Теорема 2.29. Пусть T — непротиворечивая теория с равенством в не более чем счётной сигнатуре Ω . Тогда теория T имеет не более чем счётную модель.

□ Положим $T^= = T \cup \{\text{аксиомы равенства } 16-20\}$. У этой теории существует счётная модель $M = (M, I)$, однако она не обязательно нормальна. Введём на этой модели отношение эквивалентности:

$$a \sim b := M \models a = b.$$

Утверждение 2.30. Такое определение отношения эквивалентности является корректным.

□ Все необходимые свойства следуют из аксиом равенства 16–18. ■

Утверждение 2.31. Пусть

$$a_i \sim b_i, \quad i = 1, \dots, n.$$

Тогда

$$f^M(a_1, \dots, a_n) = f^M(b_1, \dots, b_n).$$

□ Достаточно воспользоваться аксиомой 19. ■

Утверждение 2.32. Пусть

$$a_i \sim b_i, \quad i = 1, \dots, n.$$

Тогда

$$P^M(a_1, \dots, a_n) = P^M(b_1, \dots, b_n).$$

□ Достаточно воспользоваться аксиомой 20. ■

Итак, в качестве предметной области новой модели \widetilde{M} возьмём фактор прежнего носителя по построенному выше отношению эквивалентности: $\widetilde{M} := M / \sim$. Элементами этого носителя являются классы эквивалентности \tilde{a} элементов из M . Теперь определим новую интерпретирующую функцию \widetilde{I} . А именно, положим

$$\begin{cases} c^{\widetilde{M}} := c^{\widetilde{M}} \\ f^{\widetilde{M}}(\tilde{a}_1, \dots, \tilde{a}_n) := f^M(a_1, \dots, a_n) \\ P^{\widetilde{M}}(\tilde{a}_1, \dots, \tilde{a}_n) := P^M(a_1, \dots, a_n). \end{cases}$$

Такая модель будет нормальна по построению. Нужно, однако, ещё доказать, что это действительно модель теории T .

Замечание наборщика. В дальнейшем для класса эквивалентности будет также использоваться обозначение $\sim [\cdot]$.

Утверждение 2.33. Пусть $t \in \text{Tm}_\Omega$ и $\text{FV}(t) \subseteq \{x_1, \dots, x_n\}$. Тогда $\sim [t(a_1, \dots, a_n)|_M] = [t(\tilde{a}_1, \dots, \tilde{a}_n)|_{\widetilde{M}}]$.

□ Доказываем индукцией по числу функциональных символов в терме t . База (когда их нет) — очевидна (в этом случае терм — это переменная либо константа). Докажем шаг:

$$\begin{aligned} \sim [t(a_1, \dots, a_n)|_M] &= \sim [f(r_1(a_1, \dots, a_n), \dots, r_m(a_1, \dots, a_m))|_M] = [f(r_1(\tilde{a}_1, \dots, \tilde{a}_n), \dots, r_n(\tilde{a}_1, \dots, \tilde{a}_n))|_{\widetilde{M}}] = \\ &= f^{\widetilde{M}}([r_1(\tilde{a}_1, \dots, \tilde{a}_n)|_{\widetilde{M}}, \dots, |r_n(\tilde{a}_1, \dots, \tilde{a}_n)|_{\widetilde{M}}]) = f^{\widetilde{M}}(\sim [r_1(a_1, \dots, a_n)|_M], \dots, \sim [r_n(a_1, \dots, a_n)|_M]) = \\ &= \sim [f^M(|r_1(a_1, \dots, a_n)|_M, \dots, |r_n(a_1, \dots, a_n)|_M)]. \end{aligned}$$

■

Лемма 2.34. Пусть $\varphi \in \text{Fm}_\Omega$ и $\text{FV}(\varphi) \subseteq \{x_1, \dots, x_n\}$. Тогда

$$M \models \varphi(a_1, \dots, a_n) \Leftrightarrow \widetilde{M} \models \varphi(\tilde{a}_1, \dots, \tilde{a}_n).$$

□ В который раз — индукция по длине формулы. База — предикатный символ, он же атомарная формула, выполняется по определению. Проверим шаг. Пусть, к примеру, $\varphi = \varphi_1 \& \varphi_2$. Тогда

$$M \models \varphi \Leftrightarrow M \models \varphi_1 \text{ и } M \models \varphi_2,$$

