УДК 519.7
ББК 22.176
М 30

Марченков С.С. **Основы теории булевых функций.** — М.: ФИЗМАТЛИТ, 2014. — 136 с. — ISBN 978-5-9221-1562-9.

Книга содержит развернутое введение в теорию булевых функций. Изложены основные свойства булевых функций и доказан критерий функциональной полноты. Приведено описание всех замкнутых классов булевых функций (классов Поста) и дано новое доказательство их конечной порождаемости. Рассмотрено задание классов Поста в терминах некоторых стандартных предикатов. Изложены основы теории Галуа для классов Поста. Введены и исследованы два «сильных» оператора замыкания: параметрического и позитивного. Рассмотрены частичные булевы функции и доказан критерий функциональной полноты для класса частичных булевых функций. Исследована сложность реализации булевых функций схемами из функциональных элементов.

Для студентов, аспирантов и преподавателей высшей школы, изучающих и преподающих дискретную математику и математическую кибернетику.

Допущено УМО по классическому университетскому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям ВПО 010400 «Прикладная математика и информатика» и 010300 «Фундаментальная информатика и информационные технологии».

ISBN 978-5-9221-1562-9

ОГЛАВЛЕНИЕ

Предисловие

Теория булевых функций составляет фундамент современной дискретной математики. Булевы функции являют собой самые простые объекты дискретной природы. Язык булевых функций хорошо приспособлен для описания разбиения целого на части (особенно в дихотомических процессах) и взаимодействия этих частей. Поэтому он широко используется в самых разнообразных областях человеческого знания: будь то собственно математика (теория множеств и математическая логика, алгебра, теория графов и комбинаторика, теория информации, криптология и теория кодирования, теория формальных языков и языков программирования, синтез управляющих систем, распознавание образов и т. д.), техника (анализ и построение различных устройств коммутации, управления и переработки информации, включая современные ЭВМ, тестирование сложных систем и построение надежных схем из ненадежных элементов), экономика и математическая биология. Список областей, где могут применяться и с успехом применяются результаты и методы теории булевых функций, нетрудно продолжить и далее.

В приложениях теории булевых функций наиболее часто встречается следующая задача: выразить (изобразить, приблизить) заданную функцию или заданный класс функций через булевы функции из имеющегося запаса функций и (когда это возможно) указать приемы и методы для оптимального решения поставленной задачи. Арсенал выразительных средств в решении этой задачи весьма разнообразен. Однако для булевых функций наиболее востребованными являются подходы и методы, которые в той или иной степени базируются на композиции (суперпозиции) функций или близких к ней операциях. Поэтому в предлагаемой читателю книге мы попытались собрать основные результаты, относящиеся в теории булевых функций к этому направлению исследований.

Главы I, II содержат традиционный материал, вводящий в теорию булевых функций, включая критерий полноты для класса всех булевых функций. Обычно в этом объеме булевы функции излагаются в курсах дискретной математики. Единственное нетрадиционное дополнение, которое включено в главу II, это

перечисление всех замкнутых классов, содержащих константы. Иногда изучение замкнутых классов булевых функций помимо предполных классов ограничивают только классами, содержащими обе константы.

Глава III посвящена изложению замечательного результата Э. Поста (одной из «жемчужин» теории булевых функций) — описанию всех замкнутых классов булевых функций (классов Поста) с указанием их базисов и построением решетки замкнутых классов. Эта задача в принципиальном плане решена Э. Постом еще в 1921 г. Однако достаточную известность результаты Поста получили лишь в середине 1950-х гг., когда по существу и начались исследования по булевым функциям и их приложениям. Результаты Поста многократно переизлагались и передоказывались. В главе III приведено компактное доказательство конечной порождаемости классов Поста, центральные моменты которого содержатся в статье [20].

В главе IV исследуется предикатное описание классов Поста. В последние годы этой теме уделятся все большее внимание. Это связано с тем, что описание классов Поста с помощью предикатов есть описание с помощью некоторых инвариантов — прием, широко распространенный в математике. На языке предикатов удается дать унифицированное определение всех классов Поста (исключение составляют «малые» классы, не содержащие селекторных функций), которое не содержит понятий формулы и суперпозиции. Кроме того, предикатный язык позволяет связать с помощью соответствия Галуа решетку замкнутых классов булевых функций и решетку замкнутых (относительно специальных логических операций) классов предикатов. В итоге возникает возможность доказывать известные результаты по замкнутым классам булевых функций, не обращаясь по существу к понятию булевой функции.

В главе V рассмотрены примеры двух «сильных» операторов замыкания: оператора параметрического замыкания и оператора позитивного замыкания. Эти операторы позволяют «сжимать» счетную решетку замкнутых классов булевых функций до конечных размеров: размера 25 для параметрического замыкания и размера 6 для позитивного замыкания. Использование операторов параметрического и позитивного замыкания бывает полезно при проведении «грубых» классификаций множества булевых функций.

В главе VI рассматриваются вопросы полноты и конечной порождаемости для частичных булевых функций. Эта тематика практически не затрагивается в учебной и монографической

литературе. Вместе с тем многие вопросы для частичных булевых функций решаются совершенно иначе, нежели для обычных булевых функций. Одна из целей главы VI — обратить внимание исследователей на проблемы, возникающие для частичных булевых функций, и, возможно, способствовать продвижению данной тематики в лекционные курсы.

Глава VII посвящена еще одной «классической» проблеме теории булевых функций. Речь идет о сложности реализации булевых функций различными классами управляющих систем. В главе VII рассматриваются, в частности, системы булевых уравнений и схемы из функциональных элементов. Начало исследованиям в этом направлении положили работы К. Шеннона 1940-х гг. Однако все наиболее значительные (и весьма многочисленные) результаты были получены начиная с середины 1950-х гг. С. В. Яблонским, О. Б. Лупановым, их последователями и учениками. В главе VII мы, по существу, ограничились двумя результатами для схем из функциональных элементов: определением порядка функции Шеннона $L(n)$ для схем в базисе $\{-, \vee, \&\}$ (результат К. Шеннона) и получением асимптотики функции $L(n)$ — широко известный результат, принадлежащий О. Б. Лупанову.

Книга адресована широкому кругу читателей. Прежде всего, она будет полезна студентам и аспирантам математических факультетов, специализирующимся в области дискретной математики, а также преподавателям вузов, читающим курсы по дискретной математике и математической кибернетике.

Для понимания основного содержания книги не требуется никаких предварительных знаний. Некоторые элементарные сведения из математической логики, используемые в главах IV, V, можно найти, например, в книгах [8, 12].

Указатель обозначений

C — класс всех функций, равных константам 0 или 1

C_0 — класс всех функций, равных константе 0

C_1 — класс всех функций, равных константе 1

D — класс всех дизъюнкций

D_0 — класс всех дизъюнкций, сохраняющих константу 0

D_1 — класс всех дизъюнкций, сохраняющих константу 1

D_{01} — класс всех дизъюнкций, сохраняющих константы 0 и 1

E_2 — множество $\{0, 1\}$

I^m $(m = 2, 3, \ldots, \infty)$ — класс всех функций, удовлетворяющих условию 1^m

I_1^m $(m = 2, 3, \ldots, \infty)$ — класс всех функций, удовлетворяющих условию 1^m и сохраняющих константу 1

$\mathrm{Inv}(f)$ — класс всех предикатов, сохраняемых функцией f

$\mathrm{Inv}(F)$ — класс всех предикатов, сохраняемых функциями множества F

K — класс всех конъюнкций

K_0 — класс всех конъюнкций, сохраняющих константу 0

K_1 — класс всех конъюнкций, сохраняющих константу 1

K_{01} — класс всех конъюнкций, сохраняющих константы 0 и 1

L — класс всех линейных функций

L_0 — класс всех линейных функций, сохраняющих константу 0

L_1 — класс всех линейных функций, сохраняющих константу 1

L_{01} — класс всех линейных функций, сохраняющих константы 0 и 1

M — класс всех монотонных функций

M_0 — класс всех монотонных функций, сохраняющих константу 0

M_1 — класс всех монотонных функций, сохраняющих константу 1

M_{01} — класс всех монотонных функций, сохраняющих константы 0 и 1

MI^m $(m = 2, 3, \ldots, \infty)$ — класс всех монотонных функций, удовлетворяющих условию 1^m

MI_1^m $(m = 2, 3, \ldots, \infty)$ — класс всех монотонных функций, удовлетворяющих условию 1^m и сохраняющих константу 1

MO^m $(m = 2, 3, \ldots, \infty)$ — класс всех монотонных функций, удовлетворяющих условию 0^m

MO_0^m $(m = 2, 3, \ldots, \infty)$ — класс всех монотонных функций, удовлетворяющих условию 0^m и сохраняющих константу 0

MU — класс всех монотонных функций, существенно зависящих не более чем от одной переменной

O^m $(m = 2, 3, \ldots, \infty)$ — класс всех функций, удовлетворяющих условию 0^m

O_0^m $(m = 2, 3, \ldots, \infty)$ — класс всех функций, удовлетворяющих условию 0^m и сохраняющих константу 0

P_2 — класс всех булевых функций

P_2^* — класс всех частичных булевых функций

Par — язык параметрического замыкания

Par$[Q]$ — параметрическое замыкание множества функций Q

Pol(ρ) — класс всех функций, сохраняющих предикат ρ

Pol(R) — класс всех функций, сохраняющих предикаты множества R

Pos — язык позитивного замыкания

Pos$[Q]$ — позитивное замыкание множества функций Q

$\mathcal{R}_2$ — множество всех булевых предикатов

S — класс всех самодвойственных функций

S_{01} — класс всех самодвойственных функций, сохраняющих константы 0 и 1

SL — класс всех самодвойственных линейных функций

SM — класс всех самодвойственных монотонных функций

SU — класс всех самодвойственных функций, существенно зависящих не более чем от одной переменной

T_0 — класс всех функций, сохраняющих константу 0

T_1 — класс всех функций, сохраняющих константу 1

T_{01} — класс всех функций, сохраняющих константы 0 и 1

U — класс всех функций, существенно зависящих не более чем от одной переменной

U_0 — класс всех функций, существенно зависящих не более чем от одной переменной и сохраняющих константу 0

U_1 — класс всех функций, существенно зависящих не более чем от одной переменной и сохраняющих константу 1

U_{01} — класс всех функций, существенно зависящих не более чем от одной переменной и сохраняющих константы 0 и 1 (класс всех селекторных функций)

Глава I

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ

§ 1. Табличное задание булевых функций

Булевы функции определяются на множестве, состоящем из двух элементов. Обычно в качестве этих элементов берут числа 0 и 1. Множество, состоящее из 0 и 1, принято обозначать через E_2. Булева функция — это функция, аргументы которой принимают значения во множестве E_2 и значения которой также принадлежат множеству E_2.

Булеву функцию f (от) n аргументов обозначаем $f(x_1, \ldots, x_n)$ и называем также булевой функцией от переменных $x_1, \ldots, x_n$. Иногда вместо переменных $x_1, x_2, \ldots$ используем переменные $y, z, w, \ldots$, возможно, с индексами. Множество всех булевых функций обозначим посредством P_2, а множество всех булевых функций от n переменных — посредством $P_2^{(n)}$.

Булева функция $f(x_1, \ldots, x_n)$ есть отображение n-й декартовой степени множества E_2, состоящей из 2^n наборов, в множество E_2 и, значит, является конечным объектом. Поэтому ее можно задать табличным способом: перечислить в некотором порядке все наборы из множества E^n и вслед за каждым набором записать значение функции на этом наборе. Действительно, наиболее наглядно реализовать этот способ задания булевой функции можно в виде таблицы (см. табл. 1), в левой части которой выписаны в лексикографическом порядке все 2^n двоичных наборов.

Таблица 1

x_1	x_2	$\ldots$	x_n	$f(x_1, x_2, \ldots, x_n)$
0	0	$\ldots$	0	$f(0, 0, \ldots, 0)$
0	0	$\ldots$	1	$f(0, 0, \ldots, 1)$
		$\ldots$		$\ldots$
1	1	$\ldots$	0	$f(1, 1, \ldots, 0)$
1	1	$\ldots$	1	$f(1, 1, \ldots, 1)$

Условимся о том, что, говоря о табличном способе задания булевой функции, мы всегда будем иметь в виду, что в левой части соответствующей таблицы двоичные наборы выписаны

именно в лексикографическом порядке. В этом случае для всех булевых функций от n переменных левая часть таблицы 1 будет одной и той же. Поэтому потребность в ее воспроизведении, вообще говоря, отпадает. Тогда от таблицы 1 остается только столбец значений функции f высоты 2^n. Таким образом, любую булеву функцию от n переменных можно задать двоичным столбцом высоты 2^n. Верно, разумеется, и обратное: всякий двоичный столбец высоты 2^n определяет некоторую булеву функцию от n переменных. На практике вместо двоичных столбцов высоты 2^n удобнее пользоваться двоичными строками (наборами) длины 2^n. В результате для булевой функции $f(x_1, \ldots, x_n)$ получаем двоичную строку вида

$$(f(0,0,\ldots,0)f(0,0,\ldots,1)\ldots f(1,1,\ldots,0)f(1,1,\ldots,1)).$$

Таким образом, имеем взаимно однозначное соответствие между множеством $P_2^{(n)}$ всех булевых функций от n переменных и множеством всех двоичных строк длины 2^n. Из него сразу следует, что число булевых функций от n переменный равно 2^{2^n}.

§ 2. Некоторые элементарные булевы функции

Составим таблицу для всех четырех булевых функций от одной переменной.

Таблица 2

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	0	1	1	0

Функции $f_1(x)$ и $f_2(x)$ называются *константами* 0 и 1. Их часто так и обозначают (0 и 1), не указывая явно переменную x. Как видно из табл. 2, значения функции $f_3(x)$ совпадают со значениями переменной x. Поэтому функцию $f_3(x)$ называют *тождественной функцией* и вместо символа функции, как правило, пишут лишь символ переменной x. Функция $f_4(x)$ осуществляет инвертирование значений переменной x. Ее называют *отрицанием* и обозначают $\overline{x}$.

Обратимся к функциям от двух переменных. Как мы знаем, их насчитывается ровно $2^{2^2} = 16$. Мы могли бы поступить так же, как с функциями от одной переменной, и представить в одной таблице значения всех 16 функций. Однако пока нам будет достаточно выписать одиннадцать функций (по техническим

причинам в табл. 3 после символов функций опущены символы переменных x_1, x_2).

Таблица 3

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}
0	0	0	1	0	0	1	1	0	0	0	1	1
0	1	0	1	0	1	1	0	0	1	1	1	1
1	0	0	1	1	0	0	1	0	1	1	0	1
1	1	0	1	1	1	0	0	1	1	0	1	0

Как видно из табл. 3, функции $f_1(x_1, x_2)$ и $f_2(x_1, x_2)$ суть константы 0 и 1. Значения функции $f_3(x_1, x_2)$ совпадают со значениями переменной x_1. Поэтому функцию $f_3(x_1, x_2)$ называют *функцией выбора* (первого аргумента) или *селекторной функцией* и обозначают $e_1^2(x_1, x_2)$. Так же, как для тождественной функции одной переменной, вместо выражения $e_1^2(x_1, x_2)$ часто пишут лишь x_1. Аналогичным образом обстоит дело с функцией $f_4(x_1, x_2)$, которая представляет собой функцию выбора (второго аргумента) и имеет обозначение $e_2^2(x_1, x_2)$. Функции $f_5(x_1, x_2)$ и $f_6(x_1, x_2)$ инвертируют, соответственно, значения переменных x_1 и x_2. Поэтому их обычно заменяют функциями $\overline{x}_1$ и $\overline{x}_2$.

Анализируя столбец значений функции $f_7(x_1, x_2)$, нетрудно понять, что эту функцию можно определить как $x_1 \cdot x_2$ или как $\min(x_1, x_2)$. Функция f_7 — одна из важнейших в теории булевых функций. Она носит название *конъюнкции* (или логического произведения). Для функции $f_7(x_1, x_2)$ приняты обозначения: $x_1 \cdot x_2$ (или $x_1 x_2$), $x_1 \,\&\, x_2$ и $x_1 \wedge x_2$. (Так же, как в арифметике и алгебре, при написании некоторых функций от двух переменных знак функции может ставиться между символами переменных.) В дальнейшем мы будем преимущественно использовать обозначения $x_1 \cdot x_2$ или $x_1 x_2$.

Легко проверить, что функцию $f_8(x_1, x_2)$ можно определить как $\max(x_1, x_2)$. Функция f_8 также относится к числу важнейших в теории булевых функций. Функцию $f_8(x_1, x_2)$ называют *дизъюнкцией* (или логической суммой) и обозначают $x_1 \vee x_2$.

Функция $f_9(x_1, x_2)$ есть сложение по модулю 2 ($1 + 1 = 0$ по модулю 2). В отличие от обычного (арифметического) сложения $x_1 + x_2$ она обозначается $x_1 \oplus x_2$.

Функция $f_{10}(x_1, x_2)$ носит название *импликации* и обозначается $x_1 \to x_2$. Наконец, функция $f_{11}(x_1, x_2)$ называется *штрихом Шеффера* (или антиконъюнкцией) и обозначается $x_1 | x_2$.

Для любого натурального n и любого i $(1 \leqslant i \leqslant n)$ обозначим через $e_i^n(x_1, \ldots, x_i, \ldots, x_n)$ функцию выбора i-го аргумента (селекторную функцию), значения которой совпадают со значениями переменной x_i. Отметим, что вместо функции $e_i^n(x_1, \ldots, x_i, \ldots, x_n)$ часто записывают лишь переменную x_i.

§ 3. Существенные и фиктивные переменные

Когда говорят, что булева функция $f(x_1, \ldots, x_n)$ зависит от переменных $x_1, \ldots, x_n$, имеют в виду лишь то, что функция f является функцией n переменных, которые обозначены через $x_1, \ldots, x_n$. Однако в теории булевых функций важным является не только зависимость функции от переменных, но и так называемая существенная зависимость функции от переменной. Прежде чем дать строгое определение этому понятию, посмотрим на «степень» зависимости функции от переменных на примерах функций $f_1(x_1, x_2), \ldots, f_{11}(x_1, x_2)$.

Функция $f_1(x_1, x_2)$ есть константа 0. Для этой функции любое изменение значений переменных не влечет за собой изменения значения функции. В этом смысле переменные x_1, x_2 можно было бы назвать несущественными для функции f_1. Аналогичное замечание следует сделать по поводу функции $f_2(x_1, x_2)$.

Несколько иная ситуация имеет место для функции $f_3(x_1, x_2)$. Поскольку значения функции $f_3(x_1, x_2)$ совпадают со значениями переменной x_1, значения переменной x_1 являются существенными для функции $f_3(x_1, x_2)$. Напротив, значения переменной x_2 никак не влияют на значения функции $f_3(x_1, x_2)$. Таким образом, переменную x_2 следует считать несущественной для функции $f_3(x_1, x_2)$.

Аналогичные рассуждения можно провести для функций f_4, f_5, f_6 и прийти к выводу, что переменная x_1 является существенной для функции $f_5(x_1, x_2)$ и несущественной для функций $f_4(x_1, x_2)$, $f_6(x_1, x_2)$, а переменная x_2 — существенной для функций $f_4(x_1, x_2)$, $f_6(x_1, x_2)$ и несущественной для функции $f_5(x_1, x_2)$.

Обратимся теперь к конъюнкции $f_7(x_1, x_2)$. Нетрудно заметить, что обе переменные x_1, x_2 являются для нее существенными. В самом деле, из равенств $f_7(0, 1) = 0$, $f_7(1, 1) = 1$ следует, что при фиксированном значении 1 переменной x_2 изменение значения переменной x_1 влечет за собой изменение значения функции. Следовательно, переменная x_1 является существенной для функции $f_7(x_1, x_2)$. Аналогичным образом, рассматривая наборы $(1, 0)$ и $(1, 1)$, убеждаемся в существенности переменной x_2.

Отметим еще, что у селекторной функции $e_i^n(x_1, \ldots, x_i, \ldots, x_n)$ единственной существенной переменной является переменная x_i.

Дадим теперь строгое определение существенной зависимости функции от переменной.

Функция $f(x_1, \ldots, x_i, \ldots, x_n)$ *существенно зависит* от переменной x_i, если найдутся такие значения $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Приведенному определению существенной зависимости можно придать несколько иную форму.

Функция $f(x_1, \ldots, x_i, \ldots, x_n)$ *существенно зависит от переменной* x_i, если найдутся такие значения $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что функция одной переменной $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, x_n)$ не является константой (т.е. совпадает с одной из функций x_i или $\overline{x}_i$).

Если функция $f(x_1, \ldots, x_n)$ существенно зависит от переменной x_i, то переменная x_i называется *существенной переменной* функции $f(x_1, \ldots, x_n)$. В противном случае переменная x_i называется *несущественной* или *фиктивной переменной* функции $f(x_1, \ldots, x_n)$.

Из определения существенной зависимости видно, что при вычислении значений функции реально используются лишь значения существенных переменных. В связи с этим возникает желание освободиться от «ненужных» фиктивных переменных. Если, например, известно, что существенными переменными булевой функции $f(x_1, \ldots, x_n)$ являются переменные $x_1, \ldots, x_m$ $(m < n)$, а переменные $x_{m+1}, \ldots, x_n$ фиктивны, то избавиться в функции $f(x_1, \ldots, x_n)$ от фиктивных переменных $x_{m+1}, \ldots, x_n$ можно различными способами. Один из них состоит в том, чтобы значения функции f рассматривать только на наборах $(a_1, \ldots, a_n)$, у которых $a_{m+1} = \ldots = a_n = 0$. Это соответствует подстановке константы 0 на места переменных $x_{m+1}, \ldots, x_n$: $f(x_1, \ldots, x_m, 0, \ldots, 0)$. При другом способе переменным $x_{m+1}, \ldots, x_n$ придают значения какой-либо из переменных $x_1, \ldots, x_m$, например переменной x_1. Как говорят в таких случаях, переменные $x_{m+1}, \ldots, x_n$ *отождествляют* с переменной x_1: $f(x_1, \ldots, x_m, x_1, \ldots, x_1)$. Возможны, разумеется, и любые комбинации подобных способов.

На практике нередко встречается обратная задача. Имеется функция $g(x_1, \ldots, x_m)$ и требуется «добавить» к ней фиктивные переменные $x_{m+1}, \ldots, x_n$. В этом случае искомую

функцию $f(x_1, \ldots, x_n)$ можно определить равенством

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = g(x_1, \ldots, x_m),$$

которое следует считать верным при любых значениях переменных $x_1, \ldots, x_n$. Однако более «грамотный» способ введения фиктивных переменных заключается в использовании селекторных функций. Именно, рассмотренный переход от функции g к функции f выполняется с помощью «регулярной» подстановки селекторных функций в функцию g:

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = \\ = g(e_1^n(x_1, \ldots, x_n), \ldots, e_m^n(x_1, \ldots, x_n)).$$

В заключение параграфа рассмотрим вопрос о сохранении существенной зависимости при подстановке одной функции в другую. Для упрощения рассуждений будем предполагать, что функции $f(x_1, \ldots, x_n, x_{n+1})$ и $g(x_1, \ldots, x_m)$ зависят существенно от каждой из своих переменных. Определим функцию h с помощью подстановки

$$h(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}) = f(x_1, \ldots, x_n, g(x_{n+1}, \ldots, x_{n+m})),$$

где переменные $x_{n+1}, \ldots, x_{n+m}$ отличны от переменных $x_1, \ldots$ $\ldots, x_n$. Докажем, что все переменные функции h являются существенными.

Вначале рассмотрим переменные $x_1, \ldots, x_n$. Возьмем, например, переменную x_1. Ввиду существенной зависимости функции f от переменной x_1 найдутся такие значения $a_2, \ldots, a_n, b$ переменных $x_2, \ldots, x_n, x_{n+1}$, что функция $f(x_1, a_2, \ldots, a_n, b)$ отлична от константы. Однако функция g существенно зависит от всех своих переменных. В частности, она отлична от константы. Поэтому найдутся такие значения $a_{n+1}, \ldots, a_{n+m}$ переменных $x_{n+1}, \ldots, x_{n+m}$, что $g(a_{n+1}, \ldots, a_{n+m}) = b$. Следовательно, функция $h(x_1, a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+m})$ также будет отлична от константы. Тем самым установлено, что переменная x_1 является существенной для функции h.

Перейдем к переменным $x_{n+1}, \ldots, x_{n+m}$. Выберем, например, переменную x_{n+m}. В силу существенной зависимости функции f от переменной x_{n+1} найдутся такие значения $a_1, \ldots, a_n$ переменных $x_1, \ldots, x_n$, что функция $f(a_1, , \ldots, a_n, x_{n+1})$ отлична от константы. Аналогично, для функции g выбираем такие значения $a_{n+1}, \ldots, a_{n+m-1}$ переменных $x_{n+1}, \ldots, x_{n+m-1}$, что функция $g(a_{n+1}, \ldots, a_{n+m-1}, x_{n+m})$ отлична от константы. Тогда, конечно, функция $f(a_1, \ldots, a_n, g(a_{n+1}, \ldots, a_{n+m-1}, x_{n+m}))$ будет также отлична от константы.

§ 4. Формулы и реализация булевых функций формулами

Табличный способ является универсальным способом задания булевых функций. В нем в самой простой форме отражена функциональная зависимость значений функции от значений аргументов. Однако в математике часто возникает необходимость установить функциональные связи между значениями функции для нескольких наборов значений аргументов либо между значениями различных функций. Табличный способ для этих целей, как правило, не подходит. Обычно для этого используют формулы различных типов.

Самые простые формулы обобщают идею перехода от значений аргументов к значениям функции и допускают использование других функций в качестве аргументов. Например, в элементарной алгебре формула

$$(x_1 + x_2) \cdot x_2 + x_1 \cdot x_3, \tag{1.1}$$

составленнная из символов переменных x_1, x_2, x_3 и символов функций $+$ и $\cdot$, указывает на последовательность действий (правда, не всегда однозначно) при вычислении функции, представленной этой формулой: сначала вычисляем $x_1 + x_2$, затем $(x_1 + x_2) \cdot x_2$, далее $x_1 \cdot x_3$ и, наконец, $(x_1 + x_2) \cdot x_2 + x_1 \cdot x_3$. При этом функции $+$ и $\cdot$ в формуле (1.1) считаются известными, «элементарными», а формула (1.1) лишь организует процесс вычисления значений функции, представленной этой формулой, исходя из значений переменных x_1, x_2, x_3 и используя заданные функции $+$ и $\cdot$.

Переходя к булевым функциям, предположим, что имеется непустое множество F булевых функций (возможно, бесконечное). Мы хотим ввести понятие формулы, составленной из символов функций множества F (как говорят, *формулы над* множеством F). Сразу отметим, что нам не важно, какие именно функции входят в множество F и как они заданы. Нам важно лишь то, что каждая функция из F имеет собственное «имя» — индивидуальное обозначение.

Индукцией по построению определим понятие *формулы над* F. Пусть f есть обозначение функции от n переменных из множества F, а $x_1, \ldots, x_n$ — символы переменных. Тогда выражение $f(x_1, \ldots, x_n)$ считаем формулой над F. Пусть далее g есть обозначение функции от m переменных из множества F, а $A_1, \ldots, A_m$ — либо формулы над F, либо символы переменных

(не обязательно различные). Тогда выражение $g(A_1, \ldots, A_m)$ считаем формулой над F.

В качестве примера рассмотрим множество F функций, состоящее из функций $-$ (отрицание), $\cdot$ (конъюнкция), $\vee$ (дизъюнкция), $\oplus$ (сложение по модулю 2), $\to$ (импликация), $|$ (штрих Шеффера). Тогда, согласно определению, следующие выражения будут являться формулами над F:

$$\overline{x}_3, \quad (x_2 \vee \overline{x}_1) \cdot x_4,$$
$$(\overline{x}_2 \cdot (x_3 \cdot \overline{x}_1)) \oplus \overline{(\overline{x}_3 \vee (x_1 \cdot x_5))}, \quad ((x_3 \cdot \overline{x}_2) \to \overline{(x_1 \cdot x_4)})|x_1,$$
$$((x_4|\overline{x}_2) \to \overline{(x_3 \oplus x_5)}) \to ((\overline{x}_1 \vee \overline{x}_2) \to x_4)$$

(чтобы не усложнять вид формул, мы не пишем скобки при использовании отрицаний над переменными).

Понятно, что формулы предназначены для задания булевых функций. Понятно также, что функцию, задаваемую (реализуемую) формулой, следует определять по индукции параллельно определению формулы над F.

Итак, если f есть обозначение функции от n переменных из F, то формула $f(x_1, \ldots, x_n)$ реализует ту самую функцию от переменных $x_1, \ldots, x_n$, обозначением которой служит f. (Этот пункт определения может показаться несколько туманным или даже содержащим противоречие. Однако следует, видимо, еще раз обратить внимание на то, что функция — это отображение одного множества в другое, если угодно, алгоритм или процесс. Тогда как f есть всего лишь обозначение этой функции, ее «имя».)

Пусть теперь g — обозначение функции от m переменных из F, а $A_1, \ldots, A_m$ — формулы над F либо символы переменных. И пусть каждому выражению A_i, которое представляет собой формулу над F, уже сопоставлена функция h_i, реализуемая этой формулой. Если же выражение A_i представляет собой символ переменной x_j, то сопоставим ему тождественную функцию $h_i(x_j)$, значения которой сопадают со значениями переменной x_j. Тогда формула $g(A_1, \ldots, A_m)$ реализует функцию

$$g(h_1, \ldots, h_m). \tag{1.2}$$

Сделаем два замечания по поводу определения функции (1.2). Во-первых, по понятным техническим причинам мы не выписываем переменные, от которых зависят функции $h_1, \ldots, h_m$: у каждой функции h_i могут быть свои переменные, не совпадающие, вообще говоря, с переменными других функций h_k. Здесь для «выравнивания» числа переменных

у различных функций h_i может быть полезно введение фиктивных переменных, о котором мы говорили в предыдущем параграфе.

Во-вторых, при вычислении значений функции (1.2) необходимо учитывать порядок переменных, от которых зависит функция (1.2). В соответствующую формулу $g(A_1, \ldots, A_m)$ входят не обязательно переменные из начала последовательности $x_1, x_2, \ldots$. Поэтому если $x_{i_1}, \ldots, x_{i_n}$ — все переменные данной формулуы и $i_1 < \ldots < i_n$, то при вычислении значения функции (1.2) на двоичном наборе $(a_1, \ldots, a_n)$ переменной x_{i_j} $(1 \leqslant j \leqslant n)$ следует придать значение a_j. Впрочем, формула $g(A_1, \ldots, A_m)$ может быть частью другой формулы; тогда процедуру придания значений переменным необходимо будет проводить для всех переменных этой большей формулы.

Если функция f реализуется формулой, которая составлена только из символов функций $f_1, \ldots, f_s$ (а также символов переменных), то говорят, что функция f является *суперпозицией функций* $f_1, \ldots, f_s$ или что f получена суперпозицией функций $f_1, \ldots, f_s$.

Отметим один частный случай суперпозиции. Пусть f — n-местная функция и $1 \leqslant i < j \leqslant n$. О функции $f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n)$ говорим, что она получена из функции $f(x_1, \ldots, x_n)$ *отождествлением* (или в результате отождествления) переменных x_i, x_j. Термин «отождествление переменных» используем и в более сложных случаях, когда операция отождествления двух переменных применяется многократно.

§ 5. Эквивалентность формул

Из элементарной алгебры известно, что одну и ту же функцию можно задать различными формулами. Так например, формула (1.1) задает ту же функцию, что и формула

$$x_1 \cdot (x_2 + x_3) + x_2^2. \tag{1.3}$$

Этот факт обычно выражают в виде высказывания «формула (1.2) эквивалентна формуле (1.3)».

Аналогичным образом обстоит дело и в теории булевых функций: формулы Φ и Ψ называются *эквивалентными*, если они реализуют одну и ту же булеву функцию. Мы не вводим специального знака для обозначения эквивалентности формул. Если формулы Φ и Ψ эквивалентны, то будем записывать это в виде $\Phi = \Psi$.

Для функций от одной и двух переменных, определенных в § 2, можно выписать большое число связывающих их эквивалентностей. Ниже приводятся лишь наиболее употребительные из них.

1. $\overline{1} = x \cdot 0 = x \cdot \overline{x} = x \oplus x = 0$.
2. $\overline{0} = x \vee 1 = x \vee \overline{x} = x \to x = 1$.
3. $\overline{\overline{x}} = x \cdot x = x \vee x = x \cdot 1 = x \vee 0 = x \oplus 0 = x$.
4. $x \oplus 1 = x \to 0 = x|x = \overline{x}$.
5. $x \circ y = y \circ x$, где $\circ$ есть любая из функций $\cdot, \vee, \oplus, |$ (*коммутативность функции* $\circ$).
6. $(x \circ y) \circ z = x \circ (y \circ z)$, где $\circ$ есть любая из функций $\cdot, \vee, \oplus$ (*ассоциативность* функции $\circ$).
7. $x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)$ (*дистрибутивность* конъюнкции относительно дизъюнкции).
8. $x \vee (y \cdot z) = (x \vee y) \cdot (x \vee z)$ (*дистрибутивность* дизъюнкции относительно конъюнкции).
9. $x \cdot (y \oplus z) = (x \cdot y) \oplus (x \cdot z)$ (*дистрибутивность* конъюнкции относительно сложения по модулю 2).
10. $\overline{x \cdot y} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x} \cdot \overline{y}$ (*правила де Моргана*).
11. $x \vee (x \cdot y) = x \cdot (x \vee y) = x$ (*правила поглощения*).
12. $x \oplus y = (\overline{x} \cdot y) \vee (x \cdot \overline{y}) = (x \vee y) \cdot (\overline{x} \vee \overline{y})$,
$x \vee y = ((x \cdot y) \oplus x) \oplus y = \overline{x} \to y$,
$x \to y = \overline{x} \vee y = ((x \cdot y) \oplus x) \oplus 1$,
$x|y = \overline{x \cdot y}$.

Справедливость эквивалентностей 1–12 можно проверить непосредственно, используя табл. 2 и табл. 3.

Чтобы несколько упростить написание формул, часть скобок обычно опускают. При этом руководствуются следующими соглашениями. Самые внешние скобки у формул не ставятся. При использовании отрицания скобки также не ставятся (читатель мог заметить, что мы уже применяли эти соглашения). Далее, свойства ассоциативности 6 позволяют при многократном применении одной и той же функции $\cdot, \vee$ или $\oplus$ опускать внутренние скобки. Если формула содержит символы функций $\cdot, \oplus, \vee, \to, |$, то при отсутствии дополнительных скобок сначала выполняют конъюнкцию, затем сложение по модулю 2, далее дизъюнкцию и, наконец, импликацию или штрих Шеффера. Например, формулу

$$\overline{x} \cdot y \oplus z \to \overline{y} \cdot z \vee \overline{x}$$

следует понимать так:

$$((\overline{x} \cdot y) \oplus z) \to ((\overline{y} \cdot z) \vee \overline{x}).$$

§ 6. Замыкание. Замкнутые классы

Одной из центральных проблем в теории булевых функций является проблема выразимости (определимости). В общем виде ее можно сформулировать так. Имеются некоторое непустое множество F булевых функций и булева функция f. Спрашивается, выразима ли функция f через функции множества F?

Чтобы дать ответ на поставленный вопрос, необходимо сначала уточнить, что понимается под выразимостью функции через другие функции. Самой распространенной формой выразимости для булевых функций является выразимость с помощью формул. Более точно, будем говорить, что булева функция f *выразима через функции множества* F, если существует формула над F, которая реализует функцию f. Совокупность всех функций, выразимых через функции множества F (т.е. реализуемых формулами над F), обозначим через $[F]$.

Часто операцию порождения одних булевых функций через другие с помощью формул называют операцией *суперпозиции*. Соответственно этому множество $[F]$ называют *замыканием* множества F относительно (операции) суперпозиции или просто замыканием F. Из определения легко усматриваются следующие свойства замыкания (называемые также *аксиомами замыкания*).

1. $F \subseteq [F]$.
2. Если $F_1 \subseteq F_2$, то $[F_1] \subseteq [F_2]$.
3. $[[F]] = [F]$.

Если для множества булевых функций F выполняется равенство $F = [F]$, то F называют или *замкнутым множеством*, или *замкнутым классом*, или *классом Поста*. Из свойств замыкания легко вывести, что пересечение конечного числа замкнутых классов есть замкнутый класс.

Рассмотрим некоторые примеры замкнутых классов. Прежде всего, очевидно, что замкнутым классом является множество P_2 всех булевых функций. Следующий пример связан с селекторными функциями. Обозначим через U_{01} множество всех селекторных функций $e_i^n(x_1, \ldots, x_n)$ $(1 \leqslant i \leqslant n,\ n = 1, 2, \ldots)$. Чтобы убедиться в том, что U_{01} образует замкнутый класс, достаточно проанализировать «первый» шаг в определении формулы над U_{01}, когда в селекторную функцию $e_i^n(x_1, \ldots, x_n)$ на места переменных $x_1, \ldots, x_n$ подставляются выражения $A_1, \ldots, A_n$, которые являются либо селекторными функциями, либо символами переменных. Понятно, что значения функции $e_i^n(A_1, \ldots, A_n)$ будут

совпадать со значениями выражения A_i. Однако значения A_i также совпадают со значениями некоторой переменной. Следовательно, $e_i^n(A_1, \ldots, A_n)$ — селекторная функция.

Обозначим через C_0 множество всех булевых функций (от любого числа переменных), тождественно равных 0. Очевидно, что суперпозициями функций из множества C_0 можно получить лишь функцию, тождественно равную 0. Поэтому C_0 — замкнутый класс. Аналогично получаем, что замкнутым классом является множество C_1 всех булевых функций, тождественно равных 1.

Пусть T_0 есть множество всех булевых функций $f(x_1, \ldots, x_n)$, которые *сохраняют константу* 0, т.е. удовлетворяют равенству $f(0, \ldots, 0) = 0$. Покажем, что T_0 — замкнутый класс. Для этого так же, как и для класса U_{01}, достаточно проверить, что функция $g(y_1, \ldots, y_m)$ принадлежит классу T_0, если $g(y_1, \ldots, y_m)$ реализуется формулой $f(A_1, \ldots, A_n)$, в которой f — функция из T_0, а $A_1, \ldots, A_n$ — либо функции из T_0, либо символы переменных. Поскольку в множество T_0 входят все селекторные функции, а переменную также можно считать селекторной функцией, все выражения $A_1, \ldots, A_n$ можно считать зависящими от переменных $y_1, \ldots, y_m$, т.е.

$$f(A_1, \ldots, A_n) = f(h_1(y_1, \ldots, y_m), \ldots, h_n(y_1, \ldots, y_m)),$$

где функции $h_1, \ldots, h_n$ принадлежат классу T_0. Теперь легко убеждаемся в принадлежности функции g классу T_0: согласно определению функций $h_1, \ldots, h_n$ имеем

$$h_1(0, \ldots, 0) = \ldots = h_n(0, \ldots, 0) = 0,$$

а согласно определению функции f получаем $f(0, \ldots, 0) = 0$.

Подобным образом можно показать, что замкнутым классом является множество T_1 всех булевых функций, сохраняющих константу 1, т.е. функций $f(x_1, \ldots, x_n)$, удовлетворяющих равенству $f(1, \ldots, 1) = 1$.

Разумеется, далеко не каждое множество булевых функций представляет собой замкнутый класс. В качестве примера рассмотрим множество $\overline{U}_{01}$ всех «антиселекторных» функций $\overline{e}_i^n(x_1, \ldots, x_n)$,

$$\overline{e}_i^n(x_1, \ldots, x_i, \ldots, x_n) = \overline{x}_i.$$

В замыкание $[\overline{U}_{01}]$ по определению должна входить функция, реализуемая формулой $\overline{e}_1^1(\overline{e}_1^1(x))$. Нетрудно видеть, что эта

функция совпадает с функцией $e_1^1(x)$. Однако $e_1^1(x)$ не содержится в множестве $\overline{U}_{01}$. Значит, $\overline{U}_{01}$ не является замкнутым классом.

В дальнейшем нам придется особо выделять замкнутые классы, содержащие все селекторные функции. Такие замкнутые классы называются *клонами*. Отметим, что всякий клон очевидным образом замкнут относительно операции введения фиктивных переменных. По этой причине вместо «произвольной» операции суперпозиции в клонах можно рассматривать только «регулярную» суперпозицию.

С понятием замыкания тесно связано понятие полноты. Пусть теперь R — замкнутый класс, а Q — система функций из R. Говорят, что система функций Q *полна в классе* R, если $[Q] = R$. Когда R совпадает с P_2, слова «в классе P_2» обычно опускают.

Построение нетривиальных полных систем функций мы отложим до следующего параграфа. А пока докажем простое и вместе с тем полезное утверждение.

Теорема 1.1. *Пусть система булевых функций Q полна в замкнутом классе R, P — некоторое множество функций из R и любая функция системы Q реализуется формулой над P. Тогда множество P также полно в классе R.*

Доказательство. Возьмем произвольную функцию f из класса R. По условию теоремы ее можно реализовать некоторой формулой Φ над Q. В свою очередь, каждая функция из Q, которая участвует в построении формулы Φ, может быть реализована формулой над P. Заменим в формуле Φ вхождение каждого символа функции из Q соответствующей формулой над P. Мы получим формулу Φ' над P, которая, как легко понять, реализует ту же самую функцию f. Теорема доказана.

Если система функций Q полна в замкнутом классе R, то говорят также, что система Q *порождает* класс R, а класс R *порождается* системой Q.

Из определения замыкания видно, что замкнутый класс потенциально может содержать бесконечное число булевых функций. Разумеется, при задании такого класса мы не можем перечислить все входящие в него функции. В связи с этим хотелось бы иметь некоторый финитный способ описания замкнутых классов. Один из таких способов подсказывает понятие порождающей системы. Именно, назовем замкнутый класс R *конечно порождаемым*, если существует конечная система функций Q этого класса, которая порождает R.

Если класс R конечно порождаем, а конечная система Q порождает класс R, то путем удаления функций из системы Q можно получить наименьшую по числу функций систему Q', которая все еще порождает класс R. Такие минимальные системы Q' называются *базисами* класса R. Отметим (пока без доказательства), что для одного и того же класса R, отправляясь от различных порождающих систем Q, можно прийти, вообще говоря, к различным базисам, содержащим даже различное количество функций.

§ 7. Разложение булевой функции по переменным

Следующее утверждение имеет важное значение для всей теории булевых функций.

Теорема 1.2 (о разложении функции по первой переменной). *Для любой булевой функции* $f(x_1, \ldots, x_n)$ *справедливо представление*

$$f(x_1, \ldots, x_n) = x_1 \cdot f(1, x_2, \ldots, x_n) \vee \overline{x}_1 \cdot f(0, x_2, \ldots, x_n). \quad (1.4)$$

Доказательство. Возьмем произвольный двоичный набор $a = (a_1, \ldots, a_n)$ и сравним значения левой и правой частей равенства (1.4) на этом наборе. Слева мы имеем значение $f(a)$. Если $a_1 = 0$, то выражение $a_1 \cdot f(1, a_2, \ldots, a_n)$ из правой части обращается в 0. Поэтому правая часть будет равна

$$\overline{a}_1 \cdot f(0, a_2, \ldots, a_n) = \overline{0} \cdot f(a_1, a_2, \ldots, a_n) = 1 \cdot f(a) = f(a).$$

Аналогичным образом рассматриваем другую возможность, когда $a_1 = 1$. Теорема доказана.

Отметим, что в теореме 1.2 вместо первой переменной можно выбрать любую другую переменную.

Теорема 1.2 имеет целый ряд важных следствий. Во-первых, если при $n \geqslant 2$ ее применить далее к функциям $f(1, x_2, \ldots, x_n)$, $f(0, x_2, \ldots, x_n)$ и переменной x_2, то получим соотношение

$$\begin{aligned} f(x_1, \ldots, x_n) = \\ = x_1 \cdot x_2 \cdot f(1, 1, x_3, \ldots, x_n) \vee x_1 \cdot \overline{x}_2 \cdot f(1, 0, x_3, \ldots, x_n) \vee \\ \vee \overline{x}_1 \cdot x_2 \cdot f(0, 1, x_3, \ldots, x_n) \vee \overline{x}_1 \cdot \overline{x}_2 \cdot f(0, 0, x_3, \ldots, x_n). \end{aligned}$$

Вообще если ввести обозначения $x^1 = x$, $x^0 = \overline{x}$ и рассуждать далее по индукции, то получим следующее утверждение.

Следствие 1 (о разложении функции по первым m переменным). *Для любой булевой функции $f(x_1, \ldots, x_n)$ и любого m ($1 \leqslant m \leqslant n$) имеет место представление*

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_m)} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n). \quad (1.5)$$

Выражение $(\sigma_1, \ldots, \sigma_m)$ под знаком дизъюнкции в формуле (1.5) означает, что данная формула представляет собой дизъюнкцию 2^m слагаемых (по числу всех двоичных наборов длины m), каждое из которых имеет вид

$$x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n),$$

где x_i^1 должно быть заменено на x_i, а x_i^0 — на $\overline{x}_i$.

Особенно интересным следствие 1 оказывается при $m = n$. В этом случае каждое дизъюнктивное слагаемое в формуле (1.5) имеет вид

$$x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma_1, \ldots, \sigma_n). \quad (1.6)$$

Если $f(\sigma_1, \ldots, \sigma_n) = 0$, то слагаемое (1.6) равно 0. Поэтому в формуле (1.5) его можно опустить (исключение составляет единственный случай, когда функция f тождественно равна 0; тогда формула (1.5) вырождается в константу 0). Если же $f(\sigma_1, \ldots, \sigma_n) = 1$, то вместо формулы (1.6) можно написать эквивалентную формулу $x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$. Таким образом, мы приходим к следующему утверждению.

Следствие 2 (о разложении функции по всем переменным). *Если булева функция $f(x_1, \ldots, x_n)$ не равна тождественно* 0, *то имеет место представление*

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}. \quad (1.7)$$

Равенство $f(\sigma_1, \ldots, \sigma_n) = 1$ в формуле (1.7) говорит о том, что в формуле (1.7) присутствуют лишь те дизъюнктивные слагаемые $x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$, для которых $f(\sigma_1, \ldots, \sigma_n) = 1$.

Правая часть формулы (1.7) носит название *совершенной дизъюнктивной нормальной формы* (сокращенно СДНФ). Следствие 2 показывает, что любую не равную тождественно 0 булеву функцию можно представить в некоторой стандартной форме СДНФ, которая представляет собой дизъюнкцию конъюнкций

одинаковой длины, составленных из переменных $x_1, \ldots, x_n$ и их отрицаний. Для функции, тождественно равной 0, в качестве СДНФ рассматривают, например, формулу $x_1 \cdot \overline{x}_1$.

СДНФ относится к более общему классу формул над множеством $\{\overline{x}, xy, x \vee y\}$, которые носят название *дизъюнктивных нормальных форм* (сокращенно ДНФ). В отличие от СДНФ в произвольной ДНФ, которая также представляет собой дизъюнкцию конъюнкций, конъюнкции могут состоять из различных переменных и иметь различную длину. Так, первая из формул

$$xy \vee \overline{x}y \vee \overline{xy}, \quad \overline{x} \vee y$$

есть СДНФ, вторая — ДНФ. Обе формулы реализуют одну и ту же функцию $x \to y$. На этом иллюстративном примере видно, что ДНФ булевой функции может быть гораздо проще, чем ее СДНФ. Этим обстоятельством, а также сравнительной простотой строения ДНФ объясняется то внимание, которое уделяется изучению ДНФ в теории булевых функций.

Следствие 2 содержит еще одну важную информацию о классе P_2 всех булевых функций. Именно: формула (1.7) показывает, что каждую не равную 0 булеву функцию можно представить формулой над множеством функций $\{\overline{x}, xy, x \vee y\}$. Поскольку, как отмечалось, $0 = x \cdot \overline{x}$, мы получаем еще одно следствие из теоремы 1.2.

Следствие 3. *Система функций* $\{\overline{x}, xy, x \vee y\}$ *полна в классе* P_2.

Используя следствие 3 и теорему 1.1, докажем полноту следующих систем функций:

$$\{\overline{x}, xy\}, \quad \{\overline{x}, x \vee y\}, \quad \{1, x \oplus y, xy\}, \quad \{x|y\}.$$

Полнота первых двух систем вытекает из полноты системы $\{\overline{x}, xy, x \vee y\}$, теоремы 1.1 и правил де Моргана (см. п. 10 в § 5), согласно которым

$$x \vee y = \overline{(\overline{x} \cdot \overline{y})}, \quad x \cdot y = \overline{(\overline{x} \vee \overline{y})}.$$

Полнота третьей системы следует из полноты системы $\{\overline{x}, xy\}$, теоремы 1.1 и соотношения $\overline{x} = x \oplus 1$. Полнота четвертой системы следует из полноты системы $\{\overline{x}, xy\}$ и соотношений

$$\overline{x} = x|x, \quad xy = (x|y)|(x|y).$$

§ 8. Двойственность. Принцип двойственности

Каждому, кто знакомится с булевыми функциями, довольно быстро приходит в голову следующая мысль. Элементы 0,1 множества E_2 в общем-то равноправны. А что будет, если поменять их местами?

Эту мысль можно оформить вполне строгим образом и получить новое важное понятие. Именно: будем говорить, что функция $g(x_1, \ldots, x_n)$ является *двойственной* к функции $f(x_1, \ldots, x_n)$, если

$$g(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n). \tag{1.8}$$

Функция, двойственная к функции $f(x_1, \ldots, x_n)$, обозначается через $f^*(x_1, \ldots, x_n)$. Из определения (1.8) двойственной функции и тождества $\overline{\overline{x}} = x$ легко следует, что

$$f^{**}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

Таким образом, двойственные друг другу функции образуют пары (из приводимых далее примеров будет видно, что возможны случаи, когда $f^* = f$). В табл. 4 приведены некоторые пары двойственных функций.

Таблица 4

f	f^*
0	1
$e_i^n(x_1, \ldots, x_n)$	$e_i^n(x_1, \ldots, x_n)$
$\overline{x}$	$\overline{x}$
xy	$x \vee y$
$x \oplus y$	$x \oplus y \oplus 1 = \overline{x \oplus y}$
$x \to y$	$\overline{x \vee \overline{y}} = \overline{x}y = \overline{y \to x}$
$x \mid y$	$\overline{x \vee y} = \overline{x} \cdot \overline{y}$

Теорема 1.3. *Если*

$$f(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)), \tag{1.9}$$

то

$$f^*(x_1, \ldots, x_n) = g_0^*(g_1^*(x_1, \ldots, x_n), \ldots, g_m^*(x_1, \ldots, x_n)).$$

Доказательство. Согласно определению двойственной функции имеем

$$f^*(x_1,\dots,x_n)=\overline{g}_0(g_1(\overline{x}_1,\dots,\overline{x}_n),\dots,g_m(\overline{x}_1,\dots,\overline{x}_n)).$$

Заменим в правой части этого равенства каждую формулу $g_i(\overline{x}_1,\dots,\overline{x}_n)$ эквивалентной формулой $\overline{\overline{g}}_i(\overline{x}_1,\dots,\overline{x}_n)$:

$$f^*(x_1,\dots,x_n)=\overline{g}_0(\overline{\overline{g}}_1(\overline{x}_1,\dots,\overline{x}_n),\dots,\overline{\overline{g}}_m(\overline{x}_1,\dots,\overline{x}_n)).$$

Функция $\overline{g}_i(\overline{x}_1,\dots,\overline{x}_n)$ по определению есть функция $g_i^*(x_1,\dots,x_n)$. Поэтому

$$f^*(x_1,\dots,x_n)=\overline{g}_0(\overline{g}_1^*(x_1,\dots,x_n),\dots,\overline{g}_m^*(x_1,\dots,x_n)).$$

Вновь по определению получаем, что $\overline{g}_0(\overline{g}_1^*,\dots,\overline{g}_m^*)$ есть $g_0^*(g_1^*,\dots,g_m^*)$. Окончательно приходим к равенству

$$f^*(x_1,\dots,x_n)=g_0^*(g_1^*(x_1,\dots,x_n),\dots,g_m^*(x_1,\dots,x_n)).$$

Теорема доказана.

Следствие (принцип двойственности). *Если функция f реализуется формулой Φ, составленной из символов функций $g_1,\dots,g_m$, то двойственная функция f^* реализуется формулой Φ^*, которая получается из формулы Φ заменой каждого символа функции g_i $(1\leqslant i\leqslant m)$ символом двойственной функции g_i^*.*

Доказательство. Теорему 1.3 необходимо применять последовательно ко всем подформулам формулы Φ, «выравнивая», если требуется, количество переменных у функций за счет введения фиктивных переменных.

На практике принцип двойственности чаще всего применяют следующим образом. Если уже установлено некоторое утверждение о булевых функциях $f,g,\dots$ и множествах булевых функций $F,G,\dots$, в котором фигурируют лишь понятия, базирующиеся на формулах, то по принципу двойственности будет справедливо аналогичное утверждение о булевых функциях $f^*,g^*,\dots$ и множествах булевых функций $F^*,G^*,\dots$. При этом под F^* понимается множество всех булевых функций, двойственных к функциям из F.

Так например, доказав дистрибутивность конъюнкции относительно дизъюнкции (см. п. 7 из § 5), мы на основании принципа двойственности можем заключить о справедливости свойства дистрибутивности дизъюнкции относительно конъюнкции

(см. п. 8 из § 5). Аналогичное утверждение имеет место для двух правил де Моргана (см. п. 10 из § 5). Далее, на основе дистрибутивности конъюнкции относительно сложения по модулю 2 (см. п. 9 из § 5) можно получить новую эквивалентность

$$x \vee (y \oplus z \oplus 1) = (x \vee y) \oplus (x \vee z) \oplus 1.$$

С использованием принципа двойственности, теоремы 1.2 и ее следствий можно доказать несколько интересных утверждений. Во-первых, имеет место следующий аналог теоремы 2.

Теорема 1.2′. *Для любой булевой функции* $f(x_1, \ldots, x_n)$ *справедливо разложение*

$$f(x_1, \ldots, x_n) = (x_1 \vee f(0, x_2, \ldots, x_n)) \cdot (\overline{x}_1 \vee f(1, x_2, \ldots, x_n)).$$

Далее получаем разложение по n переменным.

Следствие 2′. *Если булева функция* $f(x_1, \ldots, x_n)$ *не равна тождественно* 1, *то имеет место представление*

$$f(x_1, \ldots, x_n) = \mathop{\&}_{f(\sigma_1, \ldots, \sigma_n)=0} (x_1^{\overline{\sigma}_1} \vee \ldots \vee x_n^{\overline{\sigma}_n}).$$

Правая часть этой формулы носит название *совершенной конъюнктивной нормальной формы* (сокращенно СКНФ). Так же, как и в случае СДНФ и ДНФ, СКНФ относится к более широкому классу *конъюнктивных нормальных форм* (сокращенно КНФ), которые представляют собой конъюнкции дизъюнкций переменных и их отрицаний.

§ 9. Полиномы Жегалкина

Как установлено в § 7, система $\{1, x \oplus y, x \cdot y\}$ полна в классе P_2. Это означает, что любую булеву функцию можно представить в виде формулы над множеством функций $\{1, x \oplus y, x \cdot y\}$. Преобразуем эту формулу, используя следующие эквивалентности из § 5: коммутативность сложения по модулю 2 и конъюнкции (умножения), дистрибутивность конъюнкции (умножения) относительно сложения (п. 9 слева направо),

$$x \cdot x = x \cdot 1 = x \oplus 0 = x, \quad x \cdot 0 = x \oplus x = 0.$$

Так же, как в элементарной алгебре, после выполнения этих преобразований мы получим формулу, которая имеет вид полинома: она представляет собой сумму по модулю 2 слагаемых

вида $x_{i_1} \cdot \ldots \cdot x_{i_s}$ и, быть может, константы 1 (в случаях, когда реализуемая полиномом функция тождественно равна 0 или 1, сумма вырождается в одно слагаемое 0 или 1). Эта формула носит название *полинома Жегалкина* (или полинома над полем Галуа $GF(2)$). Общий вид полинома Жегалкина для функции от n переменных может быть записан следующим образом:

$$\sum a_{i_1 \ldots i_s} \cdot x_{i_1} \cdot \ldots \cdot x_{i_s}. \tag{1.10}$$

Здесь $\sum$ означает сумму по модулю 2; суммирование распространяется по всем подмножествам $\{i_1, \ldots, i_s\}$ множества $\{1, 2, \ldots, n\}$, включая пустое подмножество $\varnothing$; коэффициенты $a_{i_1 \ldots i_s}$ принимают значения 0 или 1; при $a_{i_1 \ldots, i_s} = 0$ соответствующее слагаемое в полиноме (1.10) опускают. Наконец, если все коэффициенты $a_{i_1 \ldots i_s}$, включая коэффициент $a_\varnothing$, равны 0, то полином (1.10) записывают просто как 0.

На практике для построения полиномов Жегалкина чаще всего прибегают к методу неопределенных коэффициентов. Пусть нам требуется построить полином Жегалкина для функции $f(x, y, z)$, заданной двоичным набором (10011100). Запишем функцию $f(x, y, z)$ в виде полинома Жегалкина с неопределенными коэффициентами $a_0, \ldots, a_7$:

$$f(x, y, z) = a_0 \oplus a_1 x \oplus a_2 y \oplus a_3 z \oplus a_4 xy \oplus a_5 xz \oplus a_6 yz \oplus a_7 xyz. \tag{1.11}$$

Подставляя в функцию $f(x, y, z)$ последовательно наборы $(0, 0, 0), (0, 0, 1), \ldots, (1, 1, 1)$ и пользуясь известными значениями функции f, из (1.11) получаем следующую систему уравнений для коэффициентов $a_0, \ldots, a_7$ (слева в скобках указан набор значений переменных x, y, z, приводящий к данному соотношению):

$$\begin{array}{ll}
(0,0,0) & a_0 = 1, \\
(0,0,1) & a_0 \oplus a_3 = 0, \\
(0,1,0) & a_0 \oplus a_2 = 0, \\
(0,1,1) & a_0 \oplus a_2 \oplus a_3 \oplus a_6 = 1, \\
(1,0,0) & a_0 \oplus a_1 = 1, \\
(1,0,1) & a_0 \oplus a_1 \oplus a_3 \oplus a_5 = 1, \\
(1,1,0) & a_0 \oplus a_1 \oplus a_2 \oplus a_4 = 0, \\
(1,1,1) & a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0.
\end{array}$$

Решим ее, исключая последовательно неизвестные $a_0, \ldots, a_7$. Первое уравнение дает $a_0 = 1$, второе, третье и пятое дают $a_1 = 0$, $a_2 = a_3 = 1$. Используя далее найденные значения коэффициентов a_0, a_1, a_2, a_3, рассматриваем четвертое, шестое

и седьмое уравнения. Из них находим, что $a_4 = a_6 = 0$, $a_5 = 1$. Подставляя полученные значения в восьмое уравнение, получаем $a_7 = 0$. Окончательно полином Жегалкина для функции $f(x, y, z)$ имеет вид $1 \oplus y \oplus z \oplus xz$.

Теорема 1.4. *Любая булева функция реализуется единственным* (*с точностью до перестановок слагаемых и сомножителей в слагаемых*) *полиномом Жегалкина.*

Доказательство. В самом деле, подсчитаем число коэффициентов $a_{i_1 \ldots i_s}$ в общей формуле (1.10) полинома Жегалкина для функции от n переменных. Это число равно числу всевозможных (включая пустое) подмножеств множества $\{1, 2, \ldots, n\}$, т.е. равно 2^n. Понятно, что число различных полиномов Жегалкина вида (1.10) (при условии, что мы не различаем полиномы, которые получаются друг из друга перестановкой слагаемых или перестановкой сомножителей в слагаемых) равно числу всевозможных способов, которыми мы можем придать значения 0 и 1 коэффициентам $a_{i_1 \ldots i_s}$ полинома (1.10). Следовательно, получаем величину 2^{2^n} для числа полиномов Жегалкина от n переменных.

Итак, для каждой булевой функции от n переменных имеется хотя бы один полином Жегалкина, который реализует эту функцию; вместе с тем, число различных полиномов Жегалкина от n переменных равно числу всех булевых функций от n переменных. Это означает, что для любой булевой функции существует только один реализующий ее полином Жегалкина. Теорема доказана.

Отметим одну важную особенность полиномов Жегалкина: функция $f(x_1, \ldots, x_n)$ существенно зависит от переменной x_i тогда и только тогда, когда переменная x_i входит хотя бы в одно слагаемое полинома Жегалкина, реализующего функцию f (еще раз напомним, что в полиноме Жегалкина присутствуют лишь слагаемые, не равные тождественно 0). В самом деле, если функция $f(x_1, \ldots, x_n)$ не зависит существенно от переменной x_i, то полином Жегалкина, реализующий функцию $f(x_1, \ldots, x_n)$, можно построить следующим образом. Сначала удалением из функции $f(x_1, \ldots, x_n)$ несущественной переменной x_i образуем функцию $f'(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, затем строим полином Жегалкина Φ, который реализует функцию f'. Понятно, что ввиду несущественности переменной x_i полином Жегалкина Φ, рассматриваемый от всех переменных $x_1, \ldots, x_n$, будет также реализовать и функцию $f(x_1, \ldots, x_n)$.