а для каждой из них выполнено предположение индукции. Случаи дизъюнкции, импликации и отрицания проверяются аналогично. Остановимся отдельно на случае с квантором. Пусть $\varphi(a_1, \dots, a_n) = \exists y \psi(y, a_1, \dots, a_n)$. Истинность этой формулы в модели M означает, что в этой модели найдётся элемент носителя b , такой что $M \models \psi(b, a_1, \dots, a_n)$. Применяя предположение индукции, получим $\widetilde{M} \models \psi(\widetilde{b}, \widetilde{a}_1, \dots, \widetilde{a}_n)$, откуда следует, что $\widetilde{M} \models \varphi(\widetilde{a}_1, \dots, \widetilde{a}_n)$. Тем самым лемма доказана. ■

Таким образом, мы показали, что $M \models T' \Rightarrow \widetilde{M} \models T$. Это завершает доказательство теоремы. ■

Теперь точно так же, как в случае теорий без равенства, можно доказать следующую теорему.

Теорема 2.35 (Гёделя о полноте для исчисления предикатов с равенством).

$$\models \varphi \Rightarrow \vdash_{\text{PC}_{\Omega}^=} \varphi.$$

Следствие 2.2 (теорема Лёвенгейма – Сколема). Если теория 1го порядка с равенством выполнима, то она имеет не более чем счётную нормальную модель.

Теорема 2.36 (компактности Гёделя – Мальцева). Если всякое конечное подмножество теории T выполнимо, то теория T имеет модель.

□ Предположим обратное. Это означает, что теория T противоречива. Однако, в доказательстве её противоречивости будет присутствовать лишь конечное число формул, то есть в ней найдётся конечное подмножество, не имеющее модели. Получили противоречие, которое и доказывает теорему. ■

Следствие 2.3. Если теория имеет модели сколь угодно большой конечной мощности, то она имеет и бесконечную модель.

□ Итак, пусть теория T в сигнатуре Ω имеет модели сколь угодно большой конечной мощности. Построим сигнатуру $\Omega' := \Omega \cup \{c_n \mid n \geq 1\}$, то есть просто добавим к сигнатуре Ω счётное множество констант. В ней возьмём теорию $T' := T \cup \{c_i \neq c_j \mid i < j\}$. Покажем, что каждое конечное подмножество $T'' \subset T'$ этой теории выполнимо. Для любого конечного подмножества имеем $T'' \subseteq T_n := T \cup \{c_i \neq c_j \mid 1 \leq i < j \leq n\}$. По условию теоремы, существует модель $M \models T$, $|M| = n$. Это означает, что из неё можно сделать модель теории T_n , сопоставив новым константам попарно различные элементы из M . Таким образом, в силу теоремы компактности, теория T' имеет модель, и эта модель бесконечна, так как сама теория требует наличия в ней счётного множества попарно различных элементов. Однако, эта же модель будет моделью исходной теории T , что и доказывает теорему. ■

Пример 3.2. Не существует теории первого порядка в сигнатуре групп, такой что $M \models T$ тогда и только тогда, когда M — конечная группа.

2.4. Изоморфизм и элементарная эквивалентность интерпретаций

2.4.1. ОПРЕДЕЛЕНИЯ И ОСНОВНЫЕ СВОЙСТВА

Определение. Пусть M и M' — две интерпретации сигнатуры Ω . Будем говорить, что $\pi : M \cong M'$ — изоморфизм этих интерпретаций, если π — биекция, сохраняющая все операции и предикаты.

Лемма 2.37. Значения термов сохраняются при изоморфизме:

$$\pi(|t(a_1, \dots, a_n)|_M) = |t(\pi a_1, \dots, \pi a_n)|_{M'}.$$

□ Доказательство проводится по индукции и полностью аналогично доказательству утверждения 2.33. ■

Лемма 2.38. Выводимость формул сохраняется при изоморфизме:

$$M \models \varphi(a_1, \dots, a_n) \Leftrightarrow M' \models \varphi(\pi a_1, \dots, \pi a_n).$$

□ Доказательство полностью аналогично доказательству леммы 2.34. ■

Замечание наборщика. Такое совпадение доказательств не случайно. Когда мы брали фактор по отношению эквивалентности, мы имели дело с «гомоморфизмом» интерпретаций.

Определение. Интерпретации изоморфны, если между ними существует изоморфизм.

Утверждение 2.39. Изоморфизм интерпретаций является отношением эквивалентности.

□ Очевидно. ■

Определение. Модели называют элементарно эквивалентными, если их элементарные теории совпадают.

Теорема 2.40. Изоморфные теории элементарно эквивалентны.