Обратно: если переменная x_i не входит ни в одно слагаемое полинома Жегалкина Ф, реализующего функцию $f(x_1, \ldots, x_n)$, то, очевидно, значения переменной x_i не играют никакой роли при вычислении значений функции $f(x_1, \ldots, x_n)$ согласно формуле Ф. Поэтому переменная x_i является несущественной для функции $f(x_1, \ldots, x_n)$.

Комментарии. Булевы функции (функции алгебры логики) названы по имени английского математика и логика Дж. Буля (G. Boole, 1815–1864), применявшего данные функции при математической постановке задач логики. Полиномы Жегалкина (полиномы над полем Галуа $GF(2)$) предложены русским математиком и логиком И. И. Жегалкиным (1869–1947) в качестве удобного средства для представления функций алгебры логики. Теорему 1.4 называют теоремой Жегалкина.

Глава II

ЗАМКНУТЫЕ КЛАССЫ И КРИТЕРИЙ ПОЛНОТЫ

§ 1. Класс самодвойственных функций

Булеву функцию $f(x_1, \ldots, x_n)$ назовем *самодвойственной*, если

$$f(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n). \tag{2.1}$$

Для самодвойственной функции $f(x_1, \ldots, x_n)$ равенство (2.1) можно записать также в виде

$$\overline{f}(x_1, \ldots, x_n) = f(\overline{x}_1, \ldots, \overline{x}_n).$$

Из него следует, что самодвойственная функция f на любых двух противоположных наборах $(a_1, \ldots, a_n)$, $(\overline{a}_1, \ldots, \overline{a}_n)$ принимает противоположные значения.

Из табл. 4 видно, что самодвойственными являются функции $\overline{x}$ и $e_i^n(x_1, \ldots, x_n)$. Интересно отметить, что не существует самодвойственных функций $f(x_1, x_2)$, существенно зависящих от обеих переменных. В самом деле, если f — самодвойственная функция, то $f(0,0) = \overline{f}(1,1)$ и $f(0,1) = \overline{f}(1,0)$. Следовательно, функция f полностью определяется своими значениями на наборах $(0,0)$ и $(0,1)$. Рассматривая все четыре возможных варианта, убеждаемся, что функция $f(x_1, x_2)$ совпадает с одной из функций $e_1^2(x_1, x_2)$, $e_2^2(x_1, x_2)$, $\overline{e}_1^2(x_1, x_2)$, $\overline{e}_2^2(x_1, x_2)$, каждая из которых существенно зависит только от одной переменной.

Обозначим через S множество всех самодвойственных булевых функций. Докажем, что S образует замкнутый класс.

Поскольку селекторные функции являются самодвойственными, достаточно проверить, что из принадлежности классу S функций $g_0, g_1, \ldots, g_m$ вытекает принадлежность классу S функции f, заданной равенством (1.9). Однако это непосредственно следует из принципа двойственности.

На примере самодвойственных функций интересно еще раз проследить идею подсчета функций от n переменных с помощью таблицы. Рассмотрим табл. 1 и отметим следующий факт: противоположные наборы $(a_1, \ldots, a_n)$, $(\overline{a}_1, \ldots, \overline{a}_n)$ располагаются в ней на равных расстояниях от середины таблицы (которая проходит между 2^{n-1}-м набором $(0, 1, \ldots, 1)$ и $(2^{n-1} + 1)$-м

набором $(1, 0, \ldots, 0)$). Вспомним, что самодвойственная функция принимает противоположные значения на противоположных наборах. Таким образом, для полного задания самодвойственной функции $f(x_1, \ldots, x_n)$ достаточно указать ее значения либо на наборах из верхней половины таблицы, либо на наборах из нижней половины. Следовательно, число самодвойственных булевых функций от n переменных равно

$$2^{2^{n-1}} = 2^{\frac{1}{2}\cdot 2^n} = \sqrt{2^{2^n}}\,.$$

Иными словами, это число есть корень квадратный из числа всех булевых функций от n переменных.

Класс самодвойственных функций играет важную роль при решении проблемы полноты в классе P_2. Следующее утверждение, необходимое для ее решения, имеет также и некоторый самостоятельный интерес.

Лемма 2.1 (о несамодвойственной функции). *Из несамодвойственной функции с помощью подстановки функций x и $\overline{x}$ на места всех ее переменных можно получить несамодвойственную функцию от одной переменной, т.е. константу* 0 *или* 1.

Доказательство. Пусть функция $f(x_1, \ldots, x_n)$ несамодвойственна. Тогда найдется такая пара противоположных наборов $(a_1, \ldots, a_n)$ и $(\overline{a}_1, \ldots, \overline{a}_n)$, что

$$f(a_1, \ldots, a_n) = f(\overline{a}_1, \ldots, \overline{a}_n). \tag{2.2}$$

Подставим в функцию $f(x_1, \ldots, x_n)$ вместо переменной x_i $(1 \leqslant i \leqslant n)$ функцию $x \oplus a_i$ (т. е. функцию x или функцию $\overline{x}$). Полученную после подстановки функцию обозначим через $g(x)$. Согласно определению будем иметь

$$g(0) = f(a_1, \ldots, a_n),$$
$$g(1) = f(1 \oplus a_1, \ldots, 1 \oplus a_n) = f(\overline{a}_1, \ldots, \overline{a}_n).$$

Обращаясь к равенству (2.2), видим, что $g(0) = g(1)$, т. е. $g(x)$ — константа. Лемма доказана.

§ 2. Класс линейных функций

Булеву функцию $f(x_1, \ldots, x_n)$ назовем *линейной*, если ее полином Жегалкина (1.10) не содержит нелинейных слагаемых. Множество всех линейных функций обозначим через L.

Из определения следует, что всякую линейную функцию $f(x_1, \ldots, x_n)$ можно представить в виде

$$a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n, \tag{2.3}$$

где коэффициенты $a_0, a_1, \ldots, a_n$ равны 0 или 1. Представление (2.3) позволяет легко подсчитать число линейных функций, зависящих от n переменных. В самом деле, придавая коэффициентам $a_0, a_1, \ldots, a_n$ различные значения 0 и 1, мы будем получать различные линейные функции. Следовательно, число линейных функций, зависящих от n переменных, равно числу двоичных наборов длины $n+1$, т. е. равно 2^{n+1}.

Часто бывает полезным тот факт, что все четыре булевы функции от одной переменной 0, 1, x, $\overline{x} = x \oplus 1$ линейны и все селекторные функции также линейны.

Не представляет особого труда убедиться в том, что L является замкнутым классом (при этом следует иметь в виду, что при подстановке линейных функций в линейную функцию суммы коэффициентов рассматриваются по модудю 2 и, следовательно, дают в итоге значения 0 и 1).

Отметим, что класс L порождается системой функций $\{1, x \oplus y\}$. В самом деле, имеем $0 = 1 \oplus 1$. Суперпозициями функции $x \oplus y$ можно получить любую функцию вида $x_1 \oplus \ldots \oplus x_n$, где $n \geqslant 1$, а с использованием константы 1 — также и любую функцию вида $x_1 \oplus \ldots \oplus x_n \oplus 1$.

Булева функция, которая не является линейной, называется *нелинейной*. Полином Жегалкина нелинейной булевой функции включает хотя бы одно слагаемое, содержащее не менее двух сомножителей. Для определения линейности (нелинейности) булевой функции универсальным средством является представление функции в виде полинома Жегалкина. Однако в некоторых случаях о нелинейности функции можно судить по виду двоичного набора, задающего данную функцию. Так, отличная от константы булева функция будет заведомо нелинейной, если значение 1 (или 0) она принимает не на половине всех наборов. Это утверждение легко выводится из следующего факта: если булева функция f от n переменных линейна и отлична от константы, то значение 1 (и значение 0) она принимает ровно на 2^{n-1} наборах.

Чтобы это доказать, выделим в представлении (2.3) линейной функции f только ненулевые слагаемые. Получим функцию $x_{i_1} \oplus \ldots \oplus x_{i_m}$ либо функцию $1 \oplus x_{i_1} \oplus \ldots \oplus x_{i_m}$. Первая функция принимает значение 1 на всех наборах (длины m) с нечетным числом единиц, вторая — с четным числом единиц. Число двоичных наборов длины m с четным (нечетным) числом

единиц равно 2^{m-1}. Остается заметить, что при добавлении в функцию фиктивной переменной x_i (ей в представлении (2.3) отвечает нулевое слагаемое $a_i x_i$) число единиц функции (равно как и число ее нулей) умножается на 2.

В дальнейшем нам понадобится следующее утверждение о возможности понижения числа переменных у нелинейной функции.

Лемма 2.2 (о нелинейной функции). *Из всякой нелинейной булевой функции подстановкой вместо всех ее переменных функций* $0, x, y$ *можно получить нелинейную функцию от переменных* x, y.

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin L$. Тогда в полиноме Жегалкина функции f есть нелинейное слагаемое. Выберем нелинейное слагаемое наименьшей степени. Пусть например, оно имеет вид $x_1 \cdot \ldots \cdot x_k$, где $k \geqslant 2$. Заменим в функции $f(x_1, \ldots, x_n)$ переменную x_1 переменной x, переменные $x_2, \ldots, x_k$ — переменной y, а все остальные переменные — константой 0. Полученную функцию обозначим $g(x, y)$. В силу минимальности степени слагаемого $x_1 \cdot \ldots \cdot x_k$ полином Жегалкина функции $g(x, y)$ примет вид $x \cdot y \oplus ax \oplus by \oplus c$, где $a, b, c \in E_2$. Таким образом, $g \notin L$. Лемма доказана.

§ 3. Класс монотонных функций

Монотонно не убывающая функция — это функция, значения которой не убывают с увеличением значений аргумента. Это определение легко применить для булевых функций одной переменной, вводя на множестве E_2 естественный порядок $0 \leqslant 1$. При переходе к функциям многих переменных можно либо потребовать монотонность по каждой переменной, либо определить на декартовых степенях множества E_2 частичный порядок, индуцированный порядком $0 \leqslant 1$, и рассматривать далее монотонность относительно данного частичного порядка. Оба подхода приводят к одному и тому же классу монотонных булевых функций.

При любом n определим частичный порядок на множестве E_2^n всех двоичных наборов длины n. Считаем, что набор $(a_1, \ldots, a_n)$ не превосходит набора $(b_1, \ldots, b_n)$, если для любого i $(1 \leqslant i \leqslant n)$, выполняется неравенство $a_i \leqslant b_i$. Этот факт записываем в виде

$$(a_1, \ldots, a_n) \leqslant (b_1, \ldots, b_n). \tag{2.4}$$

Отметим, что при $n \geqslant 2$ введенное отношение частичного порядка не является отношением линейного порядка, например, наборы (0,1) и (1,0) не сравнимы относительно этого порядка.

После того, как на множестве E_2^n задан частичный порядок, стандартным образом вводится понятие монотонной функции. Именно: булева функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если для любых двух наборов $(a_1, \ldots, a_n), (b_1, \ldots, b_n)$, удовлетворяющих соотношению (2.4), выполняется неравенство

$$f(a_1, \ldots, a_n) \leqslant f(b_1, \ldots, b_n).$$

Множество всех монотонных булевых функций обозначим через M. (Еще раз отметим, что мы придем к тому же понятию монотонной булевой функции, если потребуем монотонной неубываемости функции по любой из ее переменных.)

Непосредственная проверка показывает, что множеству M принадлежат функции 0, 1, x, xy, $x \vee y$ и не принадлежат функции $\overline{x}$, $x \oplus y, x \to y$, $x|y$. В отличие от классов S и L (а также классов T_0, T_1) подсчет числа функций в множестве $M^{(n)}$ представляет собой очень серьезную проблему (*проблема Дедекинда*). Ее решение потребовало разработки специальных методов и занимает большой объем (см. [28,29]).

Для проверки монотонности булевой функции от небольшого числа переменных часто используют задание булевой функции с помощью диаграммы, на которой представлен частичный порядок на множестве E_2^n. Каждому набору из E_2^n отвечает точка на этой диаграмме, а различные точки соединяются отрезком только том случае, когда эти точки соответствуют соседним наборам — наборам, которые различаются ровно в одной координате (см. рис. 1). Обычно точки на диаграмме разделяют на (горизонтальные) «слои». При этом каждый «слой» диаграммы состоит из точек, которые отвечают двоичным наборам с одним и тем же

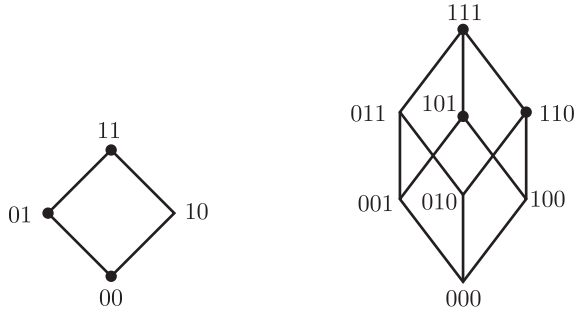


Рис. 1

числом единичных компонент. Самый нижний слой состоит из одного нулевого набора, самый верхний — из одного единичного набора. Если для наборов $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ выполняется соотношение (2.4), то от набора a до набора b в диаграмме можно «подняться» по отрезкам прямых.

Значения функции помещаются на диаграмме рядом с вершинами, которые отвечают наборам соответствующих значений переменных. На рис. 1 значения 1 функций обозначены жирными точками. На диаграмме множества E_2^2 представлена функция $x \to y$, а на диаграмме множества E_2^3 — функция $x(y \vee z)$. С помощью приведенных диаграмм можно легко проверить немонотонность функции $x \to y$ и монотонность функции $x(y \vee z)$. В самом деле, переход от меньшего набора $(0, 0)$ к большему набору $(1, 0)$ сопровождается изменением функции $x \to y$ от большего значения 1 к меньшему значению 0. Напротив, в диаграмме множества E_2^3 на любом пути, ведущем от наименьшего набора $(0, 0, 0)$ к наибольшему набору $(1, 1, 1)$, значения функции $x(y \vee z)$ не убывают.

Докажем, что множество M является замкнутым классом. Поскольку селекторные функции монотонны, нам достаточно доказать, что из монотонности функций $g_0, g_1, \ldots, g_m$ следует монотонность функции f, если f определяется равенством (1.9). Пусть для наборов $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ выполняется соотношение (2.4). Тогда в силу монотонности функций $g_1, \ldots, g_m$ будем иметь

$$g_1(a) \leqslant g_1(b), \ldots, g_m(a) \leqslant g_m(b).$$

Следовательно,

$$(g_1(a), \ldots, g_m(a)) \leqslant (g_1(b) \ldots, g_m(b)).$$

Пользуясь этим неравенством и монотонностью функции g_0, заключаем, что

$$g_0(g_1(a), \ldots, g_m(a)) \leqslant g_0(g_1(b), \ldots, g_m(b)).$$

Согласно определяющему равенству (1.9) это означает, что

$$f(a_1, \ldots, a_n) \leqslant f(b_1, \ldots, b_n),$$

и монотонность функции f установлена.

Для монотонных функций справедлив любопытный вариант теоремы 1.2 о разложении по переменной.

Теорема 2.1. *Для любой монотонной булевой функции* $f(x_1, \ldots, x_n)$ *справедливо представление*

$$f(x_1, \ldots, x_n) = x_1 \cdot f(1, x_2, \ldots, x_n) \vee f(0, x_2, \ldots, x_n). \qquad (2.5)$$

Доказательство. Пусть $a = (a_1, \ldots, a_n)$ — произвольный двоичный набор. Для набора a найдем значения левой и правой частей равенства (2.5). Слева мы имеем $f(a)$. Если $a_1 = 0$, то, как легко видеть, справа также образуется значение $f(a)$. Пусть $a_1 = 1$. Тогда справа в (2.5) получаем

$$f(1, a_2, \ldots, a_n) \vee f(0, a_2, \ldots, a_n). \qquad (2.6)$$

Однако набор $(0, a_2, \ldots, a_n)$ не превосходит набора $(1, a_2, \ldots, a_n)$. Следовательно, в силу монотонности функции f будем иметь

$$f(0, a_2, \ldots, a_n) \leqslant f(1, a_2, \ldots, a_n).$$

Поэтому значение (2.6) есть $f(1, a_2, \ldots, a_n)$. Теорема доказана.

Заметим, что в формуле (2.5) функции $f(0, x_2, \ldots, x_n)$ и $f(1, x_2, \ldots, x_n)$ также являются монотонными, поскольку получаются из монотонной функции f подстановкой монотонных функций 0 и 1. Поэтому при $n \geqslant 2$ так же, как и при выводе следствия 2 из теоремы 1.2, процесс разложения функций $f(0, x_2, \ldots, x_n)$ и $f(1, x_2, \ldots, x_n)$ можно продолжить по переменной x_2. В результате придем к разложению

$$\begin{aligned} f(x_1, \ldots, x_n) = \\ = x_1 \cdot x_2 \cdot f(1, 1, x_3, \ldots, x_n) \vee x_1 \cdot f(1, 0, x_3, \ldots, x_n) \vee \\ \vee x_2 \cdot f(0, 1, x_3, \ldots, x_n) \vee f(0, 0, x_3, \ldots, x_n). \end{aligned}$$

Если при $n \geqslant 3$ проделать указанное разложение по всем оставшимся переменным $x_3, \ldots, x_n$ и воспользоваться соотношениями $x \cdot 1 = x \vee 0 = x$, то получим следующее утверждение.

Следствие 1. *Любую монотонную функцию, отличную от константы, можно представить в виде ДНФ, не содержащей отрицаний переменных.*

Положим

$$M_0 = M \cap T_0, \quad M_1 = M \cap T_1, \quad M_{01} = M \cap T_0 \cap T_1.$$

Следствие 1 позволяет сделать выводы о системах функций, порождающих классы M, M_0, M_1, M_{01}.

Следствие 2. *Имеют место следующие равенства*:

$$M = [0, 1, x \vee y, xy], \quad M_0 = [0, x \vee y, xy],$$
$$M_1 = [1, x \vee y, xy], \quad M_{01} = [x \vee y, xy].$$

В заключение параграфа докажем лемму о немонотонной функции, которая нам понадобится в следующем разделе при доказательстве критерия полноты.

Лемма 2.3 (о немонотонной функции). *Из любой немонотонной функции путем подстановки функций* $0, 1, x$ *на места всех ее переменных можно получить немонотонную функцию одной переменной, т. е. функцию* $\overline{x}$.

Доказательство. Пусть функция $f(x_1, \ldots, x_n)$ немонотонна. Тогда найдутся такие два набора $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$, что выполняются соотношения (2.4) и $f(a) = 1$, $f(b) = 0$. Заменим в функции f переменную x_i $(1 \leqslant i \leqslant n)$ константой 0, если $a_i = b_i = 0$, константой 1, если $a_i = b_i = 1$, и функцией x в остальных случаях (заметим, что ввиду соотношения (2.4) в этих случаях должно быть обязательно $a_i = 0$, $b_i = 1$). Полученную функцию обозначим через $g(x)$. Из определения функции g следует, что $g(0) = f(a)$ и $g(1) = f(b)$. Таким образом, $g(x) = \overline{x}$. Лемма доказана.

§ 4. Критерий полноты

Существует ли эффективный способ, который по любой системе булевых функций дает ответ на вопрос, полна ли эта система? Оказывается, такой способ существует и он основан на проверке пяти «свойств»: невхождении системы функций ни в один из пяти замкнутых классов

$$T_0, \quad T_1, \quad S, \quad M, \quad L. \tag{2.7}$$

Имеет место следующий критерий полноты в классе P_2.

Теорема 2.2. *Система булевых функций полна в* P_2 *тогда и только тогда, когда она целиком не содержится ни в одном из классов* (2.7).

Доказательство. *Необходимость.* Пусть система функций Q полна в классе P_2. Тогда $[Q] = P_2$. Если бы система Q целиком содержалась в одном из классов (2.7) (обозначим этот класс через R), то по свойству 3 замыкания выполнялось бы равенство $[R] = P_2$. Однако каждый из замкнутых классов (2.7) отличен от класса P_2. Поэтому система Q целиком не содержится ни в одном из классов (2.7).

Достаточность. Пусть система Q целиком не содержится ни в одном из классов (2.7). Обозначим через f_0, f_1, f_S, f_M, f_L функции системы Q, которые не входят, соответственно,

в классы T_0, T_1, S, M, L (некоторые из функций $f_0, \ldots, f_L$ могут совпадать). Покажем, что суперпозициями функций $f_0, \ldots, f_L$ можно получить функции $\overline{x}$, xy, которые, как нам известно, образуют полную в P_2 систему. Тогда по теореме 1.1 полной будет система $\{f_0, \ldots, f_L\}$ и, следовательно, система Q.

Сначала получим из функций f_0, f_1, f_S константы 0 и 1. Из соотношения $f_0 \notin T_0$ следует, что $f_1(0, \ldots, 0) = 1$. Значит, если положить

$$g_1(x) = f_0(x, \ldots, x),$$

то функция $g_1(x)$ будет совпадать с одной из функций 1, $\overline{x}$. Если $g_1(x)$ — константа 1, то, пользуясь соотношением $f_1(1, \ldots, 1) = 0$, получаем константу 0:

$$f_1(g_1(x), \ldots, g_1(x)) = 0.$$

Пусть $g_1(x) = \overline{x}$. Тогда, применяя лемму о несамодвойственной функции к функции f_S, с помощью функций x и $\overline{x}$ получаем из нее одну из констант (0 или 1). Другую константу образуем с помощью подстановки в функцию $\overline{x}$.

Имея обе константы и применяя к функции f_M лемму о немонотонной функции, строим функцию $\overline{x}$, а с помощью леммы о нелинейной функции, применной к функции f_L, — нелинейную функцию $g_2(x, y)$. Рассмотрим полином Жегалкина для функции $g_2(x, y)$:

$$g_2(x, y) = xy \oplus a_1 x \oplus a_2 y \oplus a_3.$$

Можно считать, что $a_3 = 0$, поскольку в противном случае вместо функции $g_2(x, y)$ следует взять функцию $\overline{g}_2(x, y) = g_2(x, y) \oplus 1$ (напомним, что функция $\overline{x} = x \oplus 1$ у нас уже имеется). Если $a_1 = a_2 = 0$, то $g_2(x, y)$ — конъюнкция xy. Если $a_1 = 1$ и $a_2 = 0$, то $g_2(x, \overline{y}) = xy$. Аналогично поступаем в случае, когда $a_1 = 0$ и $a_2 = 1$. Наконец, если $a_1 = a_2 = 1$, то $g_2(x, y) = x \vee y$ и потому $\overline{g}_2(\overline{x}, \overline{y}) = xy$. Теорема доказана.

Из теоремы 2.2 вытекает несколько интересных следствий. Во-первых, как видно из доказательства, если система функций полна в P_2, то из нее можно выделить также полную подсистему, состоящую не более чем из пяти функций. Оказывается, что в общем случае это число можно понизить до четырех.

Следствие 1. *Если система функций полна в классе P_2, то из нее можно выделить полную подсистему, состоящую не более чем из четырех функций.*

Доказательство. Пусть функции $f_0, \ldots, f_L$ выбраны так, как указано в доказательстве теоремы. Рассмотрим функцию f_0.

Как мы выяснили, функция $g_1(x) = f_0(x, \ldots, x)$ совпадает с одной из функций $1, \overline{x}$. Если $g_1(x) = 1$, то функция g_1 несамодвойственна и ею можно заменить функцию f_S. Если же $g_1(x) = \overline{x}$, то функция g_1 немонотонна. Значит, в том случае функцией g_1 можно заменить функцию f_M. Следствие доказано.

Можно ли продвинуться в этом направлении еще на один шаг? Следующий пример показывает, что, вообще говоря, это сделать нельзя. Пусть

$$Q = \{0,\ 1,\ xy \vee xz \vee yz,\ x \oplus y \oplus z\}.$$

Пользуясь, например, доказанной теоремой 2.2, нетрудно убедиться, что система Q полна в P_2. Вместе с тем подсистема

$\{1,\ xy \vee xz \vee yz,\ x \oplus y \oplus z\}$ целиком лежитв классе T_1,

подсистема

$\{0,\ xy \vee xz \vee yz,\ x \oplus y \oplus z\}$ — в классе T_0,

подсистема

$\{0,\ 1,\ x \oplus y \oplus z\}$ — в классе L и

подсистема

$\{0,\ 1,\ xy \vee xz \vee yz\}$ — в классе M.

Таким образом, ни одну из функций системы Q исключить нельзя, не нарушив при этом условия полноты.

В § 7 главы 1 мы установили, что функция $x|y$ (штрих Шеффера) образует полную в P_2 систему. Будем называть функцию f *шефферовой*, если функция f является базисом класса P_2. Оказывается, что для распознавания шефферовсти функции критерий полноты из теоремы 2.2 можно несколько упростить.

Следствие 2. *Булева функция является шефферовой тогда и только тогда, когда она не принадлежит ни одному из классов* T_0, T_1, S.

Доказательство. Необходимость условия следует из теоремы 2.2. Установим достаточность условия. Покажем, что функция f, не входящая в классы T_0, T_1, S, не входит также в классы M и L.

В самом деле, из соотношений $f \notin T_0$, $f \notin T_1$ следует, что $f(0, \ldots, 0) = 1$ и $f(1, \ldots, 1) = 0$. Таким образом, f — немонотонная функция. Предположим далее, что f — линейная функция и $f(x_1, \ldots, x_n)$ представима в виде (2.3). Условие $f \notin T_0$ дает равенство $a_0 = 1$, а условие $f \notin T_1$ — равенство $a_1 \oplus \ldots \oplus a_n = 1$. Следовательно, линейная функция f имеет нечетное число существенных переменных. Нетрудно видеть, что в этом случае

функция f будет самодвойственной, что противоречит предположению $f \notin S$. Итак, функция f нелинейна, следствие доказано.

Назовем замкнутый класс R *предполным*, если $R \neq P_2$ и для любой функции f, не принадлежащей классу R, система функций $R \cup \{f\}$ полна в классе P_2.

Теорема 2.3. *Единственными предполными классами являются классы* (2.7).

Доказательство. Установим сначала, что ни один из классов (2.7) целиком не содержится в другом. Это вытекает из следующих соотношений:

$$0 \in (T_0 \cap L \cap M) \setminus (T_1 \cup S), \quad 1 \in (T_1 \cap L \cap M) \setminus (T_0 \cup S),$$
$$\overline{x} \in S \setminus (T_0 \cup T_1 \cup M), \quad xy \in (T_0 \cap T_1 \cap M) \setminus L,$$
$$x \oplus y \in (T_0 \cap L) \setminus M, \quad x \oplus y \oplus 1 \in T_1 \setminus M,$$
$$xy \oplus xz \oplus yz \in S \setminus L.$$

Далее покажем, что все классы (2.7) являются предполными. В самом деле, пусть R — один из классов (2.7) и $f \notin R$. Тогда, как мы установили, класс R целиком не содержится ни в одном из остальных классов (2.7). Следовательно, система $R \cup \{f\}$ целиком не входит ни в один из классов (2.7). По теореме 2.2 она является полной. Значит, R — предполный класс.

Остается доказать, что не существует других предполных классов, отличных от классов (2.7). Однако если Q — такой предполный класс, то ввиду соотношения $Q \neq P_2$ и теоремы 2.2 класс Q должен целиком содержаться в одном из классов R списка (2.7). Если $Q \neq R$ и $f \in R \setminus Q$, то добавление функции f к классу Q приводит к системе, целиком содержащейся в классе R. Поэтому замыкание данной системы также будет содержаться в замкнутом классе R, что противоречит определению предполного класса. Следовательно, $Q = R$ и теорема доказана.

§ 5. Замкнутые классы, содержащие константы

В предыдущих параграфах мы определили девять замкнутых классов. Еще некоторое количество замкнутых классов можно получить, если рассматривать различные пересечения упомянутых девяти классов. Однако пока у нас нет ни других способов определения замкнутых классов, ни способов получения нетривиальных верхних «границ» для семейства всех замкнутых классов.

Э. Пост установил, что число замкнутых классов в P_2 счетно-бесконечно. Эти результаты будут изложены (но с существенно другими доказательствами, нежели у Поста) в следующей главе. А пока мы решим весьма скромную задачу: найдем все замкнутые классы, содержащие константы 0 и 1. Иногда решением этой задачи (наряду с определением классов (2.7)) ограничиваются при изучении замкнутых классов булевых функций.

В этом параграфе и в следующей главе мы примем одно соглашение, которое касается определения замкнутого класса. Будем рассматривать только те замкнутые классы, которые наряду с произвольной функцией f содержат также все функции, получающиеся из f введением несущественных переменных. Это ограничение не слишком сильно сужает понятие замкнутого класса, но позволяет в дальнейшем избежать рассмотрения «параллельных» замкнутых классов, которые отличаются лишь возможностью вводить несущественные переменные. Отметим, что в «крупных» замкнутых классах (2.7) такая возможность имеется.

Из всех замкнутых классов, которые мы определили в предыдущих параграфах, обе константы содержат лишь классы P_2, M и L. Введем еще пять замкнутых классов, которые также содержат обе константы:

пусть C обозначат класс всех булевых функций-констант (от любого числа переменных);

U обозначает класс всех булевых функций, которые существенно зависят не более чем от одной переменной;

$MU = M \cap U$ (класс всех монотонных функций из U);

D обозначает класс всех дизъюнкций, т. е. всех функций $f(x_1, \ldots, x_n)$, которые представимы в виде

$$a_0 \vee a_1 x_1 \vee \ldots \vee a_n x_n, \tag{2.8}$$

где $a_0, a_1, \ldots, a_n$ — произвольные коэффициенты из E_2;

наконец, через K обозначим класс всех конъюнкций, т. е. класс всех функций $f(x_1, \ldots, x_n)$, которые представимы в виде

$$a_0 \cdot (a_1 \vee x_1) \cdot \ldots \cdot (a_n \vee x_n). \tag{2.9}$$

Замкнутость классов C, U, MU легко вытекает из их определения. Чтобы доказать замкнутость класса D, полезно иметь в виду, что при $a_0 = 1$ дизъюнкция (2.8) обращается в константу 1, при $a_0 = a_1 = \ldots = a_n = 0$ — в константу 0, а если из коэффициентов $a_0, a_1, \ldots, a_n$ равны 1 лишь коэффициенты $a_{i_1}, \ldots, a_{i_s}$, причем $a_0 = 0$, то выражение (2.8) представляет собой «настоящую» дизъюнкцию $x_{i_1} \vee \ldots \vee x_{i_s}$.

Поэтому замкнутость класса D следует из свойств дизъюнкции, отмеченных в § 5 гл. I.

Класс K, как несложно проверить, является двойственным к классу D. Из представлений (2.8) и (2.9) видно, что класс D порождается системой функций $\{0,\ 1,\ x \vee y\}$, а класс K — системой функций $\{0,\ 1,\ xy\}$.

Теорема 2.4. *Существует ровно* 8 *замкнутых классов, содержащих константы* 0 *и* 1:

$$P_2, \quad M, \quad L, \quad C, \quad U, \quad MU, \quad D, \quad K.$$

Доказательство. Пусть R — произвольный замкнутый класс, содержащий константы 0 и 1. Поскольку система функций $\{0, 1\}$ целиком не содержится ни в одном из классов T_0, T_1, S, из теоремы 2.2 выводим, что класс R либо совпадает с классом P_2, либо целиком содержится в одном из классов M, L. Рассмотрим сначала случай, когда R состоит только из линейных функций.

Если класс R состоит только из функций, существенно зависящих не более чем от одной переменной, то непосредственная проверка показывает, что R совпадает с одним из классов C, U, MU. Предположим далее, что класс R содержит линейную функцию $f(x_1, \ldots, x_n)$, существенно зависящую не менее чем от двух переменных. Можно считать, что все переменные функции $f(x_1, \ldots, x_n)$ существенны. Тогда функция $f(x_1, \ldots, x_n)$ представима в виде

$$f(x_1, \ldots, x_n) = a \oplus x_1 \oplus \ldots \oplus x_n,$$

где $n \geqslant 2$ и $a \in E_2$. При $n > 2$ подстановкой константы 0 вместо всех переменных $x_3, \ldots, x_n$ получаем функцию $a \oplus x_1 \oplus x_2$, принадлежащую классу R. Если $a = 0$, то в класс R входит система функций $\{1,\ x_1 \oplus x_2\}$, которая, как отмечалось в § 2 гл. II, порождает класс L. Значит, в этом случае $R = L$. Если же $a = 1$, то функцию $x_1 \oplus x_2$ получаем суперпозициями функций 0 и $1 \oplus x_1 \oplus x_2$:

$$1 \oplus x_1 \oplus 0 = 1 \oplus x_1, \quad 1 \oplus (1 \oplus x_1 \oplus x_2) = x_1 \oplus x_2.$$

Таким образом, если замкнутый класс R содержит обе константы 0, 1 и состоит только из линейных функций, то он совпадает с одним из классов C, U, MU, L.

Пусть теперь класс R состоит только из монотонных функций и содержит нелинейную функцию. Согласно лемме о нелинейной функции в класс R будет входить нелинейная функция от двух

переменных. Легко проверить, что нелинейными монотонными функциями от двух переменных являются лишь функции xy и $x \vee y = xy \oplus x \oplus y$. Поскольку системы функций $\{0,\ 1,\ x \vee y\}$ и $\{0,\ 1,\ xy\}$ порождают, соответственно, классы D и K, приходим к выводу, что в этом случае в класс R целиком входит хотя бы один из классов D или K.

Если в класс R целиком входят оба класса D и K, то $R = M$, так как класс M порождается системой функций $\{0,\ 1,\ xy,\ x \vee y\}$. Предположим поэтому, что в R целиком входит только один из классов D, K. Ввиду двойственности классов D, K можно считать, что это класс D. Мы покажем, что в этом случае R совпадает с D.

В самом деле, допустим, что $R \neq D$. Тогда в класс R входит функция $f(x_1, \ldots, x_n)$, которая не является дизъюнкцией. Согласно следствию 1 из теоремы 2.1 функцию $f(x_1, \ldots, x_n)$ можно представить в виде ДНФ Φ, которая не содержит отрицаний переменных. Поскольку функция $f(x_1, \ldots, x_n)$ отлична от дизъюнкции, ДНФ Φ содержит хотя бы одну конъюнкцию, имеющую более одного сомножителя. Пусть $x_{i_1} \cdot \ldots \cdot x_{i_s}$ — такая конъюнкция с наименьшим возможным числом сомножителей ($s \geqslant 2$). Можно считать, что в Φ в качестве дизъюнктивных слагаемых не входит ни одна из переменных $x_{i_1}, \ldots, x_{i_s}$ (иначе по свойству поглощения 11 конъюнкцию $x_{i_1} \cdot \ldots \cdot x_{i_s}$ в Φ можно было бы опустить). Таким образом, любая конъюнкция Φ из ДНФ, отличная от $x_{i_1} \cdot \ldots \cdot x_{i_s}$, содержит хотя бы одну переменную, не входящую в множество переменных $\{x_{i_1}, \ldots x_{i_s}\}$. Следовательно, если в функции $f(x_1, \ldots, x_n)$ заменить константой 0 все переменные, отличные от переменных $x_{i_1}, \ldots, x_{i_s}$, то получится функция, реализуемая конъюнкцией $x_{i_1} \cdot \ldots \cdot x_{i_s}$. Если теперь $s \geqslant 3$, то подстановка константы 1 вместо переменных $x_{i_3}, \ldots, x_{i_s}$ дает конъюнкцию $x_{i_1} \cdot x_{i_2}$.

Итак, получаем, что в класс R входит конъюнкция xy и (тем самым) все функции класса K. Это противоречит сделанному выше предположению о невхождении класса K в R. Теорема доказана.

Комментарии. Теорема 2.2 содержится в работе Э. Поста [47]; в такой же формулировке она опубликована в работе С. В. Яблонского [36]. Современная формулировка теоремы 2.2 появилась в работе [37], в которой доказательство теоремы приписано А. В. Кузнецову.

Глава III

РЕШЕТКА ЗАМКНУТЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

В этой главе мы перечислим все замкнутые классы булевых функций. Определение замкнутых классов будет дано как с помощью некоторых наследственных свойств, так и путем указания конечных базисов.

§ 1. Замкнутые классы, лежащие в классах U, D, K, L

Замкнутые классы C, C_0, C_1, U, U_{01}, T_0, T_1, S, M, L были определены в главах I, II. Для единообразия часть из них мы включили в следующую цепочку определений:

$$U_0 = U \cap T_0, \quad U_1 = U \cap T_1, \quad MU = M \cap U, \quad SU = S \cap U,$$
$$U_{01} = U \cap T_0 \cap T_1, \quad C_0 = C \cap T_0, \quad C_1 = C \cap T_1.$$

Теорема 3.1 легко доказывается рассмотрением всех функций от одной переменной (напомним, что все функции рассматриваются с точностью до несущественных переменных).

Теорема 3.1. *Произвольный замкнутый класс, целиком лежащий в классе U, совпадает с одним из следующих классов (в квадратных скобках указаны базисы классов)*:

$$U = [0, \overline{x}], \quad U_0 = [0, x], \quad U_1 = [1, x], \quad MU = [0, 1, x], \quad SU = [\overline{x}],$$
$$U_{01} = [x], \quad C = [0, 1], \quad C_0 = [0], \quad C_1 = [1].$$

Положим

$$D_0 = D \cap T_0, \quad D_1 = D \cap T_1, \quad D_{01} = D \cap T_0 \cap T_1,$$
$$K_0 = K \cap T_0, \quad K_1 = K \cap T_1, \quad K_{01} = K \cap T_0 \cap T_1,$$

где D, K — замкнутые классы дизъюнкций и конъюнкций.

Теорема 3.2. *Произвольный замкнутый класс, целиком лежащий в одном из классов D, K и не содержащийся в классе U, совпадает с одним из следующих классов*:

$$D = [0, 1, x \vee y], \quad D_0 = [0, x \vee y], \quad D_1 = [1, x \vee y], \quad D_{01} = [x \vee y],$$
$$K = [0, 1, xy], \quad K_0 = [0, xy], \quad K_1 = [1, xy], \quad K_{01} = [xy].$$

Доказательство. Пусть F — замкнутый класс, $F \subseteq D$ и $F \not\subseteq U$. Тогда в класс F входит такая функция $f(x_1, \ldots, x_n)$, в представлении (2.8) которой $a_0 = 0$ и хотя бы два из коэффициентов $a_1, \ldots, a_n$ отличны от 0. Пусть например, это будут коэффициенты a_1, a_2. Тогда, очевидно, функция $f(x_1, x_2, \ldots, x_2)$ совпадает с функцией $x_1 \vee x_2$. Далее рассматриваем четыре возможных случая вхождения констант 0,1 в класс F и пользуемся соотношениями $0 \vee x = x$, $1 \vee x = 1$. Двойственные рассуждения проводим для класса K. Теорема доказана.

Положим

$$L_0 = L \cap T_0, \quad L_1 = L \cap T_1, \quad SL = S \cap L, \quad L_{01} = L \cap T_0 \cap T_1.$$

Теорема 3.3. *Произвольный замкнутый класс, целиком лежащий в классе L и не содержащийся в классе U, совпадает с одним из следующих классов*:

$$L = [1, x \oplus y], \quad L_0 = [x \oplus y], \quad L_1 = [x \oplus y \oplus 1],$$
$$SL = [x \oplus y \oplus z \oplus 1], \quad L_{01} = [x \oplus y \oplus z].$$

Доказательство. Пусть F — замкнутый класс, $F \subseteq L$ и $F \not\subseteq U$. Тогда классу F принадлежит функция, существенно зависящая не менее чем от двух переменных. Используя соотношение $x \oplus x = 0$, отождествлением переменных получаем из этой функции одну из функций

$$a \oplus x \oplus y, \quad a \oplus x \oplus y \oplus z,$$

где $a \in \{0, 1\}$. Если в класс F входят обе функции вида $a \oplus x \oplus y$, то $F = L$, поскольку класс L порождается системой функций $\{1, x \oplus y\}$ и $1 = 1 \oplus x \oplus x$.

Пусть в класс F входит только одна функция вида $a \oplus x \oplus y$, например $x \oplus y$. Тогда класс F, очевидно, содержит константу 0, а функции 0, $x \oplus y$ позволяют определить в классе F все линейные функции, сохраняющие 0. Вместе с тем класс F не содержит функций, не сохраняющих 0: иначе подстановкой константы 0 в такую функцию мы получили бы константу 1 и, следовательно, пришли к функции $1 \oplus x \oplus y$. Таким образом, в этом случае класс F совпадает с классом L_0.

Двойственным образом рассматривается случай функции $1 \oplus x \oplus y$, который приводит к классу L_1.

Предположим, что класс F не содержит функций вида $a \oplus x \oplus y$. Тогда каждая функция из F существенно зависит от нечетного числа переменных. Нетрудно убедиться в том, что

в этом случае (как следует из определения самодвойственной функции) все функции класса F самодвойственны.

Если в класс F входит функция $1 \oplus x \oplus y \oplus z$, то в него входят также функции $1 \oplus x$ и $x \oplus y \oplus z$:

$$1 \oplus x = 1 \oplus x \oplus x \oplus x, \quad x \oplus y \oplus z = 1 \oplus (1 \oplus x \oplus y \oplus z).$$

Далее замечаем, что с помощью функции $x \oplus y \oplus z$ к произвольной линейной функции можно «добавить» две новые существенные переменные. Следовательно, функция $1 \oplus x \oplus y \oplus z$ порождает множество всех линейных функций с нечетным числом существенных переменных, т. е. класс SL самодвойственных линейных функций.

Предположим, наконец, что в класс F входит функция $x \oplus y \oplus z$, но не входит функция $1 \oplus x \oplus y \oplus z$. Понятно, что в этом случае все функции класса F сохраняют константу 0. Так же, как и выше, убеждаемся, что функция $x \oplus y \oplus z$ порождает множество всех линейных функций, которые сохраняют 0 и имеют нечетное число существенных переменных. Остается заметить, что класс L_{01} состоит в точности из всех таких функций. Теорема доказана.

§ 2. Замкнутые классы, лежащие в классах S, O^∞, I^∞

Положим

$$m(x, y, z) = xy \vee xz \vee yz.$$

Функция $m(x, y, z)$ называется *медианой*. Она самодвойственна, монотонна и нелинейна.

Лемма 3.1. *Пусть $f \in S \setminus L$. Тогда отождествлением и перестановкой переменных из функции f можно получить одну из функций*

$$m(x, y, z), \quad m(x, y, \overline{z}), \quad m(x, \overline{y}, \overline{z}), \quad m(\overline{x}, \overline{y}, \overline{z}).$$

Доказательство. Согласно лемме о нелинейной функции подстановкой константы 0 и переменных y, z из функции f можно получить нелинейную функцию от переменных y, z. Если вместо константы 0 в функцию f всюду подставить переменную x, то получим самодвойственную нелинейную функцию $g(x, y, z)$. Все нелинейные функции $g(0, y, z)$ суть

$$yz, \quad yz \oplus 1, \quad yz \oplus y, \quad yz \oplus y \oplus 1, \quad yz \oplus z, \quad yz \oplus z \oplus 1,$$
$$yz \oplus y \oplus z, \quad yz \oplus y \oplus z \oplus 1.$$

Восстанавливая по функции $g(0,y,z)$ соответствующую функцию $g(x,y,z)$, приходим к следующим функциям $g(x,y,z)$:

$$m(x,y,z),\quad m(\overline{x},\overline{y},\overline{z}),\quad m(x,y,\overline{z}),\quad m(\overline{x},\overline{y},z),\quad m(x,\overline{y},z),$$
$$m(\overline{x},y,\overline{z}),\quad m(\overline{x},y,z),\quad m(x,\overline{y},\overline{z}).$$

Лемма доказана.

Покажем, что

$$T_0 = [x \oplus y, xy].$$

Рассмотрим полином Жегалкина (1.10) произвольной функции из класса T_0. Тогда слагаемое нулевой степени в нем необходимо равно нулю. Вместе с тем суперпозициями функции xy можно реализовать любую функцию вида $x_{i_1} \dots x_{i_s}$, а с использованием дополнтельно функции $(x \oplus y)$ — и сумму таких функций. Следовательно, формулами над множеством $\{x \oplus y, xy\}$ можно реализовать любой полином Жегалкина, если только слагаемое нулевой степени отлично от 1 (напомним, что $0 = x \oplus x$).

В дальнейшем нам понадобится соотношение

$$T_0 = [x \vee y, x\overline{y}].$$

Оно вытекает из доказанного выше равенства и тождеств

$$x \oplus y = x\overline{y} \vee \overline{x}y, \quad xy = \overline{\overline{xy}}y.$$

В силу принципа двойственности будем также иметь

$$T_1 = [x \vee y, x \oplus y \oplus 1] = [x \vee \overline{y}, xy].$$

Положим

$$T_{01} = T_0 \cap T_1.$$

Покажем, что

$$T_{01} = [x \oplus y \oplus z, xy] = [x \vee y\overline{z}, xy].$$

Рассмотрим полином Жегалкина произвольной функции $f(x_1, \dots, x_n)$ из класса T_{01}. Поскольку функция f сохраняет 0, свободный член ее полинома равен нулю. Вместе с тем из соотношения $f \in T_1$ следует, что число слагаемых полинома нечетно. Таким образом, функция f может быть получена из функции вида $y_1 \oplus \dots \oplus y_{2k+1}$ подстановкой вместо каждой переменной y_j некоторой конъюнкции $x_{i_1} \dots x_{i_s}$, где $i_1, \dots, i_s \in \{1, \dots, n\}$. Для доказательства равенства $T_{01} = [x \oplus y \oplus z, xy]$ остается заметить, что линейная функция $y_1 \oplus \dots \oplus y_{2k+1}$ порождается функцией $x \oplus y \oplus z$, а конъюнкция $x_{i_1} \dots x_{i_s}$ — функцией xy.

Справедливость второго из доказываемых равенств вытекает из следующих построений. Из функции $x \vee y\overline{z}$ получаем функцию $w \vee x\overline{yz}$:

$$w \vee x\overline{yz} = w \vee (w \vee x\overline{y})\overline{z}.$$

Из последней функции суперпозициями образуем функцию

$$w \vee x\overline{yz} \vee \overline{x}y\overline{z} \vee \overline{xy}z.$$

Далее с помощью функции xy получаем функцию xyz и, подставив ее вместо переменной w в предыдущую функцию, приходим к совершенной ДНФ

$$xyz \vee x\overline{yz} \vee \overline{x}y\overline{z} \vee \overline{xy}z$$

функции $x \oplus y \oplus z$.

Положим

$$S_{01} = S \cap T_{01}, \quad SM = S \cap M.$$

Напомним, что *x_i-компонентой* функции f называется функция, которая получается из функции f подстановкой константы 1 вместо переменной x_i, а *$\overline{x}_i$-компонентой* — аналогичной подстановкой константы 0.

Лемма 3.2. *Имеют место соотношения*

$$S = [m(x, \overline{y}, \overline{z})] = [m(\overline{x}, \overline{y}, \overline{z})], \quad S_{01} = [m(x, y, \overline{z})],$$
$$SM = [m(x, y, z)].$$

Доказательство. Так как $m(\overline{x}, \overline{x}, \overline{x}) = m(x, \overline{x}, \overline{x}) = \overline{x}$, то ограничимся доказательством равенства $S = [m(x, \overline{y}, \overline{z})]$. Заметим, что $\overline{x}$-компонента функции $m(x, \overline{y}, \overline{z})$ есть шефферова функция $\overline{yz}$. Следовательно, если $f(x_1, \ldots, x_n)$ — произвольная функция из S, то суперпозициями функции $m(0, \overline{y}, \overline{z})$ можно получить $\overline{x}_1$-компоненту функции $f(x_1, \ldots, x_n)$. Заменяя в этих суперпозициях константу 0 всюду переменной x_1, мы в силу включения $f \in S$ получим функцию $f(x_1, \ldots, x_n)$.

Для доказательства равенства $S_{01} = [m(x, y, \overline{z})]$ заметим, что $\overline{x}$- и $\overline{z}$-компоненты функции $m(x, y, \overline{z})$ суть, соответственно, $y\overline{z}$ и $x \vee y$. Как установлено выше, система $\{y\overline{z}, x \vee y\}$ порождает класс T_0. Следовательно, $\overline{x}_1$-компоненту произвольной функции $f(x_1, \ldots, x_n)$ из класса S_{01} можно получить суперпозициями $\overline{x}$- и $\overline{z}$-компонент функции $m(x, y, \overline{z})$. Далее заменяем в этих суперпозициях константу 0 всюду переменной x_1 и приходим к функции f.

Покажем, что $SM = [m(x, y, z)]$. Пусть $f(x_1, \ldots, x_n) \in SM$ и $n \geqslant 3$. Обозначим набор переменных $x_4, \ldots, x_n$ через $\widetilde{x}$. Докажем, что имеет место тождество

$$f(x_1, x_2, x_3, \widetilde{x}) = \\ = m(f(x_1, x_1, x_3, \widetilde{x}), f(x_1, x_2, x_2, \widetilde{x}), f(x_3, x_2, x_3, \widetilde{x})).$$

Ввиду самодвойственности функции f его достаточно проверить лишь для наборов (0,0,0), (0,0,1), (0,1,0), (1,0,0). Для первого набора равенство очевидно. Взяв второй набор, для значений функции f в правой части равенства в силу монотонности функции f получим

$$f(0, 0, 0, \widetilde{x}) \leqslant f(0, 0, 1, \widetilde{x}) \leqslant f(1, 0, 1, \widetilde{x}).$$

Поэтому медианой будет «выбрано» значение $f(0, 0, 1, \widetilde{x})$. Аналогичным образом, в случае третьего набора приходим к неравенствам

$$f(0, 0, 0, \widetilde{x}) \leqslant f(0, 1, 0, \widetilde{x}) \leqslant f(0, 1, 1, \widetilde{x})$$

и выбору значения $f(0, 1, 0, \widetilde{x})$. Наконец, для четвертого набора получаем неравенства

$$f(0, 0, 0, \widetilde{x}) \leqslant f(1, 0, 0, \widetilde{x}) \leqslant f(1, 1, 0, \widetilde{x}).$$

Для завершения доказательства леммы остается заметить, что в классе SM нет функций, существенно зависящих ровно от двух переменных.

Теорема 3.4. *Произвольный замкнутый класс, целиком лежащий в классе S и не содержащийся в классе L, совпадает с одним из классов S, S_{01}, SM.*

Доказательство. Пусть F — замкнутый класс, $F \subseteq S$ и $F \not\subseteq L$. Включения $SM \subset S_{01} \subset S$ и леммы 3.1, 3.2 показывают, что $SM \subseteq F$. Поэтому если $F \subseteq M$, то $F = SM$.

Предположим, что F содержит немонотонную функцию. Согласно лемме о немонотонной функции подстановкой констант $0, 1$ и переменной z из нее можно получить немонотонную функцию $\overline{z}$. Если вместо констант $0, 1$ всюду подставить соответственно переменные x, y, то получим немонотонную (по переменной z) функцию $g(x, y, z)$ из класса S. Все такие функции $g(x, y, z)$ суть

$$m(x, y, \overline{z}), \quad m(x, \overline{y}, \overline{z}), \quad m(\overline{x}, y, \overline{z}), \quad m(\overline{x}, \overline{y}, \overline{z}), \quad \overline{z},$$
$$x \oplus y \oplus z \oplus 1, \quad x \oplus y \oplus z.$$

Во всех случаях в классе F легко определяется функция $m(x, y, \overline{z})$ (в последнем случае имеем

$$m(x, y, \overline{z}) = m(x, y, z) \oplus x \oplus y).$$

Значит, в силу леммы 3.2 получаем $S_{01} \subseteq F$. Если при этом $F \subseteq T_{01}$, то $F = S_{01}$. В противном случае в класс F входит функция, не сохраняющая 0. Отождествлением переменных из нее можно получить функцию $\overline{x}$. Остается заметить, что, согласно лемме 3.2, $[\overline{x}, m(x, y, z)] = S$. Теорема доказана.

Обозначим через O^∞ множество всех булевых функций, которые обладают следующим свойством: все наборы, на которых функция принимает значение 0, имеют общую нулевую компоненту. Двойственным образом (с заменой 0 на 1) определяется множество I^∞. Несложно проверить, что O^∞, I^∞ — замкнутые классы.

Из определения множества O^∞ следует, что функция $f(x_1, \ldots$ $\ldots, x_n)$ принадлежит множеству O^∞ в том и только том случае, когда для некоторого i $(1 \leqslant i \leqslant n)$ выполняется соотношение

$$f(x_1, \ldots, x_i, \ldots, x_n) = x_i \vee f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n). \quad (3.1)$$

Двойственное соотношение имеет место для функций из класса I^∞.

Лемма 3.3. *Пусть $f(x_1, \ldots, x_n) \in O^\infty \setminus D$. Тогда в зависимости от соотношения*

$$f \notin T_0, \quad f \in T_0 \setminus M \text{ или } f \in M \quad (3.2)$$

множество $[f]$ содержит функцию $x \vee \overline{y}$, $x \vee y\overline{z}$ или $x \vee yz$.

Доказательство. Пусть например, для функции f справедливо представление (3.1), где $i = 1$. Положим

$$g(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n).$$

Из $f \notin D$ следует, что $g \notin D$.

Пусть $g \notin M$. Согласно лемме о немонотонной функции из функции $g(x_2, \ldots, x_n)$ подстановкой вместо всех переменных констант 0,1 и переменной z можно получить функцию $\overline{z}$. Заменим в функции $f(x_1, \ldots, x_n)$ переменной x переменную x_1 и все переменные x_i, вместо которых в функцию g подставлялась константа 0, переменной y — все переменные x_j, вместо которых в функцию g подставлялась контанта 1, и переменной z — все

остальные переменные. Получим функцию $h(x,y,z)$ из класса O^∞ такую, что

$$h(x,y,z) = x \vee h(0,y,z), \quad h(0,1,z) = \overline{z}.$$

Функция $h(0,y,z)$ может совпадать лишь с одной из функций

$$\overline{z}, \quad \overline{y} \vee \overline{z}, \quad y\overline{z}, \quad y\overline{z} \vee \overline{y}z.$$

Если $f \notin T_0$, то очевидно, что $h(0,y,z) \notin T_0$. Поэтому $h(0,y,z) \in \{\overline{z}, \overline{y} \vee \overline{z}\}$. В этих случаях получаем $h(x,y,y) = x \vee \overline{y}$. Если $f \in T_0$, то также $h(0,y,z) \in T_0$. Значит,

$$h(0,y,z) \in \{y\overline{z}, y\overline{z} \vee \overline{y}z\}.$$

При $h(0,y,z) = y\overline{z}$ имеем $h(x,y,z) = x \vee y\overline{z}$, а при $h(0,y,z) = y\overline{z} \vee \overline{y}z$ —

$$h(x,y,x) = x \vee y, \quad h(x,y \vee z,z) = x \vee y\overline{z}.$$

Пусть теперь $g \in M$. Так как $g \notin D$, то функция g, в частности, отлична от константы. В силу следствия 1 из теоремы 2.1 функцию g можно представить в виде $K_1 \vee \ldots \vee K_t$, где $K_1, \ldots, K_t$ — (различные) монотонные конъюнкции, хотя бы одна из которых отлична от переменной (поскольку $g \notin D$). Выберем из неодночленных конъюнкций конъюнкцию наименьшей длины. Пусть например, она имеет вид $x_{i_1} \ldots x_{i_s}$, где $s \geqslant 2$. Если заменить в функции $f(x_1, \ldots, x_n)$ переменной x_1 все переменные x_j, отличные от переменных $x_{i_1}, \ldots, x_{i_s}$, то, получится функция $x_1 \vee x_{i_1} \ldots x_{i_s}$. Из нее дальнейшим отождествлением переменных получаем функцию $x_1 \vee x_{i_1}x_{i_2}$. Лемма доказана.

Следствие. *Пусть* $f(x_1, \ldots, x_n) \notin O^\infty$ *и* $f \neq 0$. *Тогда в зависимости от соотношения* (3.2) *множество* $[x \vee y, f]$ *содержит функцию* $x \vee \overline{y}$, $x \vee y\overline{z}$ *или* $x \vee yz$.

Доказательство. Положим

$$g(x_1, \ldots, x_n, y) = f(x_1, \ldots, x_n) \vee y.$$

Очевидно, что $g \in [x \vee y, f]$ и $g \in O^\infty \setminus D$. Далее замечаем, что соотношения (3.2) влекут, соответственно, соотношения

$$g \notin T_0, \quad g \in T_0 \setminus M, \quad g \in M.$$

Остается применить лемму 3.3.

Положим

$$O_0^\infty = O^\infty \cap T_0, \quad MO^\infty = M \cap O^\infty, \quad MO_0^\infty = M \cap O_0^\infty,$$
$$I_1^\infty = I^\infty \cap T_1, \quad MI^\infty = M \cap I^\infty, \quad MI_1^\infty = M \cap I_1^\infty.$$

Лемма 3.4. *Имеют место соотношения*

$$O^\infty = [x \vee \overline{y}], \quad O_0^\infty = [x \vee y\overline{z}], \quad MO^\infty = [1, x \vee yz],$$
$$MO_0^\infty = [x \vee yz], \quad I^\infty = [x\overline{y}], \quad I_1^\infty = [x(y \vee \overline{z})],$$
$$MI^\infty = [0, x(y \vee z)], \quad MI_1^\infty = [x(y \vee z)].$$

Доказательство. Рассмотрим классы типа O^∞. Пусть $f(x_1, \ldots, x_n) \in O^\infty$ и для функции f имеет место представление (3.1) при $i = 1$. Представим функцию f в виде

$$f(x_1, \ldots, x_n) = x_1 \vee K_1 \vee \ldots \vee K_t, \tag{3.3}$$

где $K_1, \ldots, K_t$ — конъюнкции от переменных $x_2, \ldots, x_n$ (не обязательно монотонные). Если $f \in MO_0^\infty$, то все конъюнкции $K_1, \ldots, K_t$ монотонны и отличны от констант. В этом случае функцию f можно получить из дизъюнкции $x_1 \vee y_1 \vee \ldots \vee y_t$ (которая легко реализуется суперпозициями функции $x \vee yz$) подстановкой вместо каждой переменной y_i функции $x_1 \vee K_i$. В свою очередь, функцию вида $x_1 \vee x_{i_1} \ldots x_{i_s}$, где $s \geqslant 3$, можно получить с помощью функции $x \vee yz$, используя рекуррентное соотношение

$$x_1 \vee x_{i_1} \ldots x_{i_{s+1}} = x_1 \vee x_{i_1} \ldots x_{i_s} \cdot (x_1 \vee x_{i_s} x_{i_{s+1}}).$$

При рассмотрении класса MO^∞ следует заметить, что данный класс отличается от класса MO_0^∞ только наличием константы 1.

Перейдем к классу O_0^∞. Замечаем, что при $f \in O_0^\infty$ каждая конъюнкция K_i из представления (3.3) функции f обязана содержать хотя бы одну переменную без отрицания. В связи с этим функцию вида $x_1 \vee x_{i_1} \ldots x_{i_r} \overline{x}_{i_{r+1}} \ldots \overline{x}_{i_s}$, где $r \geqslant 1$, получаем из функции $x_1 \vee x_{i_1} \ldots x_{i_r} z_{r+1} \ldots z_s$ подстановкой вместо переменных $z_{r+1}, \ldots, z_s$, соответственно, функций $x_1 \vee x_{i_r} \overline{x}_{i_{r+1}}, \ldots$ $\ldots, x_1 \vee x_{i_r} \overline{x}_{i_s}$.

Наконец, в случае $f \in O^\infty$ среди конъюнкций $K_1, \ldots, K_t$ может появиться конъюнкция $\overline{x}_{i_1} \ldots \overline{x}_{i_s}$. Поэтому функцию $x_1 \vee \overline{x}_{i_1} \ldots \overline{x}_{i_s}$ получаем из функции $x_1 \vee z_1 \ldots z_s$ подстановкой вместо переменных $z_1, \ldots, z_s$ функций $x_1 \vee \overline{x}_{i_1}, \ldots, x_1 \vee \overline{x}_{i_s}$.

Утверждения для классов $I^\infty, I_1^\infty, MI^\infty, MI_1^\infty$ получаем с использованием принципа двойственности. Лемма доказана.

Теорема 3.5. *Произвольный замкнутый класс, целиком лежащий в классе O^∞ и не содержащийся в классе D, совпадает с одним из классов O^∞, O_0^∞, MO^∞, MO_0^∞. Произвольный замкнутый класс, целиком лежащий в классе I^∞ и не содержащийся в классе K, совпадает с одним из классов I^∞, I_1^∞, MI^∞, MI_1^∞.*

Доказательство. Пусть F — замкнутый класс, $F \subseteq O^\infty$ и $F \not\subseteq D$. Если $F \subseteq M$, то в силу леммы 3.3 имеем $(x \vee yz) \in F$. Поэтому при $F \subseteq T_0$ получаем $F = MO_0^\infty$. Если же $F \not\subseteq T_0$, то из соотношения $F \subseteq M$ легко следует, что $1 \in F$. Далее применяем лемму 3.4 и приходим к равенству $F = MO^\infty$.

Пусть $F \not\subseteq M$. Из леммы 3.3 следует, что в класс F входит одна из функций $x \vee \overline{y}$, $x \vee y\overline{z}$. При $(x \vee \overline{y}) \in F$ согласно лемме 3.4 получаем $F = O^\infty$. Предположим, что $(x \vee y\overline{z}) \in F$. В случае $F \subseteq T_0$ лемма 3.4 приводит к равенству $F = O_0^\infty$. Если же $F \not\subseteq T_0$, то ввиду соотношения $F \subseteq O^\infty$ классу F принадлежит константа 1. Подстановка 1 в функцию $x \vee y\overline{z}$ дает функцию $x \vee \overline{z}$.