□ Следует из леммы 2.38. ■

Построим пример элементарно эквивалентных неизоморфных теорий.

Пример 4.1. Рассмотрим стандартную сигнатуру арифметики Ω_0 : константы 0 и 1, предикатный символ равенства, функциональные символы сложения и умножения. Пусть $\mathbb{N}_0 = (\mathbb{N}, I)$ — её стандартная интерпретация. Элементарная теория этой модели $\text{Th}(\mathbb{N}_0)$ носит название полной арифметики.

Также рассмотрим сигнатуру $\Omega_1 := \Omega \cup \{\infty\}$ и в ней теорию $T : \text{Th}(\mathbb{N}_0) \cup \{\infty \neq 0, \infty \neq 1, \dots\}$. Всякое конечное подмножество этой теории выполнимо, следовательно, в силу теоремы компактности Гёделя – Мальцева, у этой теории существует некоторая модель $\mathbb{N}_1 \models T$. При этом, очевидно, $\mathbb{N}_1 \models \text{Th}(\mathbb{N}_0)$. Однако, эти модели неизоморфны: элементу $\infty \in \mathbb{N}_1$ в $\text{Th}(\mathbb{N}_0)$ не найдётся соответствия.

Замечание наборщика. А почему, собственно, они будут элементарно эквивалентны?

Лемма 2.41 (о полноте). *Теория полна тогда и только тогда, когда все её модели элементарно эквивалентны.*

□ Пусть теория полна и M и M' — её модели. Для любой формулы φ имеем: либо $T \models \varphi$, откуда $M \models \varphi$ и $M' \models \varphi$, либо то же самое выполнено относительно $\neg\varphi$. Значит, все истинные формулы у этих моделей одни и те же, что и требовалось. Теперь докажем в обратную сторону. Пусть все модели теории T элементарно эквивалентны. Тогда если $T \not\models \varphi$, то для некоторой модели (а значит и для всех) $M \not\models \varphi$, откуда $T \models \neg\varphi$. ■

2.4.2. СИЛЬНАЯ КАТЕГОРИЧНОСТЬ И СЧЁТНАЯ КАТЕГОРИЧНОСТЬ

Определение. Теория первого порядка называется сильно категоричной, если все её модели изоморфны.

Определение. Теория первого порядка называется счётно – категоричной, если все её счётные модели изоморфны.

Утверждение 2.42. *Любая сильно категоричная теория полна.*

□ Следует из леммы о полноте. ■

Утверждение 2.43 (признак Вота). *Любая счётно – категоричная теория, не имеющая конечных моделей, полна.*

□ Пусть теория T непротиворечива (иначе, она, конечно, полна). Тогда у неё есть модель $M \models T$, и эта модель счётна (по условию).

Утверждение 2.44.

$$T \models \varphi \Leftrightarrow M \models \varphi.$$

□ В одну сторону это очевидно, ведь M — это модель T . Докажем, что $T \not\models \varphi \Rightarrow M \not\models \varphi$. Действительно, если $T \not\models \varphi$, то теория $T \cup \{\neg\varphi\}$ выполнима, а значит, по теореме Лёвенгейма – Сколема, она имеет счётную модель. Однако, по условию, она будет изоморфна исходной, откуда $M \models \neg\varphi$. ■

Это утверждение завершает доказательство признака Вота. ■

Пример 4.2. Построим теорию плотного линейного порядка без наименьшего и наибольшего элементов (DLO_{\rightarrow} — dense linear order). Сигнатура будет состоять из двух предикатных символов: $\{<, =\}$. А в теорию войдут следующие аксиомы:

1. $\forall x \neg x < x$;
2. $\forall x \forall y \forall z x < y \ \& \ y < z \rightarrow x < z$;
3. $\forall x \forall y x < y \ \& \ y < x \rightarrow x = y$;
4. $\forall x \forall y x < y \rightarrow \exists z (x < z \ \& \ z < y)$ — это и есть плотность;
5. $\forall x \exists y x < y$;
6. $\forall x \exists y y < x$.

Согласно теореме Кантора, эта теория счётно – категорична.

Пример 4.3. Рассмотрим самую простую сигнатуру с равенством: $\{=\}$. Теория будет состоять из следующих формул:

$$T = \{\beta_n | n \geq 1\} \quad \beta_n = \exists x_1 \dots \exists x_n \left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right).$$

Она счётно – категорична (очевидно).

Теорема 2.45. *Элементарная теория конечной интерпретации сильно категорична.*

□ Мы докажем эту теорему лишь для случая конечной сигнатуры.
Итак, пусть $M = \{a_1, \dots, a_n\}$. Рассмотрим следующую формулу:

$$\varphi_M := \exists x_1 \dots \exists x_n \left[\bigwedge_{i < j} x_i \neq x_j \ \& \ \forall y \left(\bigvee_{i=1}^n y = x_i \right) \ \& \ \bigwedge_{i=1}^n \{c = x_i \mid c \in \text{Cnst}, M \models c = a_i\} \ \& \right. \\ \& \ \bigwedge_{1 \leq i_1 < \dots < i_k \leq n} \{P(x_{i_1}, \dots, x_{i_k}) \mid P^k \in \text{Pr}, M \models P(a_{i_1}, \dots, a_{i_k})\} \ \& \\ \& \ \bigwedge_{1 \leq i_1 < \dots < i_k \leq n} \{\neg P(x_{i_1}, \dots, x_{i_k}) \mid P^k \in \text{Pr}, M \models \neg P(a_{i_1}, \dots, a_{i_k})\} \ \& \\ \left. \& \ \bigwedge_{1 \leq i_1 < \dots < i_k \leq n} \{f(x_{i_1}, \dots, x_{i_k}) = x_j \mid f^k \in \text{Fm}, M \models f(a_{i_1}, \dots, a_{i_k}) = a_j\} \right].$$

Утверждение 2.46.

$$N \models \varphi_M \Leftrightarrow N \cong M.$$

□ Ясно, что в доказательстве нуждается лишь прямое (\Rightarrow) утверждение. Итак, пусть

$$N \models \varphi_M = \exists x_1 \dots \exists x_n \psi(x_1, \dots, x_n).$$

Это означает, что $N \models \psi(b_1, \dots, b_n)$ для некоторого набора элементов b_i . Нам также известно, что есть набор a_i , для которого $M \models \psi(a_1, \dots, a_n)$. Покажем, что отображение

$$\pi: a_i \mapsto b_i$$

является изоморфизмом интерпретаций. Необходимо проверить, что

$$\pi(f(a_{i_1}, \dots, a_{i_k})) = f(\pi a_{i_1}, \dots, \pi a_{i_k}) \text{ и } P(a_{i_1}, \dots, a_{i_k}) = P(\pi a_{i_1}, \dots, \pi a_{i_k}).$$

Пусть $f(b_{i_1}, \dots, b_{i_k}) = b_j$. Это означает, что в формуле φ_M содержится «множитель» вида $f(x_{i_1}, \dots, x_{i_k}) = x_j$, а значит, в модели M будет иметь место равенство $f(a_{i_1}, \dots, a_{i_k}) = a_j$. Аналогичное рассуждение позволяет убедиться, что значения предикатов также сохраняются. ■

Непосредственно из доказанного утверждения следует сильная категоричность. ■

Следствие 2.4. *Для конечных теорий изоморфизм равносильна элементарной эквивалентности.*

3. Теория алгоритмов

3.1. Введение в системы Поста

3.1.1. Построение и примеры систем Поста

Определение. Система Поста (над алфавитом \mathcal{A}) есть четвёрка конечных множеств $E = (\mathcal{A}, \mathcal{B}, \mathcal{V}, \mathcal{S})$, первые три из которых попарно не пересекаются. Их называют, соответственно, основным алфавитом, вспомогательный алфавит, множество переменных и множество схем. Множество схем состоит из кортежей вида (t_1, \dots, t_n, t) , где $n \geq 0$, а элементы t_i и t суть слова над алфавитами $\mathcal{A}, \mathcal{B}, \mathcal{V}$ (их называют термами).

В дальнейшем для обозначения множества всех слов над некоторым алфавитом, скажем, \mathcal{A} , будет использоваться запись \mathcal{A}^* . Таким образом, термы являются элементами множества $(\mathcal{A} \cup \mathcal{B} \cup \mathcal{V})^*$. Схемы будут записывать так:

$$\frac{t_1, \dots, t_n}{t}.$$

В случае, когда $n = 0$, будем говорить, что t — схема аксиом. Если в схему вместо всех входящих в неё переменных подставить некоторые замкнутые термы, получим правило вывода (либо аксиому). Понятия «вывода» и «вывода из посылок» определяются аналогично тому, как это делалось в обычной логике высказываний.

Определение. Язык, порождаемый системой Поста E — это множество всех слов, выводимых в этой системе Поста:

$$L(E) := \{\alpha \in \mathcal{A}^* \mid \vdash_E \alpha\}.$$

Определение. Множество слов над некоторым алфавитом называется (рекурсивно) перечислимым, если оно совпадает с языком, порождённым некоторой системой Поста над этим алфавитом.