Случай $F \subseteq I^\infty$ рассматривается двойственным образом. Теорема доказана.

§ 3. Замкнутые классы, лежащие в классах T_1 и T_0

Лемма 3.5. *Пусть* $f_1 \in T_1 \setminus S$, $f_2 \in T_1 \setminus L$. *Тогда множество* $[f_1, f_2]$ *содержит хотя бы одну из функций* $x \vee y$, xy.

Доказательство. Из условия $f_1(x_1, \ldots, x_n) \notin S$ следует, что для некоторого набора $(a_1, \ldots, a_n)$ выполняется равенство

$$f_1(a_1, \ldots, a_n) = f_1(\overline{a}_1, \ldots, \overline{a}_n).$$

Заменим в функции $f_1(x_1, \ldots, x_n)$ переменной x все переменные x_i, для которых $a_i = 0$, и переменной y — все остальные переменные. Получим функцию $g_1(x, y)$, которая очевидным образом принадлежит множеству $T_1 \setminus S$. Поэтому

$$g_1(x, y) \in \{1,\ x \vee y,\ xy,\ x \oplus y \oplus 1,\ x \vee \overline{y},\ \overline{x} \vee y\}.$$

В последних трех случаях функция $g_1(x, x)$ есть константа 1. Таким образом, в множество $[f_1]$ входит одна из функций 1, $x \vee y$, xy.

Если $1 \in [f_1]$, то согласно утверждению, двойственному лемме о нелинейной функции, подстановкой константы 1 и переменных x, y из функции f_2 можно получить нелинейную функцию $g_2(x, y)$. Понятно, что $g_2 \in T_1$. Поэтому

$$g_2(x, y) \in \{x \vee y,\ xy,\ x \vee \overline{y},\ \overline{x} \vee y\}.$$

Однако функция $x \vee y$ порождается функцией $x \vee \overline{y}$. Лемма доказана.

Пусть $z(f)$ равно числу элементов в наименьшем множестве наборов, на которых функция f обращается в нуль и которые не имеют общей нулевой компоненты. Для любого $m \geqslant 2$ положим

$$d_m(x_1, \ldots, x_m) = \bigvee_{1 \leqslant i < j \leqslant m} x_i x_j.$$

Следующие леммы 3.6 и 3.7 являются ключевыми в данном изложении результатов Поста.

Лемма 3.6. *Пусть* $f \notin O^\infty$ *и* $f \neq 0$. *Тогда множество* $[x \vee y, f]$ *содержит функцию* d_m, *где* $m \leqslant \max(2, z(f))$.

Доказательство. Из условия $f(x_1, \ldots, x_n) \notin O^\infty$ следует, что для всякого i $(1 \leqslant i \leqslant n)$ найдется такой набор $a = (a_1, \ldots, a_n)$, что $a_i = 1$ и $f(a_1, \ldots, a_n) = 0$. Пусть $\{a^1, \ldots, a^m\}$ — наименьшее множество наборов, которое для любого i содержит набор a с указанным свойством. Очевидно, что $m \leqslant n$.

Если $m = 1$, то $f(1, \ldots, 1) = 0$ и $f(x, \ldots, x) \in \{0, \overline{x}\}$. В случае $f(x, \ldots, x) = 0$ применяем следствие из леммы 3.3 и с помощью константы 0 получаем функцию d_2. При $f(x, \ldots, x) = \overline{x}$ система $\{x \vee y, f\}$ полна в P_2 и, следовательно, вновь $d_2 \in [x \vee y, f]$.

Пусть $m \geqslant 2$. Заметим, что матрица

$$\begin{pmatrix} a_1^1 & a_2^1 & \ldots & a_n^1 \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^m & a_2^m & \ldots & a_n^m \end{pmatrix}, \tag{3.4}$$

в которой по строкам расположены наборы $a^1, a^2, \ldots, a^m$, не содержит нулевых столбцов, но после удаления любой строки такой столбец появляется. Значит, в матрице (3.4) можно так переставить столбцы, что образуется матрица вида

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & b_{m+1}^1 & \ldots & b_n^1 \\ 0 & 1 & \ldots & 0 & b_{m+1}^2 & \ldots & b_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & b_{m+1}^m & \ldots & b_n^m \end{pmatrix} \tag{3.5}$$

(напомним, что $m \leqslant n$). Обозначим через $g(x_1, \ldots, x_n)$ функцию, которая получается из функции f в результате соответствующей перестановки переменных. По определению функция g принимает значение 0 на всех наборах, образующих строки матрицы (3.5).

Мы хотим далее получить из функций $x \vee y, g$ функцию h от m переменных, которая принимает значение 0 на всех наборах с одной единичной компонентой. Если $m = n$, то в качестве функции h можно взять функцию g. Пусть $m < n$. Для любого i $(1 \leqslant i \leqslant n - m)$ суперпозициями функции $x \vee y$ определим функцию

$$h_i(x_1, \ldots, x_m) = b^1_{m+i} x_1 \vee b^2_{m+i} x_2 \vee \ldots \vee b^m_{m+i} x_m$$

(определение функции h_i корректно, поскольку $(b^1_{m+i}, \ldots, b^m_{m+i}) \neq (0, \ldots, 0)$). Тогда можно положить

$$h(x_1, \ldots, x_m) = \\ = g(x_1, \ldots, x_m, h_1(x_1, \ldots, x_m), \ldots, h_{n-m}(x_1, \ldots, x_m)).$$

Пользуясь следствием из леммы 3.3 и леммой 3.4, выберем в классе $MO^\infty_0 \subseteq [x \vee y, f]$ функцию $y \vee d_m(x_1, \ldots, x_m)$. Если $h(0, \ldots, 0) = 0$, то функция d_m получается из последней функции подстановкой функции $h(x_1, \ldots, x_m)$ вместо переменной y.

Пусть $h(0, \ldots, 0) = 1$. Как в предыдущем случае, образуем функцию

$$h_1(x_1, \ldots, x_m) = h(x_1, \ldots, x_m) \vee d_m(x_1, \ldots, x_m).$$

Замечаем теперь, что

$$h_1(x_1 \vee h_1(x_1, \ldots, x_m), x_2, \ldots, x_m) = d_m(x_1, \ldots, x_m).$$

Лемма доказана.

Согласно лемме 3.6 при выполнении условий $f \notin O^\infty$, $f \neq 0$ множество $[x \vee y, f]$ содержит некоторую функцию d_m. Обозначим через $p(f)$ такое наименьшее m, что $d_m \in [x \vee y, f]$.

В доказательстве леммы 3.7 используется свойство *мажоритарности* функций d_m $(m \geqslant 3)$: при любом i $(1 \leqslant i \leqslant m)$ справедливо тождество

$$d_m(x, \ldots, x, x_i, x, \ldots, x) = x.$$

Лемма 3.7. *Пусть* $f \in T_1 \setminus O^\infty$. *Тогда* $f \in [x \vee \overline{y}, d_{p(f)}]$. *Если дополнительно* $f \in T_0$ *или* $f \in M$, *то*, *соответственно*, $f \in [x \vee y\overline{z}, d_{p(f)}]$ *или* $f \in [x \vee yz, d_{p(f)}]$.

Доказательство. Предположим сначала, что $p(f) = 2$. Тогда утверждение леммы вытекает из установленных ранее соотношений

$$[x \vee \overline{y}, xy] = T_1, \quad [x \vee y\overline{z}, xy] = T_{01}, \quad [x \vee y, xy] = M_{01}.$$

Пусть $p(f) \geqslant 3$ и $\{a^1, \ldots, a^t\}$ — наименьшее множество наборов, на которых функция $f(x_1, \ldots, x_n)$ принимает значение 0 и которые не имеют общей нулевой компоненты. Если $t < p(f)$, то (согласно лемме 3.6) в множество $[x \vee y, f]$ входит функция d_m, где $m < p(f)$. Это противоречит определению числа $p(f)$. Значит, $t \geqslant p(f)$.

Предположим, что $f \in M$. Напомним, что верхним нулем функции f называется такой набор a, что $f(a) = 0$ и $f(b) = 1$ для любого набора b, который строго больше набора a. Заметим, что все наборы $a^1, \ldots, a^t$ можно считать верхними нулями функции f. В самом деле, если набор a^i не является верхним нулем функции f, то его можно заменить верхним нулем a, который строго больше набора a^i (поскольку все единичные компоненты набора a^i являются единичными компонентами набора a). Понятно, что наборы $a^1, \ldots, a^{i-1}, a, a^{i+1}, \ldots, a^t$ также не имеют общей нулевой компоненты.

Для любого i $(1 \leqslant i \leqslant p(f))$ обозначим через f_i такую монотонную функцию из класса T_1, что $f_i(a^i) = 1$ и $f_i(a) = f(a)$ при $a \neq a^i$ (монотонность функции f_i следует из того, что $f \in M$ и a^i — верхний нуль функции f). Из свойства мажоритарности функции $d_{p(f)}$ следует, что

$$f(x_1, \ldots, x_n) = d_{p(f)}(f_1(x_1, \ldots, x_n), \ldots, f_{p(f)}(x_1, \ldots, x_n)). \quad (3.6)$$

Таким образом, если функции $f_1, \ldots, f_{p(f)}$ принадлежат множеству $[x \vee yz, d_{p(f)}]$, то и $f \in [x \vee yz, d_{p(f)}]$.

Если $f_i \in O^\infty$, то согласно лемме 3.4 имеем $f_i \in [x \vee yz]$. Пусть $f_i \notin O^\infty$. Тогда $f_i \in [x \vee y, f]$. Действительно, согласно следствию из леммы 3.3 множество $[x \vee y, f]$ содержит функцию $x \vee yz$. Если в наборе a^i равны 1 компоненты с номерами $j_1, \ldots, j_k$, то функция f_i получается подстановкой функции f вместо переменной y в функцию $y \vee x_{j_1} \ldots x_{j_k}$, которая входит в множество $[x \vee yz]$. Из соотношения $f_i \in [x \vee y, f]$ следует, что $p(f_i) \geqslant p(f)$. Вместе с тем, как легко видеть, при $p > p(f)$ имеем $d_p \in [x \vee yz, d_{p(f)}]$. Далее поступаем с функцией f_i так же, как с функцией f. Этот индуктивный процесс продолжается до тех пор, пока не будут получены функции, входящие в класс O^∞.

Пусть теперь $f \in T_0 \setminus M$. Так же, как в случае $f \in M$, определяем функции $f_1, \ldots, f_{p(f)}$ из класса T_{01} (при этом $a^1, \ldots, a^t$ могут быть любыми ненулевыми наборами) и приходим к тождеству (3.6). Если $f_i \in O^\infty$, то $f_i \in O_0^\infty$ и применение леммы 3.4 дает $f_i \in [x \vee y\overline{z}]$. Пусть $f_i \notin O^\infty$. По следствию из леммы 3.3 имеем $(x \vee y\overline{z}) \in [x \vee y, f]$. Если, например, в наборе a^i равны 1

первые k компонент (причем $k \geqslant 1$, поскольку набор a^i отличен от нулевого набора), то $f_i = f \vee x_1 \dots x_k \overline{x}_{k+1} \dots \overline{x}_n$, где функция $y \vee x_1 \dots x_k \overline{x}_{k+1} \dots \overline{x}_n$ входит в множество $[x \vee y\overline{z}]$. Таким образом, $f_i \in [x \vee y, f]$. Как и выше, из включения $f_i \in [x \vee y, f]$ следует, что $p(f_i) \geqslant p(f)$. Наконец, дальнейший индуктивный процесс рассмотрения функций f_i обрывается при получении функций, входящих либо в класс O^∞, либо в класс M.

Пусть $f \in T_1 \setminus T_0$. Отличие от предыдущего случая состоит в том, что при $f_i \in O^\infty$ лемма 3.4 дает $f_i \in [x \vee \overline{y}]$, а при $f_i \notin O^\infty$ следствие из леммы 3.3 дает $(x \vee \overline{y}) \in [x \vee y, f]$. Лемма доказана.

Для любого $m \geqslant 2$ обозначим через O^m множество всех таких функций f, что любые m наборов, на которых функция f принимает значение 0, имеют общую нулевую компоненту. Положим

$$O_0^m = O^m \cap T_0, \quad MO^m = M \cap O^m, \quad MO_0^m = M \cap O_0^m.$$

Двойственным образом (с заменой 0 на 1) определяем классы I^m, I_1^m, MI^m, MI_1^m.

Нетрудно убедиться в том, что O^m, O_0^m, MO^m, MO_0^m есть замкнутые классы, причем

$$MO_0^m \subset MO^m \subset O^m, \quad MO_0^m \subset O_0^m \subset O^m,$$
$$d_{m+1} \in MO_0^m \quad \text{и} \quad d_m \notin MO_0^m$$

· **Теорема 3.6.** *Произвольный замкнутый класс, целиком лежащий в классе T_1 и не содержащийся в классах S, L, O^∞, I^∞, совпадает с одним из следующих классов*:

$$T_1 = [x \vee \overline{y}, xy], \quad M_1 = [1, x \vee y, xy], \quad O^m = [x \vee \overline{y}, d_{m+1}],$$
$$T_{01} = [x \vee y\overline{z}, xy], \quad M_{01} = [x \vee y, xy], \quad O_0^m = [x \vee y\overline{z}, d_{m+1}],$$
$$MO^m = [1, d_{m+1}] \quad (m = 2, 3, \dots), \quad MO_0^2 = [x \vee y, d_3],$$
$$MO_0^m = [d_{m+1}] \quad (m = 3, 4, \dots),$$
$$I_1^m = [x(y \vee \overline{z}), d_{m+1}^*] \quad (m = 2, 3, \dots),$$
$$MI_1^2 = [xy, d_3], \quad MI_1^m = [d_{m+1}^*] \quad (m = 3, 4, \dots).$$

Доказательство. Пусть F — замкнутый класс, $F \subseteq T_1$ и

$$F \not\subseteq S, \quad F \not\subseteq L, \quad F \not\subseteq O^\infty, \quad F \not\subseteq I^\infty.$$

Согласно лемме 3.5 классу F принадлежит одна из функций $x \vee y, xy$.

Предположим сначала, что $(x \vee y) \in F$. По лемме 3.6 в класс F входит некоторая функция d_{m+1}. Будем

считать, что m выбрано наименьшим возможным. Функция $y \vee d_{m+1}(x_1, \ldots, x_{m+1})$ из множества $F^\infty = F \cap O^\infty$, очевидно, не принадлежит классу D. Поэтому согласно теореме 3.5 класс F^∞ совпадает с одним из классов $O^\infty, O_0^\infty, MO^\infty, MO_0^\infty$.

Пусть $m = 1$. Тогда $xy \in F$. Если $F^\infty = O^\infty$, то (см. лемму 3.4) классу F принадлежит функция $x \vee \overline{y}$. Поскольку $[x \vee \overline{y}, xy] = T_1$, в этом случае получаем $F = T_1$. Если $F^\infty = O_0^\infty$, то все функции класса F сохраняют 0 (иначе ввиду $F \subseteq T_1$ было бы $1 \in F^\infty$). Кроме того (см. лемму 3.4), имеем $(x \vee y\overline{z}) \in F$. Однако $[x \vee y\overline{z}, xy] = T_{01}$. Следовательно, в этом случае $F = T_{01}$. Аналогичные рассуждения в случаях $F^\infty = MO^\infty$ и $F^\infty = MO_0^\infty$ показывают, что $F = M_1$ или $F = M_{01}$.

Предположим, что $m \geqslant 2$. Пусть $F^\infty = O^\infty$. Если $f \in F \setminus O^\infty$ и $p(f) = m + 1$, то в силу леммы 3.7 получаем $f \in [x \vee \overline{y}, d_{m+1}]$. Если $f \in F \setminus O^\infty$ и $p(f) > m + 1$, то соотношение $f \in [x \vee \overline{y}, d_{m+1}]$ следует из леммы 3.7 и соотношения $d_{p(f)} \in [x \vee y, d_{m+1}]$. Если же $f \in O^\infty$, то $f \in [x \vee \overline{y}]$ согласно лемме 3.4. Таким образом, в рассматриваемом случае $F = [x \vee \overline{y}, d_{m+1}]$. Вместе с тем функции $x \vee \overline{y}, d_{m+1}$ принадлежат классу O^m и класс O^m не содержит функций d_p при $p \leqslant m$. Следовательно,

$$F = O^m = [x \vee \overline{y}, d_{m+1}].$$

Пусть $F^\infty = O_0^\infty$. Тогда все функции класса F сохраняют 0, т. е. $F \subseteq T_{01}$. Далее повторяем те же рассуждения, что и в случае $F = O^\infty$, пользуясь леммой 3.7 для класса T_0 и леммой 3.4 для класса O_0^∞. В результате приходим к равенствам

$$F = O_0^m = [x \vee y\overline{z}, d_{m+1}].$$

Случаи $F^\infty = MO^\infty$ и $F^\infty = MO_0^\infty$ рассматриваются аналогичным образом. Стоит лишь отметить, что при $m \geqslant 3$ функция $x \vee yz$ (а значит, и функция $x \vee y$) получается из функции d_{m+1} отождествлением переменных: $x \vee yz = d_{m+1}(x, \ldots, x, y, z)$.

Предположим теперь, что в класс F входит функция xy. Рассмотрим класс $F_0 = F \cap T_0$. Предыдущее доказательство в силу принципа двойственности дает все замкнутые классы, лежащие в классе F_0 и не содержащиеся в классах S, L, O^∞, I^∞:

$$T_{01} = [x \vee y\overline{z}, xy], \quad M_{01} = [x \vee y, xy],$$
$$I_1^m = [x(y \vee \overline{z}), d_{m+1}^*] \quad (m = 2, 3, \ldots),$$
$$MI_1^2 = [xy, d_3], \quad MI_1^m = [d_{m+1}^*] \quad (m = 3, 4, \ldots).$$

Если же в класс F входит функция f, не сохраняющая 0, то ввиду включения $F \subseteq T_1$ имеем $f(x,\ldots,x)=1$. Добавление константы 1 к классам T_{01}, M_{01}, I_1^m, MI_1^m приводит к уже полученным классам T_1 и M_1. Это вытекает из следующих очевидных соотношений:

$$[1, x\vee y\overline{z}, xy] = [1, x(y\vee\overline{z}), d^*_{m+1}] = T_1,$$
$$[1, xy, d_3] = [1, d^*_{m+1}] = M_1 \quad (m=3,4,\ldots).$$

Теорема доказана.

Двойственной к теореме 3.6 является теорема 3.7.

Теорема 3.7. *Произвольный замкнутый класс, целиком лежащий в классе T_0 и не содержащийся в классах S, L, O^∞, I^∞, совпадает с одним из следующих классов*:

$$T_0=[x\vee y, x\overline{y}], \quad M_0=[0, x\vee y, xy], \quad I^m=[x\overline{y}, d^*_{m+1}],$$
$$T_{01}=[x\vee y, x(y\vee\overline{z})], \quad M_{01}=[x\vee y, xy], \quad I_1^m=[x(y\vee\overline{z}), d^*_{m+1}],$$
$$MI^m=[0, d^*_{m+1}] \quad (m=2,3,\ldots), \quad MI_1^2=[xy, d_3],$$
$$MI_1^m=[d^*_{m+1}] \quad (m=3,4,\ldots),$$
$$O_0^m=[x\vee y\overline{z}, d_{m+1}] \quad (m=2,3,\ldots),$$
$$MO_0^2=[x\vee y, d_3], \quad MO_0^m=[d_{m+1}] \quad (m=3,4,\ldots).$$

§ 4. Основной результат

Теорема Поста. *Совокупность всех замкнутых классов булевых функций счетна и состоит из следующих классов.*

1. *Классы, содержащие константы* 0 *и* 1:

$$P_2,\ L,\ M,\ D,\ K,\ U,\ MU,\ C.$$

2. *Классы, содержащие* 0 *и не содержащие* 1:

$$L_0,\ M_0,\ T_0,\ D_0,\ K_0,\ U_0,\ C_0,\ I^m,\ MI^m \quad (m=2,3,\ldots,\infty).$$

3. *Классы, содержащие* 1 *и не содержащие* 0:

$$L_1,\ M_1,\ T_1,\ D_1,\ K_1,\ U_1,\ C_1,\ O^m,\ MO^m \quad (m=2,3,\ldots,\infty).$$

4. *Классы, не содержащие* 0 *и* 1:

$$L_{01},\ M_{01},\ S_{01},\ T_{01},\ D_{01},\ K_{01},\ U_{01},\ S,\ SL,\ SM,\ SU,$$
$$I_1^m,\ MI_1^m,\ O_0^m,\ MO_0^m \quad (m=2,3,\ldots,\infty).$$

Каждый из перечисленных замкнутых классов порождается конечной системой своих функций.

Таблица 5

Замкнутый класс	Пример базиса
Классы, содержащие константы 0 и 1	
P_2	$\overline{x}, x \vee y$
M	$0, 1, x \vee y, xy$
L	$1, x \oplus y$
D	$0, 1, x \vee y$
K	$0, 1, xy$
U	$1, \overline{x}$
MU	$0, 1, x$
C	$0, 1$
Классы, содержащие 1 и не содержащие 0	
T_1	$x \vee \overline{y}, xy$
M_1	$1, x \vee y, xy$
L_1	$x \oplus y \oplus 1$
D_1	$1, x \vee y$
K_1	$1, xy$
U_1	$1, x$
C_1	1
O^m	$x \vee \overline{y}, d_{m+1}$
$(m = 2, 3, \ldots)$	
MO^m	$1, d_{m+1}$
$(m = 2, 3, \ldots)$	
O^∞	$x \vee \overline{y}$
MO^∞	$1, x \vee yz$
Классы, содержащие 0 и не содержащие 1	
T_0	$x \vee y, x\overline{y}$
M_0	$0, x \vee y, xy$
L_0	$x \oplus y$
D_0	$0, x \vee y$
K_0	$0, xy$
U_0	$0, x$
C_0	0

Замкнутый класс	Пример базиса
Классы, содержащие 0 и не содержащие 1	
I^m	$x\overline{y}, d^*_{m+1}$
$(m = 2, 3, \ldots)$	
MI^m	$0, d^*_{m+1}$
$(m = 2, 3, \ldots)$	
I^∞	$x\overline{y}$
MI^∞	$0, x(y \vee z)$
Классы, не содержащие 0 и 1	
T_{01}	$xy, x \vee y\overline{z}$
S_{01}	$d_3(x, y, \overline{z})$
M_{01}	$x \vee y, xy$
L_{01}	$x \oplus y \oplus z$
D_{01}	$x \vee y$
K_{01}	xy
U_{01}	x
S	$\overline{x}, d_3$
SM	d_3
SL	$x \oplus y \oplus z \oplus 1$
SU	$\overline{x}$
O^m_0	$x \vee y\overline{z}, d_{m+1}$
$(m = 2, 3, \ldots)$	
MO^2_0	$x \vee y, d_3$
MO^m_0	d_{m+1}
$(m = 3, 4, \ldots)$	
I^m_1	$x(y \vee \overline{z}), d^*_{m+1}$
$(m = 2, 3, \ldots)$	
MI^2_1	xy, d_3
MI^m_1	d^*_{m+1}
$(m = 3, 4, \ldots)$	
O^∞_0	$x \vee y\overline{z}$
MO^∞_0	$x \vee yz$
I^∞_1	$x(y \vee \overline{z})$
MI^∞_1	$x(y \vee z)$

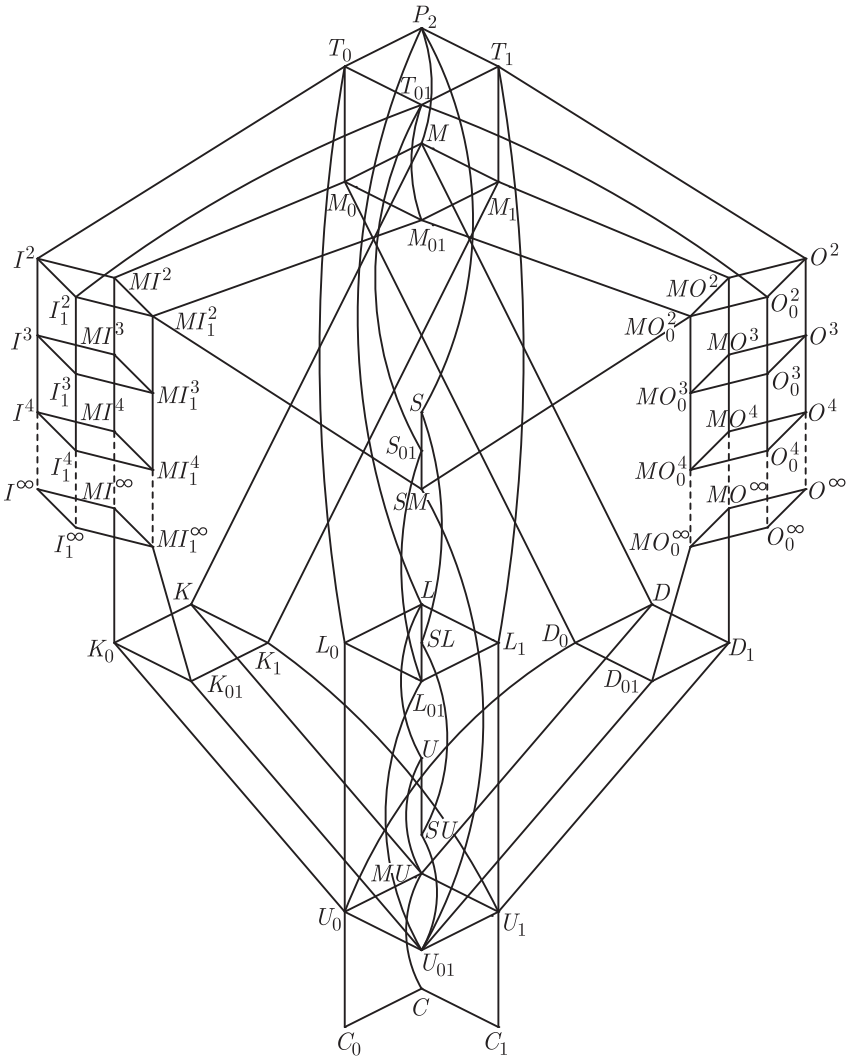


Рис. 2

Доказательство. Согласно теореме 2.2 всякий замкнутый класс булевых функций, отличный от класса P_2, целиком содержится в одном из классов S, M, L, T_0, T_1. Теоремы 3.1–3.7 описывают все замкнутые классы, которые целиком лежат в классах T_0, T_1, S, L, D, K. Остается исследовать замкнутые классы $F \subseteq M$, которые не содержатся в классах T_0, T_1, S, L, D, K. Однако из $F \subseteq M$ и $F \not\subseteq T_0$ следует, что

в класс F входит константа 1. Аналогично образом, из соотношений $F \subseteq M$ и $F \not\subseteq T_1$ следует, что $0 \in F$. Кроме того, лемма о нелинейной функции позволяет утверждать, что в классе F имеется монотонная нелинейная функция от переменных x, y, т. е. $x \vee y$ или xy.

Пусть например, $(x \vee y) \in F$. Поскольку $F \not\subseteq D$, в классе F есть функция $f(x_1, \ldots, x_n)$, которая не является дизъюнкцией. Тогда классу F принадлежит функция $g = y \vee f(x_1, \ldots, x_n)$, входящая в множество $O^\infty \setminus D$. Согласно теореме 3.5 класс $[g]$ может совпадать лишь с одним из классов MO^∞, MO_0^∞. В обоих случаях $(x \vee yz) \in [g]$. Подстановкой константы 0 получаем из функции $x \vee yz$ конъюнкцию yz. Таким образом, $\{0, 1, x \vee y, xy\} \subset F$. Однако $[0, 1, x \vee y, xy] = M$. Следовательно, в этом случае $F = M$.

Двойственным образом рассматривается случай, когда $xy \in F$. Теорема доказана.

Полный перечень замкнутых классов булевых функций приведен выше в табл. 5. Диаграмма включений всех замкнутых классов булевых функций представлена на рис. 2.

Комментарии. Все замкнутые классы булевых функций найдены Э.Постом [47, 48]. С середины 1960-х гг. начали появляться работы [39–41, 44], где с иных позиций и в более доступной форме излагались результаты Поста. К настоящему времени опубликована довольно большая серия работ [5, 6, 19–22, 25, 30, 31, 45, 49], в которых с использованием различных подходов и различной техники получены достаточно компактные доказательства теоремы Поста. Изложение в гл. III в основном следует статье [20].

Глава IV

ПРЕДИКАТНОЕ ОПИСАНИЕ ЗАМКНУТЫХ КЛАССОВ

Все замкнутые классы, отличные от класса P_2, определялись нами с помощью некоторых «свойств». Нетрудно заметить, что таких «ключевых» свойств бесконечно много: с их помощью определяются классы

$$T_0,\ T_1,\ S,\ L,\ M,\ D,\ K,\ U,\ C,\ O^\infty,\ I^\infty, O^n,\ I^n \quad (n = 2, 3, \ldots).$$

Остальные замкнутые классы можно определить в виде пересечений данных замкнутых классов (однако различные пересечения часто приводят к одинаковым замкнутым классам).

В этой главе мы хотим некоторым образом формализовать и унифицировать эти свойства, чтобы с определениями замкнутых классов можно было бы оперировать примерно так же, как с формулами, задающими булевы функции. При этом, однако, небольшая часть замкнутых классов (три класса типа C и восемь классов типов O^∞ и I^∞) останется за пределами конечных «формализаций». В основе формализации лежат понятия булева предиката и функции, сохраняющей предикат.

§ 1. Булевы предикаты и операции над предикатами

Понятие булева предиката близко к понятию булевой функции. *Булевым предикатом* (или предикатом на множестве E_2) будем называть истинностную функцию $\rho(x_1, \ldots, x_k)$ вида $\{0,1\}^k \to \{\text{И, Л}\}$, где И, Л — истинностные значения «истина» и «ложь». Набор $(a_1, \ldots, a_k)$ удовлетворяет предикату ρ, если $\rho(a_1, \ldots, a_k) = \text{И}$. Совокупность всех булевых предикатов обозначим через Π_2. В дальнейшем слово «булев» в сочетании «булев предикат» будем, как правило, опускать.

Если предикаты $\rho(x_1, \ldots, x_k)$ и $\sigma(x_1, \ldots, x_k)$ совпадают как функции, то называем их *эквивалентными предикатами* и записываем это в виде

$$\rho(x_1, \ldots, x_k) \equiv \sigma(x_1, \ldots, x_k),$$

оставляя знак равенства для булевых функций.