Пример 1.1. Построим систему Поста, которая порождает множество всех пропозициональных формул.

$$\begin{aligned}\mathcal{A} &= \{p, |, \&, \vee, \rightarrow, \neg, (,)\}, \\ \mathcal{B} &= \{A, F\}, \quad \mathcal{V} = \{x, y\}, \\ \mathcal{S} &= \left\{ Ap, \frac{Ax}{Ax|}, \frac{Ax}{Fx}, \frac{Fx}{F\neg x}, \frac{Fx, Fy}{F(x \& y)}, \frac{Fx, Fy}{F(x \vee y)}, \frac{Fx, Fy}{F(x \rightarrow y)}, \frac{Fx}{x} \right\}.\end{aligned}$$

Пример 1.2. Построим систему Поста, которая порождает всё множество \mathcal{A}^* .

$$\mathcal{A} = \{a_1, \dots, a_n\}, \quad \mathcal{S} = \left\{ \Lambda, \frac{x}{xa_1}, \dots, \frac{x}{xa_n} \right\}.$$

Здесь и далее Λ обозначает пустое слово.

Теорема 3.1. *Объединение и пересечение перечислимых множеств само перечислимо.*

□ Итак, пусть $X, Y \subseteq \mathcal{A}^*$ — перечислимы, то есть $X = L(E)$ и $Y = L(F)$, где $E = (\mathcal{A}, \mathcal{B}_E, \mathcal{V}_E, \mathcal{S}_E)$ и $F = (\mathcal{A}, \mathcal{B}_F, \mathcal{V}_F, \mathcal{S}_F)$ — некоторые системы Поста. Рассмотрим случай объединения. Будем строить систему Поста $G = (\mathcal{A}, \mathcal{B}, \mathcal{V}, \mathcal{S})$, для которой $X \cup Y = L(G)$. Введём новые символы $A, \varepsilon, \varphi, x$ и положим

$$\mathcal{B} = \mathcal{B}_E \cup \mathcal{B}_F \cup \{A, \varepsilon, \varphi\}, \quad \mathcal{V} = \mathcal{V}_E \cup \mathcal{V}_F \cup \{x\}.$$

Теперь заполним множество схем \mathcal{S} . Пусть в \mathcal{S}_E содержится схема вида

$$\frac{t_1, \dots, t_n}{t},$$

тогда в \mathcal{S} включим схему

$$\frac{\varepsilon t_1, \dots, \varepsilon t_n}{\varepsilon t}.$$

В случае, если такая схема есть в \mathcal{S}_F , добавляем в \mathcal{S} схему

$$\frac{\varphi t_1, \dots, \varphi t_n}{\varepsilon t}.$$

Кроме схем, получаемых таким образом, добавим ещё схемы

$$A, \frac{Ax}{Axa_1}, \dots, \frac{Ax}{Axa_n}, \frac{Ax, \varepsilon x}{x}, \frac{Ax, \varphi x}{x}.$$

Теперь уже несложно убедиться, что для такой системы G будет выполнена следующая лемма.

Лемма 3.2.

1. $\vdash_G At \Leftrightarrow t \in \mathcal{A}^*$
2. $\vdash_G \varepsilon t \Leftrightarrow \vdash_E t$
3. $\vdash_G \varphi t \Leftrightarrow \vdash_F t$
4. $\vdash_G \alpha \in \mathcal{A}^* \Leftrightarrow \alpha \in X \cup Y$

Что же касается доказательства для случая пересечения, его единственным отличием будет то, что вместо схем

$$\frac{Ax, \varepsilon x}{x}, \frac{Ax, \varphi x}{x}$$

следует добавлять схему

$$\frac{Ax, \varepsilon x, \varphi x}{x}.$$

■

3.1.2. ПОДСТАНОВКИ И ПРАВИЛА

Лемма 3.3. *Пусть даны термы r_1, \dots, r_k, t, s и переменные x_1, \dots, x_k, y , причём все они все попарно различны. Тогда*

$$[s/y] [\bar{r}/\bar{x}] t = \begin{cases} [r'_1, \dots, r'_k, s/x_1, \dots, x_k, y] t, & y \notin \bar{x} \\ [r'_1, \dots, r'_k/x_1, \dots, x_k] t, & y \in \bar{x}, \end{cases}$$

где $r'_i := [s/y] r_i$.