Предикат $\rho(x_1, \ldots, x_k)$ нередко отождествляют с его множеством истинности, то есть с множеством всех наборов $(a_1, \ldots, a_k)$ из E_2^k, которые удовлетворяют предикату ρ. В связи с этим тождественно истинный предикат называют *полным* предикатом, а тождественно ложный — *пустым*. Если множество истинности предиката $\rho(x_1, \ldots, x_k)$ является подмножеством множества истинности предиката $\sigma(x_1, \ldots, x_k)$, то говорят, что предикат ρ *содержится* в предикате σ или что предикат σ есть *расширение* предиката ρ.

Пусть на множестве $\{1, 2, \ldots, k\}$ задано отношение эквивалентности ε, т. е. бинарное рефлексивное, симметричное и транзитивное отношение. *Диагональю*, соответствующей отношению ε, называется такой предикат $\delta(x_1, \ldots, x_k)$, что

$$\delta(x_1, \ldots, x_k) \equiv \mathop{\&}_{\varepsilon(i,j)} (x_i = x_j), \tag{4.1}$$

где конъюнкция (рассматриваемая как логическая связка) берется по всем числам i, j из $\{1, 2, \ldots, k\}$, эквивалентным в смысле отношения ε. Иными словами, для произвольного набора $(a_1, \ldots, a_k)$ из E_2^k значение $\delta(a_1, \ldots, a_k)$ истинно в том и только том случае, когда для любых чисел i, j из множества $\{1, 2, \ldots, k\}$ справедлива импликация

$$\varepsilon(i, j) \Rightarrow (a_i = a_j).$$

Если отношение эквивалентности ε единичное (то есть ему удовлетворяют лишь пары равных чисел), то соответствующая диагональ $\delta(x_1, \ldots, x_k)$ есть

$$(x_1 = x_1) \,\&\, \ldots \,\&\, (x_k = x_k),$$

что представляет собой полный предикат. Если же отношение ε полное, то диагональ $\delta(x_1, \ldots, x_k)$ имеет вид

$$\mathop{\&}_{1 \leqslant i,j \leqslant k} (x_i = x_j).$$

Очевидно, что в этом случае диагонали δ удовлетворяют лишь два набора $(0, \ldots, 0), (1, \ldots, 1)$ и ее можно изобразить короче, в виде

$$x_1 = x_2 = \ldots = x_k.$$

При записи диагонали по формуле (4.1) присутствующие в ней предикаты вида $x_i = x_i$ часто опускают. Так же поступают с одним из двух эквивалентных предикатов $x_i = x_j$ и $x_j = x_i$. Например, если отношению эквивалентности ε помимо

пар равных чисел удовлетворяют лишь пары (1,2) и (2,1), то соответствующую диагональ δ можно записать в виде $x_1 = x_2$.

По причинам, которые будут ясны из дальнейшего, мы причисляем к диагоналям пустой (тождественно ложный) предикат.

Ввиду близости понятий булева предиката и булевой функции для булевых предикатов без специальных определений будут использоваться понятия существенной и фиктивной переменных, перестановки и отождествления переменных.

Введем две важные операции над предикатами.

Пусть $\rho(x_1, \ldots, x_k) \in \Pi_2$ и $1 \leqslant i \leqslant k$. *Проекцией предиката* $\rho(x_1, \ldots, x_k)$ по переменной x_i называется предикат

$$\rho(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_k) \vee \rho(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_k),$$

где дизъюнкция $\vee$ рассматривается как логическая связка.

Проекция предиката $\rho(x_1, \ldots, x_k)$ по переменной x_i обозначается через $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$. Из определения легко усматривается, что набор $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k)$ удовлетворяет предикату $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$ в том и только том случае, когда найдется такой элемент a_i из E_2, что набор $(a_1, \ldots, a_i, \ldots, a_k)$ удовлетворяет предикату $\rho(x_1, \ldots, x_k)$. Это оправдывает название «проекция предиката» и обозначение $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$. Отметим, что $(\exists x_1)\rho(x_1)$ есть 0-местный предикат, который ложен, если тождественно ложен предикат ρ, и истинен в противном случае.

Пусть $\rho(x_1, \ldots, x_k), \sigma(y_1, \ldots, y_l)$ — предикаты из Π_2. *Конъюнкцией* предикатов ρ и σ называется $(k+l)$-местный предикат, который задается формулой

$$\rho(x_1, \ldots, x_k) \,\&\, \sigma(y_1, \ldots, y_l).$$

Отметим, что с использованием операций конъюнкции, переименования и отождествления переменных из предикатов $\rho(x_1, \ldots, x_k)$ и $\sigma(x_1, \ldots, x_k)$ можно получить предикат

$$\rho(x_1, \ldots, x_k) \,\&\, \sigma(x_1, \ldots, x_k). \tag{4.2}$$

А именно: сначала с помощью введенной операции конъюнкции предикатов образуем $2k$-местный предикат

$$\rho(x_1, \ldots, x_k) \,\&\, \sigma(y_1, \ldots, y_k), \tag{4.3}$$

а затем из предиката (4.3) получаем предикат (4.2) с помощью очевидных отождествлений переменных.

Можно показать, что операции проектирования и отождествления переменных перестановочны.

Выше мы фактически применяли некоторые формулы с предикатами. Мы хотим далее продолжить аналогию с формулами над булевыми функциями и ввести понятия формулы над множеством булевых предикатов. Итак, пусть R — непустое множество булевых предикатов. Если ρ есть обозначение k-местного предиката из R, а $x_1, \ldots, x_k$ — различные символы переменных, то $\rho(x_1, \ldots, x_k)$ есть *формула над* R. Все переменные $x_1, \ldots, x_k$ считаются свободными в формуле $\rho(x_1, \ldots, x_k)$, и эта формула не содержит связанных переменных.

Пусть $\Phi(y_1, \ldots, y_l)$ — формула над R со свободными переменными $y_1, \ldots, y_l$, $1 \leqslant j \leqslant l$, а $x_{i_1}, \ldots, x_{i_l}$ — (не обязательно различные) символы переменных, которые отличаются от связанных переменных формулы $\Phi(y_1, \ldots, y_l)$. Тогда

$$\Phi(x_{i_1}, \ldots, x_{i_l}), \quad (\exists y_j)\Phi(y_1, \ldots, y_j, \ldots, y_l)$$

суть *формулы над* R.

Свободными переменными формулы $\Phi(x_{i_1}, \ldots, x_{i_l})$ являются переменные $x_{i_1}, \ldots, x_{i_l}$, а связанные переменные совпадают со связанными переменными формулы $\Phi(y_1, \ldots, y_l)$.

Свободные переменные формулы $(\exists y_j)\Phi(y_1, \ldots, y_j, \ldots, y_l)$ суть $y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_l$, а связанные переменные образуются из связанных переменных формулы $\Phi(y_1, \ldots, y_l)$ добавлением переменной y_j.

Если, наконец, $\Phi(x_1, \ldots, x_k)$, $\Psi(y_1, \ldots, y_l)$ — формулы над R со свободными переменными $x_1, \ldots, x_k$ и $y_1, \ldots, y_l$ соответственно, причем переменные формулы $\Phi(x_1, \ldots, x_k)$ (свободные и связанные) отличны от (свободных и связанных) переменных формулы $\Psi(y_1, \ldots, y_l)$, то

$$\Phi(x_1, \ldots, x_k) \,\&\, \Psi(y_1, \ldots, y_l)$$

есть *формула над* R со свободными переменными $x_1, \ldots, x_k$, $y_1, \ldots, y_l$, связанные переменные которой получаются объединением множеств связанных переменных формул $\Phi(x_1, \ldots, x_k)$ и $\Psi(y_1, \ldots, y_l)$.

Так же, как и для формул над множествами булевых функций, вводится понятие *предиката*, *реализуемого формулой над множеством булевых предикатов*. Если R — множество булевых предикатов, то через $[R]$ обозначается множество всех предикатов, реализуемых формулами над R. Множество предикатов R, для которого $[R] = R$, называется *замкнутым*. Для оператора замыкания на множестве булевых предикатов справедливы те же самые свойства (аксиомы), которые отмечались в гл. I для оператора замыкания на множестве булевых функций.

Для замкнутых классов предикатов важным свойством является наличие диагоналей. Оно позволяет, например, естественным образом вводить фиктивные переменные.

В самом деле, добавить фиктивную переменную x_{k+1} в предикат $\rho(x_1, \ldots, x_k)$ можно с помощью конъюнкции с полной диагональю $x_{k+1} = x_{k+1}$:

$$\rho(x_1, \ldots, x_k) \,\&\, (x_{k+1} = x_{k+1}).$$

Ясно, что из принадлежности одной диагонали $x_1 = x_2$ замкнутому классу предикатов R вытекает принадлежность классу R вообще всех диагоналей. Поэтому иногда в определение формулы над множеством предикатов добавляется еще один пункт, согласно которому формулой над любым множеством предикатов считается выражение $x_1 = x_2$. Это приводит к более широкому понятию замкнутого класса предикатов. Однако далее мы будем пользоваться приведенными выше определениями замыкания и замкнутого класса, оговаривая особо те случаи, когда замкнутый класс содержит все диагонали.

§ 2. Отношение сохранения предиката функцией

Пусть $\rho(x_1, \ldots, x_k)$ — булев предикат, $f(y_1, \ldots, y_n)$ — булева функция. Говорят, что функция $f(y_1, \ldots, y_n)$ *сохраняет предикат* $\rho(x_1, \ldots, x_k)$, если для любых n наборов

$$(a_{11}, \ldots, a_{k1}), \ldots, (a_{1n}, \ldots, a_{kn}),$$

удовлетворяющих предикату ρ, набор

$$(f(a_{11}, \ldots, a_{1n}), \ldots, f(a_{k1}, \ldots, a_{kn}))$$

также удовлетворяет предикату ρ. По определению считаем, что пустой (тождественно ложный) предикат сохраняет любая функция.

Множество истинности непустого предиката $\rho(x_1, \ldots, x_k)$ удобно изображать в виде матрицы X_ρ, состоящей из k строк. Наборы $(a_1, \ldots, a_k)$, удовлетворяющие предикату ρ, записываются в матрице X_ρ (сверху вниз) в виде столбцов, так что элемент a_1 стоит в первой строке, элемент a_2 — во второй и т. д. Порядок столбцов в матрице X_ρ, как правило, несуществен. Число столбцов матрицы X_ρ, то есть количество наборов, удовлетворяющих предикату ρ, называется *шириной* предиката ρ. Отметим, что для диагонали $\delta(x_1, \ldots, x_k)$, соответствующей отношению эквивалентности ε, матрица X_δ состоит из всех

столбцов размера k, в которых совпадают i-й и j-й элементы для любой пары (i, j), удовлетворяющей отношению ε.

В качестве примера рассмотрим предикат

$$\rho(x_1, x_2) \equiv (x_1 \leqslant x_2).$$

Его матрица X_ρ имеет вид

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Если функция $f(x_1, \ldots, x_n)$ сохраняет предикат ρ, то (согласно определению) для любых n наборов

$$(a_{11}, a_{21}), (a_{12}, a_{22}), \ldots, (a_{1n}, a_{2n}),$$

удовлетворяющих соотношениям

$$a_{11} \leqslant a_{21},\ a_{12} \leqslant a_{22}, \ldots, a_{1n} \leqslant a_{2n},$$

будет выполняться соотношение

$$f(a_{11}, a_{12}, \ldots, a_{1n}) \leqslant f(a_{21}, a_{22}, \ldots, a_{2n}).$$

Как видно, мы фактически пришли к определению монотонной функции.

Отношение сохранения предиката $\rho(x_1, \ldots, x_k)$ функцией $f(y_1, \ldots, y_n)$ можно задать в весьма наглядной форме на «матричном» языке. Пусть матрица X_ρ предиката ρ имеет вид

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \ldots & a_{km} \end{pmatrix}. \tag{4.4}$$

Для произвольных n чисел $i_1, \ldots, i_n$, где $1 \leqslant i_1, \ldots, i_n \leqslant m$, из i_1-го, ..., i_n-го столбцов матрицы X_ρ образуем матрицу

$$\begin{pmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \end{pmatrix}. \tag{4.5}$$

Затем к ней по строкам «применим» функцию f:

$$f\begin{pmatrix} a_{1i_1} & a_{1i_2} & \dots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \dots & a_{2i_n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{ki_1} & a_{ki_2} & \dots & a_{ki_n} \end{pmatrix} = \begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \dots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \dots, a_{2i_n}) \\ \dots\dots\dots \\ f(a_{ki_1}, a_{ki_2}, \dots, a_{ki_n}) \end{pmatrix}. \qquad (4.6)$$

Полученный в результате столбец значений также должен быть столбцом матрицы X_ρ.

Для любого предиката ρ из Π_2 через $\mathrm{Pol}(\rho)$ обозначим множество всех функций, сохраняющих предикат ρ, а для любой функции f из P_2 через $\mathrm{Inv}(f)$ — множество всех предикатов, каждый из которых сохраняется функцией f.

Отметим ряд свойств множеств $\mathrm{Pol}(\rho)$ и $\mathrm{Inv}(f)$.

1. *Для любого булева предиката ρ множество* $\mathrm{Pol}(\rho)$ *содержит все селекторные функции*; *для любой булевой функции f множество* $\mathrm{Inv}(f)$ *содержит все диагонали*.

В самом деле, если e_i^n — селекторная функция, то при применении e_i^n к матрице (4.5) в качестве значения получается ее i-й столбец, то есть один из столбцов матрицы (4.4) предиката ρ. Если же $\rho(x_1, \dots, x_k)$ — диагональ и, например, в матрице (4.4) предиката ρ совпадают i-я и j-я строки, то эти же строки будут, очевидно, совпадать в матрице (4.5). Следовательно, в столбце из правой части равенства (4.6) будут равны i-й и j-й элементы. Это означает, что функция f сохраняет диагональ ρ.

Из свойства 1 вытекает, что $\mathrm{Pol}(\rho) = P_2$ для диагонали ρ и $\mathrm{Inv}\, l(f) = \Pi_2$ для селекторной функции f.

2. *Для любого булева предиката ρ множество* $\mathrm{Pol}(\rho)$ *является замкнутым классом булевых функций*.

Поскольку классу $\mathrm{Pol}(\rho)$ принадлежат все селекторные функции, для доказательства свойства 2 достаточно установить, что из $\{f_0, f_1, \dots, f_l\} \subseteq \mathrm{Pol}(\rho)$ и

$$f(y_1, \dots, y_n) = f_0(f_1(y_1, \dots, y_n), \dots, f_l(y_1, \dots, y_n))$$

следует $f \in \mathrm{Pol}(\rho)$. Действительно, из принадлежности функций $f_1, \dots, f_l$ множеству $\mathrm{Pol}(\rho)$ вытекает, что применение каждой из функций $f_1, \dots, f_l$ к матрице (4.5) дает некоторый столбец из матрицы (4.4) предиката ρ. Значит, в силу включения $f_0 \in \mathrm{Pol}(\rho)$ применение функции f_0 к матрице размера $k \times l$, составленной из этих столбцов, вновь дает столбец из матрицы (4.4).

3. *Если π — перестановка на множестве* $\{1, 2, \dots, k\}$ *и*

$$\sigma(x_1, \dots, x_k) \equiv \rho(x_{\pi(1)}, \dots, x_{\pi(k)}),$$

то $\mathrm{Pol}(\sigma) = \mathrm{Pol}(\rho)$.

В самом деле, матрица X_σ получается из матрицы X_ρ путем перестановки строк в соответствии с π^{-1}. Поэтому, применяя перестановку π^{-1} к строкам матрицы X_ρ, можно получить аналоги матрицы (4.5) и равенства (4.6). Это показывает, что $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma)$. Обратное включение доказывается аналогичным образом, поскольку матрица X_ρ, в свою очередь, получается из матрицы X_σ с помощью перестановки строк π.

4. *Пусть предикат* $\sigma(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$ *получается из предиката* $\rho(x_1, \ldots, x_i, \ldots, x_k)$ *проектированием по переменной* x_i:

$$\sigma(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) \equiv (\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k).$$

Тогда $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma)$.

Если предикат ρ пуст или $k = 1$, то предикат σ пуст или полон. В обоих случаях $\mathrm{Pol}(\sigma) = P_2$, и доказываемое включение выполняется тривиально. В остальных случаях, как нетрудно видеть, матрица X_σ получается из матрицы X_ρ вычеркиванием i-ой строки (если при этом образуются одинаковые столбцы, то из каждой группы одинаковых столбцов оставляется один). Поэтому если $f \in \mathrm{Pol}(\rho)$, то для доказательства соотношения $f \in \mathrm{Pol}(\sigma)$ можно пользоваться матрицами (4.4),(4.5) и равенством (4.6), вычеркнув предварительно из них i-ю строку.

5. *Пусть предикат* σ *получается из предиката* ρ *отождествлением переменных. Тогда*

$$\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma).$$

Предположим, например, что

$$\sigma(x_1, \ldots, x_k) \equiv \rho(x_1, \ldots, x_k, x_k).$$

Если предикат σ пуст, то $\mathrm{Pol}(\sigma) = P_2$ и требуемое включение выполняется тривиально. В противном случае рассмотрим произвольную функцию $f(y_1, \ldots, y_n)$ из класса $\mathrm{Pol}(\rho)$. Если каждый столбец матрицы (4.5) является столбцом матрицы X_σ, то по определению предиката σ в матрицу X_ρ будет входить каждый столбец матрицы

$$\begin{pmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \end{pmatrix}.$$

Из включения $f \in \mathrm{Pol}(\rho)$ следует, что столбец

$$\begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \ldots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \ldots, a_{2i_n}) \\ \vdots \\ f(a_{ki_1}, a_{ki_2}, \ldots, a_{ki_n}) \\ f(a_{ki_1}, a_{ki_1}, \ldots, a_{ki_n}) \end{pmatrix}$$

также является столбцом матрицы X_ρ. Однако последние две компоненты этого столбца равны. Поэтому в матрицу X_σ входит столбец

$$\begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \ldots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \ldots, a_{2i_n}) \\ \vdots \\ f(a_{ki_1}, a_{ki_2}, \ldots, a_{ki_n}) \end{pmatrix},$$

что доказывает включение $f \in \mathrm{Pol}(\sigma)$.

6. *Пусть предикат* $\tau(x_1, \ldots, x_k, y_1, \ldots, y_l)$ *получается конъюнкцией непустых предикатов* $\rho(x_1, \ldots, x_k)$ *и* $\sigma(y_1, \ldots, y_l)$:

$$\tau(x_1, \ldots, x_k, y_1, \ldots, y_l) \equiv \rho(x_1, \ldots, x_k) \,\&\, \sigma(y_1, \ldots, y_l).$$

Тогда

$$\mathrm{Pol}(\tau) = \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma).$$

В самом деле, в силу определения предиката τ имеем

$$\rho(x_1, \ldots, x_k) \equiv (\exists y_1) \ldots (\exists y_l)\tau(x_1, \ldots, x_k, y_1, \ldots, y_l),$$

$$\sigma(y_1, \ldots, y_l) \equiv (\exists x_1) \ldots (\exists x_k)\tau(x_1, \ldots, x_k, y_1, \ldots, y_l).$$

Отсюда по свойству 4 получаем

$$\mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\rho), \quad \mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\sigma)$$

и, следовательно,

$$\mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma).$$

Пусть теперь $f(z_1, \ldots, z_n) \in \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma)$. Нетрудно видеть, что столбцы матрицы X_τ получаются из столбцов матриц X_ρ и X_σ следующим образом: берется произвольный столбец матрицы X_ρ и к нему снизу приписывается произвольный столбец

матрицы X_σ. Возьмем произвольные n столбцов в матрице X_τ:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kn} \\ a_{k+1,1} & a_{k+1,2} & \dots & a_{k+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k+l,1} & a_{k+l,2} & \dots & a_{k+l,n} \end{pmatrix}.$$

Как отмечено, столбцы матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}$$

входят в матрицу X_ρ, а столбцы матрицы

$$\begin{pmatrix} a_{k+1,1} & a_{k+1,2} & \dots & a_{k+1,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k+l,1} & a_{k+l,2} & \dots & a_{k+l,n} \end{pmatrix}$$

— в матрицу X_σ. Поэтому в силу соотношения $f \in \mathrm{Pol}(\rho)$ столбец

$$\begin{pmatrix} f(a_{11}, a_{12}, \dots, a_{1n}) \\ \vdots \\ f(a_{k1}, a_{k2}, \dots, a_{kn}) \end{pmatrix}$$

будет входить в матрицу X_ρ и в силу соотношения $f \in \mathrm{Pol}(\sigma)$ столбец

$$\begin{pmatrix} f(a_{k+1,1}, a_{k+1,2}, \dots, a_{k+1,n}) \\ \vdots \\ f(a_{k+l,1}, a_{k+l,2}, \dots, a_{k+l,n}) \end{pmatrix}$$

будет входить в матрицу X_σ. Значит, столбец

$$\begin{pmatrix} f(a_{11}, a_{12}, \dots, a_{1n}) \\ \vdots \\ f(a_{k1}, a_{k2}, \dots, a_{kn}) \\ f(a_{k+1,1}, a_{k+1,2}, \dots, a_{k+1,n}) \\ \vdots \\ f(a_{k+l,1}, a_{k+l,2}, \dots, a_{k+l,n}) \end{pmatrix}$$

будет входить в матрицу X_τ, то есть $f \in \mathrm{Pol}(\tau)$.

7. Если предикаты ρ и σ отличаются только несущественными переменными, то

$$\mathrm{Pol}(\rho) = \mathrm{Pol}(\sigma). \tag{4.7}$$

Пусть например, предикат $\sigma(x_1, \ldots, x_k, x_{k+1})$ получается из предиката $\rho(x_1, \ldots, x_k)$ добавлением несущественной переменной x_{k+1}. Тогда

$$\sigma(x_1, \ldots, x_k, x_{k+1}) \equiv \rho(x_1, \ldots, x_k) \,\&\, (x_{k+1} = x_{k+1}).$$

Поэтому свойства 6 и 1 дают равенство (4.7).

8. *Для любой функции f из P_2 множество* $\mathrm{Inv}(f)$ *является замкнутым классом, содержащим все диагонали.*

Это свойство есть следствие свойств 1 и 3–6.

9. *Если* $R = \mathrm{Pol}(\rho(x_1, \ldots, x_k))$, *то* $R^* = \mathrm{Pol}(\rho(\overline{x}_1, \ldots, \overline{x}_k))$.

Достаточно заметить, что матрица $\overline{X}_\rho$ предиката $\rho(\overline{x}_1, \ldots, \overline{x}_k)$ получается из матрицы X_ρ предиката $\rho(x_1, \ldots, x_k)$ заменой нулей единицами и единиц нулями.

§ 3. Соответствие Галуа

Обозначим через $\Phi(f, \rho)$ отношение «булева функция f сохраняет булев предикат ρ» на множестве $P_2 \times \Pi_2$. Отношение Φ определяет *соответствие Галуа* между подмножествами множеств P_2 и Π_2. Более подробно, если F — произвольное подмножество множества P_2, а R — произвольное подмножество множества Π_2, то пусть

$$\mathrm{Inv}(F) = \bigcap_{f \in F} \mathrm{Inv}(f), \quad \mathrm{Pol}(R) = \bigcap_{\rho \in R} \mathrm{Pol}(\rho).$$

Из опредений вытекает, что отображения Inv и Pol антимонотонны: если $F_1 \subseteq F_2$ и $R_1 \subseteq R_2$, то

$$\mathrm{Inv}(F_1) \supseteq \mathrm{Inv}(F_2), \quad \mathrm{Pol}(R_1) \supseteq \mathrm{Pol}(R_2). \tag{4.8}$$

Кроме того, для произвольных подмножеств F из P_2 и R из Π_2 очевидным образом выполняются соотношения

$$F \subseteq \mathrm{Pol}(\mathrm{Inv}(F)), \tag{4.9}$$

$$R \subseteq \mathrm{Inv}(\mathrm{Pol}(R)). \tag{4.10}$$

Соотношения (4.8)–(4.10) показывают, что пара отображений Inv и Pol является *соответствием Галуа* между частично упорядоченными по включению множествами всех подмножеств P_2 и Π_2. Множество $\mathrm{Pol}(\mathrm{Inv}(F))$ называется *Галуа-замыканием* F, а множество $\mathrm{Inv}(\mathrm{Pol}(R))$ — *Галуа-замыканием* R. Нетрудно убедиться в том, что Галуа-замыкания обладают всеми свойствами обычного замыкания.

Из свойств 1, 2, 8 § 2 вытекает, что $\mathrm{Inv}(F)$ является замкнутым классом булевых предикатов, содержащим все диагонали, а $\mathrm{Pol}(R)$ — замкнутым классом булевых функций, содержащим все селекторные функции. В частности, такими же замкнутыми классами будут Галуа-замыкания $\mathrm{Pol}(\mathrm{Inv}(F))$ и $\mathrm{Inv}(\mathrm{Pol}(R))$.

Основное содержание *теории Галуа для классов Поста* состоит в доказательстве обратных утверждений: всякий замкнутый класс F булевых функций, содержащий все селекторные функции, представляет собой Галуа-замыкание подходящего множества булевых функций; всякий замкнутый класс R булевых предикатов, содержащий все диагонали, представляет собой Галуа-замыкание подходящего множества булевых предикатов. Более того, для упомянутых классов F и R имеют место равенства

$$F = \mathrm{Pol}(\mathrm{Inv}(F)), \quad R = \mathrm{Inv}(\mathrm{Pol}(R)).$$

Доказательству этих утверждений будет посвящена оставшаяся часть этого параграфа.

Пусть F — произвольное множество булевых функций, n — натуральное число, $\widetilde{a}_1, \widetilde{a}_2, \ldots, \widetilde{a}_{2^n}$ — все двоичные наборы длины n, расположенные в лексикографическом порядке. Назовем *n-графиком* множества F 2^n-местный предикат $\gamma_n(y_1, \ldots, y_{2^n})$, которому удовлетворяют те и только те наборы длины 2^n, которые имеют вид

$$(f(\widetilde{a}_1), f(\widetilde{a}_2), \ldots, f(\widetilde{a}_{2^n})),$$

где f — n-местная функция из F.

Теорема 4.1. *Пусть F — замкнутый класс булевых функций, содержащий все селекторные функции. Тогда $F = \mathrm{Pol}(\mathrm{Inv}(F))$.*

Доказательство. Ввиду справедливости включения (4.9) для доказательства теоремы достаточно установить лишь включение

$$\mathrm{Pol}(\mathrm{Inv}(F)) \subseteq F. \tag{4.11}$$

Докажем сначала, что при любом n ($n \geqslant 1$) n-график γ_n класса F принадлежит множеству $\mathrm{Inv}(F)$. Действительно, пусть $g(x_1, \ldots, x_m)$ — произвольная функция из F, а наборы

$$(a_1^1, \ldots, a_{2^n}^1), \ldots, (a_1^m, \ldots, a_{2^n}^m),$$

удовлетворяющие предикату γ_n, отвечают n-местным функциям $f_1, \ldots, f_m$ из F. Тогда набор

$$(g(a_1^1, \ldots, a_1^m), \ldots, g(a_{2^n}^1, \ldots, a_{2^n}^m)) \tag{4.12}$$

имеет вид

$$(h(\widetilde{a}_1), h(\widetilde{a}_2), \ldots, h(\widetilde{a}_{2^n})),$$

где

$$h(x_1, \ldots, x_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

В силу замкнутости класса F n-местная функция h принадлежит классу F. Следовательно, набор (4.12) удовлетворяет предикату γ_n и $\gamma_n \in \mathrm{Inv}(F)$.

Теперь нетрудно установить включение (4.11). В самом деле, пусть $f(x_1, \ldots, x_n)$ — произвольная функция из множества $\mathrm{Pol}(\mathrm{Inv}(F))$. Тогда, в частности, f сохраняет предикат γ_n. Возьмем n наборов

$$(a_1^1, \ldots, a_{2^n}^1), \ldots, (a_1^n, \ldots, a_{2^n}^n),$$

которые удовлетворяют предикату γ_n и отвечают селекторным функциям $e_1^n, \ldots, e_n^n$. Тогда набор

$$(f(a_1^1, \ldots, a_1^n), \ldots, f(a_{2^n}^1, \ldots, a_{2^n}^n)) \tag{4.13}$$

также удовлетворяет предикату γ_n. Однако

$$f(e_1^n(x_1, \ldots, x_n), \ldots, e_n^n(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n).$$

Поэтому набор (4.13) совпадает с набором

$$(f(\widetilde{a}_1), f(\widetilde{a}_2), \ldots, f(\widetilde{a}_{2^n})).$$

А это (согласно определению предиката γ_n) означает, что $f \in F$. Теорема доказана.

Предикат ρ назовем *стандартным*, если соответствующая ему матрица X_ρ не содержит одинаковых строк.

Лемма 4.1. *Пусть F — множество булевых функций, содержащее все селекторные функции, $\rho(x_1, \ldots, x_k)$ — стандартный предикат ширины n и $\rho \in \mathrm{Inv}(F)$. Тогда ρ получается из n-графика γ_n множества F с помощью операций проектирования и перестановки переменных.*

Доказательство. Поскольку F содержит все селекторные функции, без ограничения общности можно считать, что в матрице X_{γ_n} n-графика γ_n первые n столбцов отвечают селекторным функциям $e_1^n, \ldots, e_n^n$. Тогда любой двоичный набор длины n является началом подходящей строки матрицы X_{γ_n}. Пусть j-я строка матрицы X_ρ предиката ρ является началом i_j-ой строки матрицы X_{γ_n} $(1 \leqslant j \leqslant k)$. Так как $\rho \in \mathrm{Inv}(F)$, то, используя при необходимости свойство 3 из § 2, заключаем, что в подматрице матрицы X_{γ_n}, образованной строками с номерами $i_1, \ldots, i_k$,

каждый столбец начиная с $(n+1)$-го равен одному из первых n столбцов. Следовательно, если спроектировать предикат γ_n по всем переменным, отличным от переменных $x_{i_1}, \ldots, x_{i_k}$, то получится k-местный предикат, который будет отличаться от предиката ρ, быть может, лишь перестановкой переменных. Лемма доказана.

Теорема 4.2. *Пусть R — замкнутый класс предикатов, содержащий все диагонали. Тогда $R = \mathrm{Inv}(\mathrm{Pol}(R))$.*

Доказательство. Так как включение (4.10) справедливо для любых множеств R булевых предикатов, для доказательства теоремы достаточно установить включение

$$\mathrm{Inv}(\mathrm{Pol}(R)) \subseteq R. \tag{4.14}$$

Далее (в силу леммы 4.1), всякий стандартный предикат $\sigma_1(x_1, \ldots, x_l)$ из $\mathrm{Inv}(\mathrm{Pol}(R))$ ширины n получается из n-графика γ_n множества $\mathrm{Pol}(R)$ с помощью проектирования и перестановки переменных. Кроме того, если предикат σ_2 не является стандартным, то его можно получить из подходящего стандартного предиката с помощью формулы, содержащей диагональ. Например, если матрица X_{σ_2} предиката $\sigma_2(x_1, \ldots, x_l, x_{l+1})$ получается из матрицы X_{σ_1} предиката σ_1 повторением последней строки, то

$$\sigma_2(x_1, \ldots, x_l, x_{l+1}) \equiv \sigma_1(x_1, \ldots, x_l) \,\&\, (x_l = x_{l+1}).$$

Таким образом, включение (4.14) будет доказано, если мы установим, что при любом n $(n \geqslant 1)$ n-график γ_n множества $\mathrm{Pol}(R)$ реализуется некоторой формулой над множеством R.

Отметим еще, что это утверждение достаточно доказать для всех значений n, больших некоторого. В самом деле, для всякой n-местной функции f из $\mathrm{Pol}(R)$ в $\mathrm{Pol}(R)$ имеется $(n+1)$-местная функция, которая получается из f добавлением фиктивной переменной. Поэтому n-график множества $\mathrm{Pol}(R)$ можно получить из $(n+1)$-графика множества $\mathrm{Pol}(R)$ проектированием, например, по последним 2^n переменным.

Рассмотрим вначале случай, когда множество $\mathrm{Pol}(R)$ порождается одним предикатом, то есть существует такой предикат $\rho(x_1, \ldots, x_k)$ из R, что

$$\mathrm{Pol}(R) = \mathrm{Pol}(\rho).$$

Пусть ширина предиката ρ равна s. Зафиксируем натуральное число $n \geqslant 2^k$ и будем предполагать, что первые n столбцов матрицы X_{γ_n} соответствуют селекторным функ-

циям $e_1^n(x_1,\dots,x_n),\dots,e_n^n(x_1,\dots,x_n)$. Посмотрим, каким требованиям удовлетворяют все остальные столбцы матрицы X_{γ_n}. Очевидно, что эти требования вытекают из принадлежности соответствующих функций классу $\mathrm{Pol}(\rho)$. Именно: если в подматрице матрицы X_{γ_n}, образованной произвольными k строками, первые n столбцов принадлежат матрице X_ρ, то и остальные столбцы этой подматрицы также принадлежат матрице X_ρ. Следовательно, «максимальная» (по числу столбцов) матрица с 2^n строками, у которой в первых n столбцах расположены значения селекторных функций $e_1^n,\dots,e_n^n$ и которая удовлетворяет сформулированному условию, и будет являться матрицей X_{γ_n}. Этими соображениями мы будем руководствоваться при построении предиката γ_n из предиката ρ.

Положим $l=s^n$ (при $s=1$ полагаем $l=2^n$) и пусть

$$\rho_1(x_1^1,\dots,x_k^1,\dots,x_1^l,\dots,x_k^l)\equiv\rho(x_1^1,\dots,x_k^1)\,\&\,\dots\,\&\,\rho(x_1^l,\dots,x_k^l).$$

Из определений предиката ρ_1 и операции конъюнкции следует, что в матрице X_{ρ_1} можно так расположить столбцы, что для любых (не обязательно различных) n столбцов матрицы X_ρ в матрице X_{ρ_1} найдутся такие k строк, что подматрица матрицы X_{ρ_1}, образованная этими k строками, в качестве первых n столбцов содержит указанные столбцы матрицы X_ρ. Из определения предиката ρ_1 следует также, что в качестве этих k строк всегда можно выбрать строки с номерами $ik+1,\dots,(i+1)k$.

Мы хотели бы рассматривать матрицу X_{ρ_1} как «заготовку» для получения матрицы X_{γ_n}. Как и в матрице X_{γ_n}, первые n столбцов матрицы X_{ρ_1} будут соответствовать селекторным функциям $e_1^n,\dots,e_n^n$, а остальные столбцы — другим функциям из класса $\mathrm{Pol}(\rho)$.

Отметим все отличия матрицы X_{ρ_1} от матрицы X_{γ_n}. Во-первых, в матрице X_{ρ_1} могут содержаться различные строки, у которых совпадают начала длины n. Во-вторых, начала строк длины n в матрице X_{ρ_1} расположены не обязательно в лексикографическом порядке. В-третьих, в матрице X_{ρ_1} среди начал строк длины n могут не содержаться некоторые двоичные наборы длины n. Наконец, мы должны быть уверены в том, что в столбцах матрицы X_{ρ_1} потенциально «содержатся» все функции из класса $\mathrm{Pol}(\rho)$.

Довольно просто убедиться в выполнении последнего требования. Действительно, для любых l столбцов матрицы X_ρ в матрице X_{ρ_1} содержится столбец, который составлен из этих l столбцов. Если вспомнить свойство, которым мы наделили первые n столбцов матрицы X_{ρ_1}, то становится понят-

но, что функции, потенциально «содержащиеся» в столбцах матрицы X_{ρ_1}, удовлетворяют всем требованиям сохранения предиката ρ.

Далее мы последовательно устраним отмеченные выше отличия матрицы X_{ρ_1} от матрицы X_{γ_n}.

Чтобы избавиться от первого нежелательного свойства, определим отношение эквивалентности ε на множестве $\{1, 2, \ldots, kl\}$, полагая $\varepsilon(i, j)$ истинным в том только том случае, когда в матрице X_{ρ_1} у строк с номерами i, j совпадают начала длины n. Отождествляя в предикате ρ_1 все переменные, которым в отношении ε отвечают эквивалентные номера строк, образуем предикат ρ_2, в матрице X_{ρ_2} которого различны строки с различными началами длины n. В результате мы избавляемся от столбцов матрицы X_{ρ_1}, которые (в силу многозначности) не могут определять функции от n переменных.

Переставим далее в предикате ρ_2 переменные так, чтобы в матрице X_{ρ_3} полученного предиката $\rho_3(y_1, \ldots, y_m)$ наборы длины n, начинающие строки матрицы X_{ρ_3}, следовали в лексикографическом порядке. Если после этого окажется, что $m < 2^n$, то с помощью операции конъюнкции с полными диагоналями добавим к предикату ρ_3 фиктивные переменные $y_{m+1}, \ldots, y_{2^n}$:

$$\rho_4(y_1, \ldots, y_{2^n}) \equiv \\ \equiv \rho_3(y_1, \ldots, y_m) \,\&\, (y_{m+1} = y_{m+1}) \,\&\, \ldots \,\&\, (y_{2^n} = y_{2^n}).$$

Нетрудно видеть, что предикат ρ_4 и будет совпадать с предикатом γ_n.

Обратимся теперь к случаю, когда множество $\mathrm{Pol}(R)$ не порождается одним предикатом. Согласно свойству 6 из § 2 это равносильно тому, что множество $\mathrm{Pol}(R)$ не порождается конечным числом предикатов из R. Пусть поэтому $R = \{\rho_1, \rho_2, \ldots\}$. Тогда по определению отображения Pol имеем

$$\mathrm{Pol}(R) = \bigcap_{i=1}^{\infty} \mathrm{Pol}(\{\rho_1, \ldots, \rho_i\}).$$

Используя свойство 6 из § 2, перепишем это равенство в виде

$$\mathrm{Pol}(R) = \bigcap_{i=1}^{\infty} \mathrm{Pol}(\sigma_i), \tag{4.15}$$

где предикат σ_i получен конъюнкцией предикатов $\rho_1, \ldots, \rho_i$. Очевидно также, что

$$\mathrm{Pol}(\sigma_1) \supseteq \mathrm{Pol}(\sigma_2) \supseteq \ldots . \tag{4.16}$$

Для любого n ($n \geqslant 1$) множество n-местных функций из $\mathrm{Pol}(R)$ конечно. Поэтому из соотношений (4.15) и (4.16) вытекает, что для любого n найдется такое i_n, что у множеств $\mathrm{Pol}(R)$ и $\mathrm{Pol}(\sigma_{i_n})$ совпадают множества n-местных функций. Следовательно, по доказанному, предикат γ_n реализуется формулой, содержащей предикат σ_{i_n} и диагонали. Теорема доказана.

Пусть $\mathcal{M}$ обозначает частично упорядоченное по включению множество всех замкнутых классов булевых функций, содержащих все селекторные функции, $\mathcal{N}$ — частично упорядоченное по включению множество всех замкнутых классов булевых предикатов, содержащих все диагонали. Теоремы 4.1, 4.2 и соотношения (4.8) показывают, что отображения Pol и Inv устанавливают антиизоморфизм частично упорядоченных множеств $\mathcal{M}$ и $\mathcal{N}$. Это позволяет, например, для множества $\mathcal{N}$ строить диаграмму включений, аналогичную диаграмме Поста, если предварительно исключить из последней точки, соответствующие классам C_0, C_1, C (эти и только эти замкнутые классы не содержат селекторных функций). Многие утверждения, касающиеся замкнутых классов булевых функций, имеют свои очевидные аналоги для замкнутых классов булевых предикатов. Поэтому некоторые факты из глав I, II можно устанавливать принципиально иным способом: сначала на языке булевых предикатов доказать аналоги этих фактов, а затем перенести их на булевы функции, пользуясь антиизоморфизмом частично упорядоченных множеств $\mathcal{M}$ и $\mathcal{N}$.

§ 4. Замкнутые классы, определяемые конечным числом предикатов

Согласно результатам § 3 всякий замкнутый класс булевых функций, содержащий все селекторные функции, определяется подходящим множеством булевых предикатов (может быть, бесконечным). Оказывается, что «почти все» замкнутые классы булевых функций можно задать конечным множеством предикатов, т. е. представить в виде $\mathrm{Pol}(R)$, где множество R состоит из конечного числа предикатов. Ниже, в теореме 4.3, полностью охарактеризованы замкнутые классы, обладающие этим свойством. Поскольку в соответствии со свойством 6 из § 2 при определении замкнутого класса булевых функций конечное множество предикатов можно заменить одним предикатом, в доказательстве теоремы 4.3 рассматриваются лишь одноэлементные множества предикатов.

Теорема 4.3. *Для того чтобы замкнутый класс R булевых функций, отличный от P_2, определялся конечным множеством предикатов, необходимо и достаточно, чтобы выполнялись следующие условия: R содержит все селекторные функции и существует конечная последовательность $R_1, \ldots, R_s$ замкнутых классов такая, что класс R строго содержится в каждом из классов $R_1, \ldots, R_s$ и всякий замкнутый класс, строго содержащий R, включает хотя бы один из классов $R_1, \ldots, R_s$.*

Доказательство. *Необходимость.* Пусть замкнутый класс R определяется предикатом $\rho(x_1, \ldots, x_k)$, т. е. $R = \mathrm{Pol}(\rho)$. Согласно свойству 1 из § 2, класс R содержит все селекторные функции. Предполагая, что $R \neq P_2$, возьмем произвольный замкнутый класс R' такой, что $R \subset R'$ (включение строгое). Тогда в классе R' найдется функция $f(y_1, \ldots, y_n)$, которая не сохраняет предикат ρ. Это значит, что можно выбрать такие n наборов

$$(a_{11}, \ldots, a_{k1}), \ldots, (a_{1n}, \ldots, a_{kn}), \tag{4.17}$$

удовлетворяющих предикату ρ, что набор

$$(f(a_{11}, \ldots, a_{1n}), \ldots, f(a_{k1}, \ldots, a_{kn})) \tag{4.18}$$

не удовлетворяет предикату ρ.

Пусть предикат ρ имеет ширину m. Если $n > m$, то среди наборов (4.17) имеются одинаковые. Отождествляя в функции f соответствующие переменные, получим функцию f' из класса R', зависящую не более чем от m переменных, которая тоже не сохраняет предикат ρ (мы получим тот же самый набор (4.18), если из каждой группы одинаковых столбцов матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \end{pmatrix}$$

оставим один и применим к полученной матрице функцию f').

Таким образом, всякий замкнутый класс, строго содержащий класс R, включает функцию, не принадлежащую классу R и зависящую не более чем от m переменных. Если $f_1, \ldots, f_s$ — все такие функции, то любой замкнутый класс, содержащий класс R и отличный от него, содержит хотя бы один из замкнутых классов

$$[R \cup \{f_1\}], \ \ldots, \ [R \cup \{f_s\}].$$

Достаточность. Пусть замкнутый класс R отличен от P_2, содержит все селекторные функции, а замкнутые классы $R_1, \ldots, R_s$ выбраны в соответствии с условиями теоремы. Выберем число m так, чтобы множество $R^{(m)}$ всех m-местных функций из R отличалось от любого из множеств $R_1^{(m)}, \ldots, R_s^{(m)}$. Докажем, что $R = \mathrm{Pol}(\gamma_m)$, где γ_m — m-график множества R.

В самом деле, очевидно, что все функции из R сохраняют предикат γ_m и потому $R \subseteq \mathrm{Pol}(\gamma_m)$. С другой стороны, если замкнутый класс $\mathrm{Pol}(\gamma_m)$ отличен от R, то он целиком включает некоторый класс R_i и, следовательно, по выбору числа m содержит некоторую функцию $f(y_1, \ldots, y_m)$, не входящую в множество $R^{(m)}$. Однако функция f не может сохранять предикат γ_m, поскольку в $R^{(m)}$ содержатся селекторные функции $e_1^m, \ldots, e_m^m$ и

$$f(e_1^m(y_1, \ldots, y_m), \ldots, e_m^m(y_1, \ldots, y_m)) = f(y_1, \ldots, y_m).$$

Таким образом, класс $\mathrm{Pol}(\gamma_m)$ не может отличаться от класса R; теорема доказана.

Следствие. *Любой замкнутый класс булевых функций, отличный от классов*

$$O^\infty,\ O_0^\infty,\ MO^\infty,\ MO_0^\infty,\ I^\infty,\ I_1^\infty,\ MI^\infty,\ MI_1^\infty,\ C,\ C_0,\ C_1, \tag{4.19}$$

определяется конечным числом предикатов. Никакой из классов (4.19) *нельзя определить конечным числом предикатов.*

Доказательство. Как отмечалось выше, класс P_2 определяется любой диагональю. Классы C, C_0, C_1 не содержат селекторных функций и потому вообще не могут определяться никаким множеством булевых предикатов. Для всех остальных замкнутых классов из списка (4.19) вопрос о задании их с помощью конечного числа предикатов решается на основе теоремы 4.3 и анализа диаграммы включений замкнутых классов.

Доказательство теоремы 4.3 указывает на некоторый предикат, определяющий заданный замкнутый класс R. А именно: этим предикатом является m-график γ_m класса R, где число m выбрано так, что множество $R^{(m)}$ отличается от множеств $Q^{(m)}$ для любых классов Q, непосредственно содержащих класс R. Однако (как правило) такой предикат γ_m является избыточным. Более простые предикаты, задающие класс R, можно получить из предиката γ_m с помощью проектирования. Отметим, что все такие предикаты принадлежат классу $\mathrm{Inv}(R)$, поскольку $R = \mathrm{Pol}(\gamma_m)$.

В качестве примера рассмотрим предикатное задание предполных классов T_0, T_1, S, M, L. Легко видеть, что каждое из множеств $T_0^{(1)}$, $T_1^{(1)}$, $S^{(1)}$, $M^{(1)}$ отлично от множества $P_2^{(1)}$. Поэтому каждый из классов T_0, T_1, S, M можно задать одним двуместным предикатом — 1-графиком соответствующего класса. Для классов S и M матрицы 1-графиков имеют вид (для класса M соответствующую матрицу мы построили в § 2)

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

а для классов T_0 и T_1

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Нетрудно понять, что 1-график класса S эквивалентен предикату $x_1 \neq x_2$, а 1-график класса M — предикату $x_1 \leqslant x_2$. Далее заметим, что 1-график класса T_0 получается из предиката $x = 0$ добавлением фиктивной переменной. Поэтому согласно свойству 7 из § 2 имеем

$$T_0 = \mathrm{Pol}\{x = 0\}.$$

Аналогичным образом показываем, что класс T_1 определяется предикатом $x = 1$. К такому же выводу мы придем, если воспользуемся равенствами $T_0 = \mathrm{Pol}\{x = 0\}$, $T_1 = T_0^*$ и свойством 9 из § 2.

Для класса L множество $L^{(1)}$ совпадает с множеством $P_2^{(1)}$ (1-график класса L является полным предикатом), однако множества $L^{(2)}$ и $P_2^{(2)}$ уже различны. Матрица 2-графика класса L имеет вид

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

а сам 2-график эквивалентен предикату $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$. Нетрудно проверить, что отождествлением переменных и проектированием из 2-графика класса L можно получить лишь диагонали.

Покажем, что предикаты, определяющие предполные классы T_0, T_1, S, M, L, имеют наименьшее возможное число переменных. Это очевидно для предикатов $x = 0$ и $x = 1$, задающих классы T_0 и T_1, и почти очевидно для двуместных предикатов, определяющих классы S и M, поскольку всякий непустой и неполный одноместный предикат совпадает с одним из предикатов

$x = 0$ или $x = 1$. Таким образом, остается исследовать на минимальность числа переменных предикат $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$, который задает класс L.

Пусть в класс $\mathrm{Inv}(L)$ входит двух- или трехместный предикат λ. Поскольку функции $0, 1, \overline{x}$ принадлежат классу L, матрица X_λ предиката λ содержит нулевой и единичный столбцы и вместе с любым столбцом матрице X_λ принадлежит столбец из противоположных значений (противоположный столбец). Если предикат λ зависит от двух переменных, то мы имеем две возможные матрицы X_λ:

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Первая матрица определяет диагональ $x_1 = x_2$, вторая — полный предикат.

Пусть предикат λ зависит от трех переменных. Матрица X_λ не может состоять только из нулевого и единичного столбцов, иначе предикат λ был бы диагональю. Значит, X_λ содержит по крайней мере две пары противоположных столбцов. Если ширина предиката λ равна четырем, то матрица X_λ содержит две одинаковые строки. Как нетрудно видеть, в этом случае класс $\mathrm{Pol}(\lambda)$ можно определить двуместным предикатом, что невозможно. Следовательно, ширина предиката λ не меньше шести. Используя теперь включение $(x \oplus y) \in \mathrm{Pol}(\lambda)$, легко убеждаемся в том, что матрица X_λ наряду с тремя парами противоположных столбцов обязательно содержит и четвертую пару противоположных столбцов. Таким образом, предикат λ оказывается полным.

§ 5. Предикатное задание замкнутых классов

В предыдущем параграфе мы нашли предикаты, которые задают предполные классы T_0, T_1, S, M, L. Здесь мы рассмотрим все остальные замкнутые классы.

Класс U определяется предикатом $x_1 = x_2 \vee x_1 = x_3$. В самом деле, выписав матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{4.20}$$

предиката $x_1 = x_2 \vee x_1 = x_3$, легко убедиться в том, что функции класса U сохраняют данный предикат. Вместе с тем класс U непосредственно содержится только в классе L, а линейная

функция $x_1 \oplus x_2$ не сохраняет предикат $x_1 = x_2 \vee x_1 = x_3$ (достаточно рассмотреть 2-й и 3-й столбцы матрицы (4.20)).

Предикат $x_1 = x_2 x_3$ имеет матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \tag{4.21}$$

Убеждаемся, что функции $0,\ 1,\ xy$, образующие базис класса K, сохраняют предикат $x_1 = x_2 x_3$. Значит,

$$K \subseteq \mathrm{Pol}\{x_1 = x_2 x_3\}.$$

Класс K непосредственно содержится только в классе M, а монотонная функция $x \vee y$ не сохраняет предикат $x_1 = x_2 x_3$ (следует рассмотреть 2-й и 3-й столбцы матрицы (4.21)). Следовательно, класс K можно задать предикатом $x_1 = x_2 x_3$.

Покажем, что при любом m $(m \geqslant 2)$ класс I^m определяется предикатом $x_1 \cdot \ldots \cdot x_m = 0$. Заметим, что матрица предиката $x_1 \cdot \ldots \cdot x_m = 0$ состоит из всех столбцов высоты m, отличных от единичного столбца. Функции $x\overline{y}$ и

$$d^*_{m+1}(x_1, \ldots, x_{m+1}) = \mathop{\&}_{1 \leqslant i < j \leqslant m+1} (x_i \vee x_j),$$

образующие базис класса I^m, сохраняют предикат $x_1 \cdot \ldots \cdot x_m = 0$. Значит,

$$I^m \subseteq \mathrm{Pol}\{x_1 \cdot \ldots \cdot x_m = 0\}.$$

С другой стороны, класс I^2 непосредственно содержится только в классе T_0, а класс I^m при $m \geqslant 3$ — только в классе I^{m-1}. Для доказательства равенства

$$I^m = \mathrm{Pol}\{x_1 \cdot \ldots \cdot x_m = 0\}$$

остается теперь проверить, что функция $x \vee y$ из класса T_0 не сохраняет предикат $x_1 \cdot x_2 = 0$ (достаточно рассмотреть противоположные столбцы в матрице предиката $x_1 \cdot x_2 = 0$), а при $m \geqslant 3$ функция $d^*_m(x_1, \ldots, x_m)$ из класса I^{m-1} не сохраняет предикат $x_1 \cdot \ldots \cdot x_m = 0$:

$$d^*_m \begin{pmatrix} 0 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \ldots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \ldots & 0 & 1 \\ 1 & 1 & \ldots & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \cdots \\ 1 \\ 1 \end{pmatrix}.$$

Согласно свойству 9 из § 2 класс D, двойственный классу K, определяется предикатом $x_1 = x_2 \vee x_3$, а класс O^m, двойственный классу I^m, предикатом $x_1 \vee \ldots \vee x_m = 1$.

Все остальные замкнутые классы булевых функций, отличные от классов C, C_0, C_1, можно представить в виде пересечения подходящих классов из числа

$$T_0,\ T_1,\ S,\ M,\ L,\ U,\ K,\ D,\ I^m,\ O^m \quad (m = 2, 3, \ldots).$$

Поэтому (согласно свойству 6 из § 2) будут иметь место следующие утверждения:

- класс T_{01} как пересечение классов T_0 и T_1 определяется предикатами $x = 0,\ x = 1$;
- класс M_0 как пересечение классов T_0 и M определяется предикатами $x = 0,\ x_1 \leqslant x_2$;
- класс M_{01} как пересечение классов T_0, T_1 и M определяется предикатами $x = 0,\ x = 1, x_1 \leqslant x_2$;
- класс S_{01} как пересечение классов T_0 и S определяется предикатами $x = 0,\ x_1 \neq x_2$;
- класс SM как пересечение классов S и M определяется предикатами $x_1 \neq x_2,\ x_1 \leqslant x_2$;
- классы K_0, K_1 и K_{01} как пересечения класса K, соответственно, с классами T_0, T_1 и T_{01} определяются предикатами
$$\{x = 0,\ x_1 = x_2 x_3\},\ \{x = 1,\quad x_1 = x_2 x_3\},$$
$$\{x = 0,\ x = 1,\ x_1 = x_2 x_3\};$$
- класс MU как пересечение классов M и U определяется предикатами $x_1 \leqslant x_2,\ x_1 = x_2 \vee x_1 = x_3$;
- класс U_0 как пересечение классов T_0 и U определяется предикатами $x = 0,\ x_1 = x_2 \vee x_1 = x_3$;
- класс U_{01} как пересечение классов T_{01} и U определяется предикатами $x = 0,\ x = 1,\ x_1 = x_2 \vee x_1 = x_3$.

Из $L_0 = T_0 \cap L$ следует, что

$$L_0 = \mathrm{Pol}\{x = 0,\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\}.$$

Однако

$$(x_1 \oplus x_2 \oplus x_3 = 0) \equiv (\exists y)((y = 0)\ \&\ (x_1 \oplus x_2 \oplus x_3 \oplus y = 0))$$

и

$$(x = 0) \equiv (x \oplus x \oplus x = 0),$$
$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0) \equiv$$
$$\equiv (\exists y)((x_1 \oplus x_2 \oplus y = 0)\ \&\ (x_3 \oplus x_4 \oplus y = 0)).$$

Поэтому

$$L_0 = \mathrm{Pol}\{x_1 \oplus x_2 \oplus x_3 = 0\}.$$

Поскольку $L_{01} = T_1 \cap L_0$, имеем

$$L_{01} = \mathrm{Pol}\{x = 1,\ x_1 \oplus x_2 \oplus x_3 = 0\}.$$

Из соотношений $SL = S \cap L$ и

$$(x_1 \neq x_2) \equiv (x_1 \oplus x_2 = 1)$$

выводим, что

$$SL = \mathrm{Pol}\{x_1 \oplus x_2 = 1,\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0\}.$$

Имеем далее

$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 1) \equiv$$
$$\equiv (\exists y)((x_4 \oplus y = 1)\ \&\ (x_1 \oplus x_2 \oplus x_3 \oplus y = 0)),$$
$$(x_1 \oplus x_2 = 1) \equiv (\exists x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_3 = 1),$$
$$(x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0) \equiv$$
$$\equiv (\exists y)((x_1 \oplus x_2 \oplus x_3 \oplus y = 1)\ \&\ (x_4 \oplus y = 1)).$$

Значит, класс SL можно задать предикатом

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 1.$$

Из равенства $SU = S \cap U$ вытекает, что

$$SU = \mathrm{Pol}\{x_1 \neq x_2,\ x_1 = x_2 \vee x_1 = x_3\}.$$

Эквивалентности

$$(x_1 \neq x_2 \vee x_1 \neq x_3) \equiv (\exists y)((x_1 \neq y)\ \&\ (y = x_2 \vee y = x_3)),$$
$$(x_1 \neq x_2) \equiv (x_1 \neq x_2 \vee x_1 \neq x_2),$$
$$(x_1 = x_2 \vee x_1 = x_3) \equiv (\exists y)((x_1 \neq y)\ \&\ (y \neq x_2 \vee y \neq x_3))$$

показывают, что класс SU можно определить предикатом $x_1 \neq$ $\neq x_2 \vee x_1 \neq x_3$.

Для любого m $(m \geqslant 2)$ имеем $MI^m = M \cap I^m$. Поэтому

$$MI^m = \mathrm{Pol}\{x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0\}.$$

Аналогично,

$$I_1^m = T_1 \cap I^m, \quad MI_1^m = M \cap I_1^m.$$

Следовательно,

$$I_1^m = \mathrm{Pol}\{x = 1,\ x_1 \cdot \ldots \cdot x_m = 0\},$$
$$MI_1^m = \mathrm{Pol}\{x = 1, x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0\}.$$

Наконец, поскольку

$$I^\infty = \bigcap_{m=2}^{\infty} I^m, \quad MI^\infty = \bigcap_{m=2}^{\infty} MI^m,$$
$$I_1^\infty = \bigcap_{m=2}^{\infty} I_1^m, \quad MI_1^\infty = \bigcap_{m=2}^{\infty} MI_1^m,$$

имеем

$$I^\infty = \mathrm{Pol}\{x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$
$$MI^\infty = \mathrm{Pol}\{x_1 \leqslant x_2,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$
$$I_1^\infty = \mathrm{Pol}\{x = 1,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$
$$MI_1^\infty = \mathrm{Pol}\{x = 1,\ x_1 \leqslant x_2,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\}.$$

Двойственным образом рассматриваются оставшиеся замкнутые классы MO^m, O_0^m, MO_0^m, O^∞, MO^∞, O_0^∞, MO_0^∞, отличные от классов C, C_0, C_1.

Основные результаты, полученные в этом параграфе, приведены в табл. 6.

Таблица 6

Класс	Предикаты, задающие класс
P_2	$x = x$
T_0	$x = 0$
T_1	$x = 1$
T_{01}	$x = 0,\ x = 1$
S	$x_1 \neq x_2$
M	$x_1 \leqslant x_2$
M_0	$x = 0,\ x_1 \leqslant x_2$
M_1	$x = 1,\ x_1 \leqslant x_2$
M_{01}	$x = 0,\ x = 1,\ x_1 \leqslant x_2$
S_{01}	$x = 0,\ x_1 \neq x_2$
SM	$x_1 \neq x_2,\ x_1 \leqslant x_2$
L_0	$x_1 \oplus x_2 \oplus x_3 = 0$
L_1	$x_1 \oplus x_2 \oplus x_3 = 1$
L_{01}	$x = 1,\ x_1 \oplus x_2 \oplus x_3 = 0$
U	$x_1 = x_2 \vee x_1 = x_3$
SU	$x_1 \neq x_2 \vee x_1 \neq x_3$
MU	$x_1 \leqslant x_2,\ x_1 = x_2 \vee x_1 = x_3$
U_0	$x = 0,\ x_1 = x_2 \vee x_1 = x_3$

Продолжение табл. 6

Класс	Предикаты, задающие класс
U_1	$x = 1,\ x_1 = x_2 \vee x_1 = x_3$
U_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \vee x_1 = x_3$
K	$x_1 = x_2 \cdot x_3$
K_0	$x = 0,\ x_1 = x_2 \cdot x_3$
K_1	$x = 1,\ x_1 = x_2 \cdot x_3$
K_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \cdot x_3$
D	$x_1 = x_2 \vee x_3$
D_0	$x = 0,\ x_1 = x_2 \vee x_3$
D_1	$x = 1,\ x_1 = x_2 \vee x_3$
D_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \vee x_3$
L	$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 0$
SL	$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = 1$
I^m	$x_1 \cdot \ldots \cdot x_m = 0$
MI^m	$x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0$
I_1^m	$x = 1,\ x_1 \cdot \ldots \cdot x_m = 0$
MI_1^m	$x = 1,\ x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0$
O^m	$x_1 \vee \ldots \vee x_m = 1$
MO^m	$x_1 \leqslant x_2,\ x_1 \vee \ldots \vee x_m = 1$
O_0^m	$x = 0,\ x_1 \vee \ldots \vee x_m = 1$
MO_0^m	$x = 0,\ x_1 \leqslant x_2,\ x_1 \vee \ldots \vee x_m = 1$

Комментарии. Отношение сохранения предиката функций введено А. В. Кузнецовым [9]. Соответствия Галуа между произвольными частично упорядоченными множествами и замыкания Галуа введены О. Оре [46] (см. также [27]). На возможность построения теории Галуа для алгебр Поста указывал А. В. Кузнецов [10]. Само построение выполнено независимо В. Г. Боднарчуком, Л. А. Калужниным, В. Н. Котовым, Б. А. Ромовым [4] и Д. Гейгером [42]. Все замкнутые классы булевых предикатов внешним образом охарактеризованы в [17]. Теорема 4.3 представляет собой булев вариант более общего утверждения, доказанного С. В. Яблонским [35]. Предикатное описание замкнутых классов булевых функций было известно А. В. Кузнецову (результат не опубликован). Первой публикацией на эту тему явилась статья [3].

Глава V

ОПЕРАТОРЫ ПАРАМЕТРИЧЕСКОГО И ПОЗИТИВНОГО ЗАМЫКАНИЯ

Наряду с операцией суперпозиции и соответствующим оператором замыкания в теории булевых функций рассматриваются более сильные операторы замыкания, которые приводят к конечным решеткам замкнутых классов. Наиболее интересными из них представляются операторы параметрического и позитивного замыкания. Они базируются на идее, значительно отличающейся от идеи формульного (термального) порождения булевых функций. По существу, используется идея определения графика функции через графики других функций с помощью некоторых логических формул. Близкие конструкции рассматривались нами в гл. IV при введении замкнутых классов булевых предикатов.

§ 1. Параметрическое замыкание

Определим язык параметрического замыкания Par. Исходными символами языка Par являются предметные переменные $x_1, x_2, \ldots$ (с областью значений E_2), символы $f_i^{(n)}$ для обозначения n-местных булевых функций $(1 \leqslant i \leqslant 2^{2^n}, n = 1, 2, \ldots)$, знак равенства $=$, логическая связка конъюнкция $\&$, квантор существования $\exists$, левая и правая скобки и запятая.

Обычным образом вводится понятия *терма* в языке Par. Любая предметная переменная есть терм; если $x_{j_1}, \ldots, x_{j_n}$ — предметные переменные (не обязательно различные), а $f_i^{(n)}$ — символ n-местной функции, то $f_i^{(n)}(x_{j_1}, \ldots, x_{j_n})$ есть терм; если $t_1, \ldots, t_m$ — термы, а $f_l^{(m)}$ — символ m-местной функции, то $f_l^{(m)}(t_1, \ldots, t_m)$ также есть терм.

Для удобства изложения наряду с исходными обозначениями будем использовать также обозначения вида x, y, z, $f^{(n)}$, $g^{(n)}$, $h^{(n)}$, возможно, с нижними индексами. В тех случаях, когда число переменных у функции определяется из контекста, верхний индекс у функции будем опускать.

Всякий терм t языка Par очевидным образом определяет некоторую булеву функцию g (переменная определяет тождественную

функцию). Если $f_1, \ldots, f_r$ — все символы функций, входящие в терм t, то говорим, что терм t выражает функцию g через функции $f_1, \ldots, f_r$. (В теории булевых функций термы обычно называют формулами; терм, составленный из символов функций $f_1, \ldots, f_r$, — формулой над множеством функций $\{f_1, \ldots, f_r\}$, а функцию, выразимую термом t через функции $f_1, \ldots, f_r$, — функцией, реализуемой формулой t над множеством функций $\{f_1, \ldots, f_r\}$.)

Если t_1, t_2 — термы языка Par, то выражение $(t_1 = t_2)$ называем *элементарной формулой*. Из элементарных формул по обычным логическим правилам определяем остальные формулы языка Par. Именно: если Φ_1, Φ_2 — формулы языка Par, а x_i — предметная переменная, то

$$(\Phi_1 \,\&\, \Phi_2), \quad (\exists x_i)\Phi_1$$

— также формулы языка Par. При образовании многочленных конъюнкций скобки в формулах будем опускать. Понятия свободной и связанной переменных предполагаем известными.

Всякая формула языка Par с m свободными переменными определяет некоторое m-местное отношение (предикат) на E_2. Пусть $Q \subseteq P_2$, $\Phi(x_1, \ldots, x_m)$ — формула языка Par со свободными переменными $x_1, \ldots, x_m$, все функциональные символы которой суть обозначения функций из Q, и формула $\Phi(x_1, \ldots, x_m)$ определяет отношение $\rho(x_1, \ldots, x_m)$ на E_2. В этом случае говорим, что формула $\Phi(x_1, \ldots, x_m)$ *параметрически выражает отношение* $\rho(x_1, \ldots, x_m)$ через функции множества Q. Отношение ρ называем *параметрически выразимым* через функции множества Q, если существует формула, которая параметрически выражает отношение ρ через функции множества Q.

Понятие параметрической выразимости перенесем с отношений на функции. Именно: если $g(x_1, \ldots, x_m)$ — булева функция, а формула $\Phi(x_1, \ldots, x_m, y)$ языка Par параметрически выражает отношение $g(x_1, \ldots, x_m) = y$ (*график* функции g) через функции множества Q, то говорим, что формула Φ *параметрически выражает функцию* g через функции множества Q. Совокупность всех функций, параметрически выразимых через функции множества Q, называем *параметрическим замыканием* множества Q и обозначаем $\mathrm{Par}[Q]$. Множества вида $\mathrm{Par}[Q]$ называем *параметрически замкнутыми классами*.

Установим некоторые свойства параметрического замыкания.

Утверждение 5.1. $\mathrm{Par}[\cdot]$ *является оператором замыкания на множестве* P_2. *Иными словами, для любых двух подмножеств* Q, R *множества* P_2 *выполняются следующие свойства*:

$$Q \subseteq \mathrm{Par}[Q]; \quad \text{если} \quad Q \subseteq R, \ \text{то} \quad \mathrm{Par}[Q] \subseteq \mathrm{Par}[R];$$
$$\mathrm{Par}[\mathrm{Par}[Q]] = \mathrm{Par}[Q].$$

Доказательство. При рассмотрении первого свойства достаточно заметить, что если f — символ n-местной функции из Q, то формула

$$y = f(x_1, \ldots, x_n) \tag{5.1}$$

параметрически выражает функцию f через функции множества Q. Второе свойство очевидно. При доказательстве третьего свойства следует учесть, что формулу Φ языка Par, выражающую некоторую функцию через функции множества $\mathrm{Par}[Q]$, можно превратить в формулу языка Par, выражающую ту же функцию через функции множества Q, если каждое отношение вида (5.1), где $f \in \mathrm{Par}[Q]$, заменить соответствующей формулой языка Par, которая выражает данное отношение через функции множества Q.

Утверждение 5.2. *Любой параметрически замкнутый класс содержит все селекторные функции.*

Доказательство. В самом деле, для селекторной функции e_i^n отношение $y = e_i^n(x_1, \ldots, x_n)$ параметрически выразимо формулой

$$(y = x_i) \,\&\, \left(\mathop{\&}_{1 \leqslant j \leqslant n} (x_j = x_j) \right).$$

Сомножители $x_j = x_j$ добавлены в эту формулу только для того, чтобы обозначить зависимость функции $e_i^n(x_1, \ldots, x_n)$ от всех переменных $x_1, \ldots, x_n$.

Утверждение 5.3. *Любой параметрически замкнутый класс замкнут относительно операции суперпозиции.*

Доказательство. Ввиду утверждения 5.2 рассмотрим только «регулярную» суперпозицию. Пусть функции $g_0, g_1, \ldots$ $\ldots, g_m$ принадлежат параметрически замкнутому классу Q и

$$g(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

Обозначим через

$$\Phi_0(x_1, \ldots, x_m, y), \ \Phi_1(x_1, \ldots, x_n, y), \ldots, \Phi_m(x_1, \ldots, x_n, y)$$

формулы языка Par_k, которые параметрически выражают отношения

$$y = g_0(x_1, \ldots, x_m),\ y = g_1(x_1, \ldots, x_n),\ \ldots,\ y = g_m(x_1, \ldots, x_n)$$

через функции множества Q. Тогда формула

$$(\exists y_1) \ldots (\exists y_m)(\Phi_1(x_1, \ldots, x_n, y_1)\ \&\ \ldots$$
$$\ldots\ \&\ \Phi_m(x_1, \ldots, x_n, y_m)\ \&\ \Phi_0(y_1, \ldots, y_m, z))$$

языка Par параметрически выражает отношение $z = g(x_1, \ldots, x_n)$ через функции класса Q. Таким образом, $g \in Q$. Утверждение доказано.

Утверждения 5.2, 5.3 показывают, что всякий параметрически замкнутый класс является клоном.

Утверждение 5.4 (принцип двойственности для параметрической выразимости). *Пусть формула* Φ *языка* Par *параметрически выражает функцию* $g(x_1, \ldots, x_n)$ *через функции* $g_1, \ldots, g_m$. *Тогда функция* g^* *параметрически выразима формулой* Φ^*, *которая получается из формулы* Φ *заменой всех символов функций* $g_1, \ldots, g_m$, *соответственно, символами двойственных функций* $g_1^*, \ldots, g_m^*$.

Доказательство. По определению двойственной функции справедлива эквивалентность

$$(y = g_i^*(x_1, \ldots, x_{n_i})) \equiv (\overline{y} = g_i(\overline{x}_1, \ldots, \overline{x}_{n_i})).$$

Далее индукцией по построению формулы Φ доказываем следующее утверждение: если подформула Φ_1 формулы Φ определяет отношение $\rho(z_1, \ldots, z_l)$, то соответствующая подформула Φ_1^* формулы Φ^* определяет отношение $\rho(\overline{z}_1, \ldots, \overline{z}_l)$. Базис индукции установлен выше. Переход от подформул Φ_1, Φ_2 к подформуле $\Phi_1\ \&\ \Phi_2$ не вызывает никаких затруднений. При рассмотрении подформул вида $(\exists z_1)\Phi_1$ следует воспользоваться эквивалентностью

$$(\exists z_1)\rho(z_1, \overline{z}_2, \ldots, \overline{z}_l) \equiv (\exists z_1)\rho(\overline{z}_1, \overline{z}_2, \ldots, \overline{z}_l).$$

Таким образом, формула Φ^* определяет отношение $\overline{y} = g(\overline{x}_1, \ldots, \overline{x}_n)$, т. е. отношение $y = g^*(x_1, \ldots, x_n)$. Утверждение доказано.

Если $Q \subseteq P_2$, то через Q^* обозначим множество всех булевых функций, двойственных к функциям из Q.

Следствие 1. *Если* $\mathrm{Par}[Q] = R$, *то* $\mathrm{Par}[Q^*] = R^*$.

Следствие 2. *Класс* S *параметрически замкнут.*

Утверждение 5.5. *Классы T_0, T_1 параметрически замкнуты.*

Доказательство. Пусть $g_1, \ldots, g_m \in T_0$ и функция g параметрически выразима формулой Φ через функции $g_1, \ldots, g_m$. Придадим всем свободным переменным формулы Φ значение 0. Нетрудно понять, что значение формулы Φ будет истинным. Чтобы убедиться в этом, достаточно взять в качестве общего значения всех связанных переменных формулы Φ значение 0 и воспользоваться тем, что все функции $g_1, \ldots, g_m$ сохраняют 0. Отсюда следует, что $g \in T_0$. Аналогично рассматривается класс T_1. Утверждение доказано.

Утверждение 5.6. *Класс L параметрически замкнут.*

Доказательство. Пусть формула $\Phi(x_1, \ldots, x_n, y)$ параметрически выражает функцию $f(x_1, \ldots, x_n)$ через функции класса L.

Предположим сначала, что формула Φ не содержит кванторов. Поскольку термы, составленные из линейных функций, реализуют линейные функции, можно считать, что формула Φ представляет собой конъюнкцию формул вида

$$g_1(z_1, \ldots, z_p) = g_2(w_1, \ldots, w_q), \tag{5.2}$$

где g_1, g_2 — линейные функции и $\{z_1, \ldots, z_p, w_1, \ldots, w_q\} \subseteq \{x_1, \ldots, x_n, y\}$. Перенося в формуле (4.2) слагаемые из правой части равенства в левую часть и проводя сокращения, получим эквивалентную формулу вида

$$g(z_1, \ldots, z_r) = 0, \tag{5.3}$$

где g — линейная функция и $\{z_1, \ldots, z_r\} \subseteq \{x_1, \ldots, x_n, y\}$. Можно предполагать, что функция g не равна тождественно нулю. Если функция $g(z_1, \ldots, z_r)$ не зависит существенно от переменной y, то формула Φ дает нетождественное линейное соотношение между независимыми переменными $x_1, \ldots, x_n$, что невозможно. Таким образом, далее будем предполагать, что в формуле (5.3) функция $g(z_1, \ldots, z_r)$ существенно зависит от переменной y. В силу этого формулу (5.3) можно переписать в эквивалентном виде

$$y = h(x_1, \ldots, x_n), \tag{5.4}$$

где h — линейная функция. Если из формулы Φ указанным выше способом можно получить формулу вида (5.4) с другой функцией h, то мы вновь придем к нетождественному линейному

соотношению между переменными $x_1, \ldots, x_n$. Значит, остается одна возможность, когда все формулы вида (5.4) имеют одну и ту же функцию h. В этом случае функция $f(x_1, \ldots, x_n)$, параметрически выразимая формулой $\Phi(x_1, \ldots, x_n, y)$, очевидно, совпадает с функцией $h(x_1, \ldots, x_n)$.

Покажем теперь, как можно элиминировать из формулы Φ кванторы $\exists$. Пусть область действия квантора $\exists z$ состоит из конъюнкции m формул вида (5.2), содержащих переменную z. Как и выше, преобразуем i-ю формулу (5.2) к эквивалентному виду

$$z = h_i(z_1^i, \ldots, z_{n_i}^i),$$

где h_i — линейная функция. Далее устраняем квантор $\exists z$ в соответствии со следующими эквивалентностями: при $m \geqslant 2$ формула

$$(\exists z)\left(\mathop{\&}_{1 \leqslant i \leqslant m}(z = h_i(z_1^i, \ldots, z_{n_i}^i))\right)$$

эквивалентна формуле

$$\mathop{\&}_{1 \leqslant i < j \leqslant m}(h_i(z_1^i, \ldots, z_{n_i}^i) + h_j(z_1^j, \ldots, z_{n_j}^j) = 0),$$

а при $m = 1$ тождественно истинна. Утверждение доказано.

Утверждение 5.7. *Классы D, K параметрически замкнуты.*

Доказательство. Ввиду двойственности классов D, K рассмотрим только класс D.

Предположим, что класс D не является параметрически замкнутым. Тогда классу $\mathrm{Par}[D]$ принадлежит отрицание. В самом деле, если в класс $\mathrm{Par}[D]$ входит немонотонная функция, то согласно лемме о немонотонной функции путем подстановки в немонотонную функцию констант 0,1 (которые содержатся в классе D) и тождественной функции можно получить отрицание. Если же в класс $\mathrm{Par}[D]$ входит монотонная функция, не принадлежащая классу D, то ее можно представить в виде ДНФ, которая не содержит отрицаний переменных и отлична от дизъюнкции. Выберем в ДНФ неодночленную конъюнкцию наименьшей длины и подставим в рассматриваемую функцию константу 0 вместо всех переменных, не входящих в выбранную конъюнкцию. В результате образуется функция, совпадающая с данной конъюнкцией. Параметрическая формула

$$(yx = 0)\ \&\ (y \vee x = 1)$$

выражает теперь отношение $y = \overline{x}$ через функции класса D и конъюнкцию.

Итак, если класс D не является параметрически замкнутым, то $\mathrm{Par}[D]$ совпадает с классом P_2. Следовательно, существует формула $\Phi(x, y)$, которая параметрически выражает функцию $\overline{x}$ через функции класса D.

Проведем некоторые упрощающие преобразования формулы Φ. Пользуясь тождествами $0 \vee z = z$ и $1 \vee z = 1$, исключим из формулы Φ вхождения констант 0 и 1, стоящих под знаком дизъюнкции. Далее, формула

$$z_1 \vee \ldots \vee z_p = 0 \tag{5.5}$$

эквивалентна формуле

$$(z_1 = 0)\ \&\ \ldots\ \&\ (z_p = 0). \tag{5.6}$$

Заменим поэтому в формуле Φ всякую подформулу вида (5.5) соответствующей формулой (5.6). Полученную после всех указанных преобразований формулу обозначим через $\Phi_1(x, y)$. Очевидно, что формула $\Phi_1(x, y)$ также параметрически выражает функцию $\overline{x}$ через функции класса D.

Пусть $v_1, \ldots, v_r$ — все связанные переменные формулы $\Phi_1(x, y)$. Из формулы Φ_1 можно исключить все подформулы вида $v_i = 0$ и $v_i = 1$ (а также соответствующие кванторы $\exists v_i$), заменив все остальные вхождения переменной v_i константой 0 или 1. Понятно, что в формулу Φ_1 не могут входить подформулы $x = 0$, $x = 1$, $y = 0$ или $y = 1$, поскольку в противном случае формула Φ_1 не может быть истинной, соответственно, при $x = 1$, $x = 0$, $y = 1$ или $y = 0$.

Таким образом, исключая из формулы $\Phi_1(x, y)$ все подформулы вида $v_i = 0$ и $v_i = 1$ с последующим исключением, если необходимо, констант 0 и 1 из-под знаков дизъюнкции, мы придем к формуле $\Phi_2(x, y)$, которая параметрически выражает функцию $\overline{x}$ через функции класса D и которая содержит в качестве элементарных подформул лишь формулы вида

$$0 = 0, \quad 1 = 1, \quad z_1 \vee \ldots \vee z_p = 1, \quad z_1 \vee \ldots \vee z_p = w_1 \vee \ldots \vee w_q, \tag{5.7}$$

где $\{z_1, \ldots, z_p, w_1, \ldots, w_q\} \subseteq \{x, y, v_1, \ldots, v_r\}$. Очевидно, что формулам (5.7) удовлетворяют значения $z_1 = \ldots = z_p = w_1 = \ldots = w_q = 1$. Но тогда значение $\Phi_2(1, 1)$ истинно, что противоречит параметрической выразимости отношения $y = \overline{x}$ формулой $\Phi_2(x, y)$.

Утверждение 5.8. *Класс U параметрически замкнут.*

Доказательство. Пусть формула $\Phi(x_1, \ldots, x_n, y)$ параметрически выражает функцию $f(x_1, \ldots, x_n)$ через функции

класса U. Предположим сначала, что формула Φ не содержит кванторов. Поскольку каждая функция класса U существенно зависит не более чем от одной переменной, формулу Φ можно представить в виде конъюнкции равенств, обе части которых суть элементы множества

$$\{0, 1, x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n, y, \overline{y}\}.$$

Очевидно, что формула Φ не может содержать противоречивых равенств. Она не может также содержать равенств вида

$$x_i = a, \quad x_i = x_j, \quad x_i = \overline{x}_j, \quad \overline{x}_i = \overline{x}_j,$$

где $i \neq j$, поскольку каждое из таких равенств налагает нетождественное условие на (независимые) переменные $x_1, \ldots, x_n$. Исключая далее из формулы Φ тождественно истинные равенства, приходим к выводу, что в формулу Φ обязана входить хотя бы одна из формул вида

$$y = a, \quad y = x_i, \quad y = \overline{x}_i.$$

Понятно, что одновременное вхождение двух различных формул этого вида приводит к противоречию. Оставшаяся возможность показывает, что функция $f(x_1, \ldots, x_n)$ существенно зависит не более чем от одной переменной.

Пусть теперь формула Φ содержит кванторы $\exists$. Поскольку функции класса U являются линейными, можно применить процедуру элиминирования кванторов, описанную в доказательстве утверждения 5.6. При этом следует иметь в виду, что формулы вида

$$g_i(z_1^i, \ldots, z_{n_i}^i) \oplus g_j(z_1^j, \ldots, z_{n_j}^j) = 0$$

редуцируются к формулам вида

$$z_p^i + z_q^j = a, \quad z_p^i = a, \quad z_q^j = a, \quad 0 = 0,$$

где $a \in \{0, 1\}$, $1 \leqslant p \leqslant n_i$, $1 \leqslant q \leqslant n_j$. Утверждение доказано.

Теорема 5.1. *Существует ровно* 25 *параметрически замкнутых классов булевых функций*:

$$P_2,\ T_0,\ T_1,\ T_{01},\ S,\ S_{01},\ L,\ L_0,\ L_1,\ SL,\ L_{01},\ D,\ D_0,$$
$$D_1,\ D_{01},\ K,\ K_0,\ K_1,\ K_{01},\ U,\ SU,\ MU,\ U_0,\ U_1,\ U_{01}. \quad (5.8)$$

Доказательство. Заметим, что все классы последовательности (5.8), отличные от класса P_2, параметрически замкнуты как пересечения некоторых из параметрически замкнутых классов T_0, T_1, S, L, D, K, U (класс MU есть пересечение классов D и K). Далее, из результатов гл. III будет следовать

1) все замкнутые (относительно операции суперпозиции) классы булевых функций, лежащие в классе L и целиком включающие класс U_{01} селекторных функций, суть $L, L_0, L_1, SL, L_{01}, U, MU, U_0, U_1, SU, U_{01}$;

2) все замкнутые классы булевых функций, лежащие в классе D и целиком включающие класс U_{01}, суть $D, D_0, D_1, D_{01}, U_0, U_1, U_{01}$;

3) все замкнутые классы булевых функций, лежащие в классе K и целиком включающие класс U_{01}, суть $K, K_0, K_1, K_{01}, U_0, U_1, U_{01}$;

4) все замкнутые классы булевых функций, целиком включающие класс S_{01}, суть $P_2, T_0, T_1, T_{01}, S, S_{01}$.

Таким образом, если имеется параметрически замкнутый класс Q, который не содержится в списке (5.8), то он должен не входить целиком ни в один из классов L, D, K и не содержать целиком класс S_{01}. Из результатов главы III следует, что при этих условиях в классе Q должен содержаться один из классов $MO_0^\infty, MI_1^\infty, SM$. Базисами (по суперпозиции) этих классов являются, соответственно, функции $x \vee yz, x(y \vee z), xy \vee xz \vee yz$. Однако функция $x \vee yz$ параметрически порождает функции xy и $x \vee y\overline{z}$. В самом деле, функция $x \vee y$ получается из функции $x \vee yz$ отождествлением переменных y, z. Далее имеем

$$(w = xy) \equiv (w \vee x = x) \,\&\, (w \vee y = y) \,\&\, (w \vee xy = w).$$

Отношение $w = x \vee y\overline{z}$ определяется теперь параметрической формулой

$$(wx = x) \,\&\, (w \vee y = x \vee y) \,\&\, (w \vee z = x \vee y \vee z) \,\&\, (wz = xz).$$

Поскольку базис по суперпозиции в классе T_{01} образуют функции $xy, x \vee y\overline{z}$, постольку в рассматриваемом случае класс Q целиком содержит класс T_{01}. Двойственным образом показываем, что при $x(y \vee z) \in Q$ выполняется соотношение $T_{01} \subseteq Q$.

Пусть в класс Q входит функция $xy \vee xz \vee yz$. Положим

$$g(x, y, z, w) = xy \vee x(xz \vee xw \vee zw) \vee y(xz \vee xw \vee zw).$$

Замечаем, что функция $\overline{x}y \vee \overline{x}z \vee yz$ параметрически выразима через функцию $xy \vee xz \vee yz$:

$$(w = \overline{x}y \vee \overline{x}z \vee yz) \equiv (y = xy \vee xw \vee yw) \,\&\, (z = xz \vee xw \vee zw) \,\&\, (w = g(w, x, y, z)).$$

Однако функция $\overline{x}y \vee \overline{x}z \vee yz$ образует базис по суперпозиции в классе S_{01}. Следовательно, в данном случае класс Q целиком содержит класс S_{01}. Теорема доказана.

Следствие (критерий параметрической полноты в классе P_2). *Система булевых функций параметрически полна в классе P_2 тогда и только тогда, когда она целиком не содержится ни в одном из параметрически замкнутых классов T_0, T_1, S, L, D, K.*

Диаграмма включений параметрически замкнутых классов приведена на рис. 3. С ее помощью (а также путем непосредственной проверки) можно определить параметрические базисы

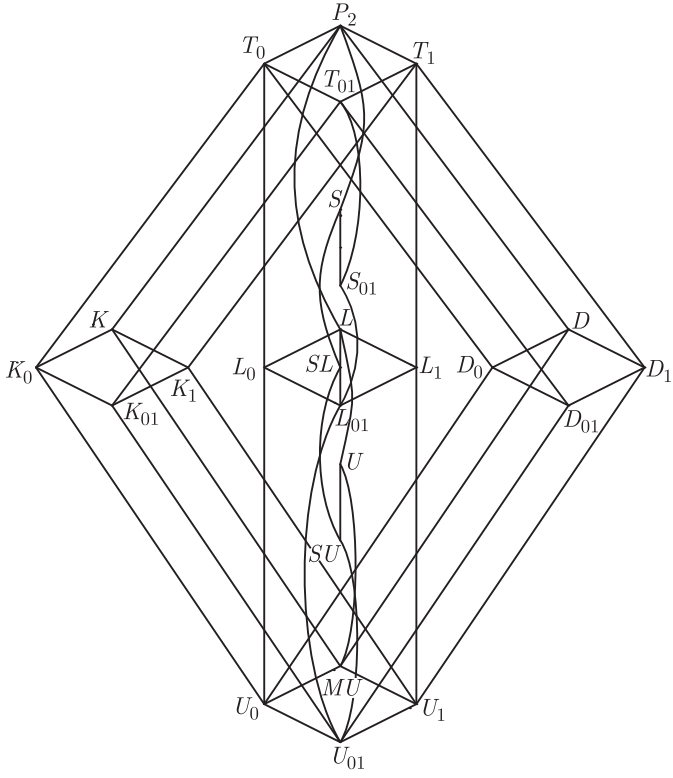


Рис. 3

во всех классах (5.8). Ниже мы выписываем лишь часть из этих параметрических базисов, которые отличаются от соответствующих базисов по суперпозиции:

$$P_2 = \mathrm{Par}[0, 1, x \vee y, xy], \quad T_0 = \mathrm{Par}[0, x \vee y, xy],$$
$$T_1 = \mathrm{Par}[1, x \vee y, xy], \quad T_{01} = \mathrm{Par}[x \vee y, xy], \quad MU = \mathrm{Par}[0, 1],$$
$$U_0 = \mathrm{Par}[0], \quad U_1 = \mathrm{Par}[1], \quad U_{01} = \mathrm{Par}[\varnothing].$$

§ 2. Централизаторы и бицентрализаторы

В этом параграфе мы хотим охарактеризовать параметрическое замыкание в духе сохранения некоторых инвариантов. Ключевым понятием здесь будет понятие перестановочности функций.

Говорят, что функции $f(x_1,\dots,x_m)$, $g(x_1,\dots,x_n)$ *перестановочны*, если имеет место тождество

$$f(g(x_{11},\dots,x_{1n}),\dots,g(x_{m1},\dots,x_{mn})) = \\ = g(f(x_{11},\dots,x_{m1}),\dots,f(x_{1n},\dots,x_{mn})).$$

Иными словами, функции f, g перестановочны, если для любой булевой $(m\times n)$-матрицы

$$\begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix}$$

значение функции f на столбце

$$\begin{pmatrix} g(x_{11},x_{12},\dots,x_{1n}) \\ g(x_{21},x_{22},\dots,x_{2n}) \\ \vdots \\ g(x_{m1},x_{m2},\dots,x_{mn}) \end{pmatrix}$$

совпадает со значением функции g на строке

$$(f(x_{11},x_{21},\dots,x_{m1}), f(x_{12},x_{22},\dots,x_{m2}),\dots \\ \dots, f(x_{1n},x_{2n},\dots,x_{mn})).$$

Отметим, что понятие перестановочности функций симметрично.

Пусть Q — произвольное множество булевых функций и f — функция из P_2. Говорят, что функция f *централизует* множество Q, если f перестановочна со всеми функциями из Q. Множество всех функций из P_2, централизующих Q, называют *централизатором* Q и обозначают через $\langle Q\rangle$. *Бицентрализатором* множества Q называют множество $\langle\langle Q\rangle\rangle$.

Из определений сразу вытекают следующие свойства централизатора и бицентрализатора:

$$\text{если } Q_1\subseteq Q_2, \text{ то } \langle Q_1\rangle\supseteq\langle Q_2\rangle$$

и, следовательно,

$$\langle\langle Q_1\rangle\rangle\subseteq\langle\langle Q_2\rangle\rangle;\quad Q\subseteq\langle\langle Q\rangle\rangle.$$

Можно также показать, что $\langle Q\rangle=\langle\langle\langle Q\rangle\rangle\rangle$.

Таким образом, оператор $\langle\langle\ \rangle\rangle$ есть оператор замыкания. На самом деле этот оператор совпадает с оператором параметрического замыкания. Однако существующие дедуктивно-логическое [11] и алгебраическое доказательства [42,51] этого факта несколько выходят за рамки настоящего издания.

Ниже мы установим некоторые простейшие свойства централизатора, а также покажем, что все параметрические классы (5.8) являются централизаторами тех же самых классов (5.8).

Утверждение 5.9. *Функции f, g перестановочны тогда и только тогда, когда функция g сохраняет график функции f — предикат*

$$f(x_1, \ldots, x_m) = y. \tag{5.9}$$

Доказательство. Пусть функции f, g перестановочны. Возьмем произвольные n наборов

$$(x_{11}, \ldots, x_{m1}, y_1), \ldots, (x_{1n}, \ldots, x_{mn}, y_n), \tag{5.10}$$

удовлетворяющие предикату (5.9). В силу перестановочности функций f, g будем иметь

$$f(g(x_{11}, \ldots, x_{1n}), \ldots, g(x_{m1}, \ldots, x_{mn})) = \\ = g(f(x_{11}, \ldots, x_{m1}), \ldots, f(x_{1n}, \ldots, x_{mn})) = g(y_1, \ldots, y_n). \tag{5.11}$$

Равенство (5.11) показывает, что применение функции g по строкам к матрице

$$\begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \ldots & \ldots & \ldots \\ x_{m1} & \ldots & x_{mn} \\ y_1 & \ldots & y_n \end{pmatrix},$$

столбцы которой удовлетворяют предикату (5.9), дает столбец, также удовлетворяющий предикату (5.9).

Обратно: пусть функция g сохраняет предикат (5.9). Возьмем произвольные n наборов (5.10), удовлетворяющие предикату (5.9). Тогда по условию сохранения предиката (5.9) функцией g набор

$$(g(x_{11}, \ldots, x_{1n}), \ldots, g(x_{m1}, \ldots, x_{mn}), g(y_1, \ldots, y_n))$$

будет также удовлетворять предикату (5.9). Это значит, что выполняется равенство

$$f(g(x_{11}, \ldots, x_{1n}), \ldots, g(x_{m1}, \ldots, x_{mn})) = g(y_1, \ldots, y_n)).$$

Заменяя в нем переменные $y_1, \ldots, y_n$ соответствующими значениями $f(x_{11}, \ldots, x_{m1}), \ldots, f(x_{1n}, \ldots, x_{mn})$, получим равенство,

которое определяет перестановочность функций f и g. Утверждение доказано.

Следствие 1. *Централизатор любого множества функций содержит все селекторные функции и замкнут относительно операции суперпозиции, т. е. является клоном.*

Следствие 2. *Пусть каждая из функций $f_1, \ldots, f_r$ перестановочна с функцией g и функция f является суперпозицией функций $f_1, \ldots, f_r$. Тогда функция f перестановочна с функцией g.*

Доказательство. Каждая из функций $f_1, \ldots, f_r$ сохраняет график функции g. Согласно результатам гл. IV функция f также будет сохранять график функции g, т. е. функция f будет перестановочна с функцией g.

Легко видеть, что $\langle U_{01} \rangle = P_2$ и $\langle P_2 \rangle = U_{01}$. В самом деле, графиками функций из класса U_{01} являются диагонали. Любая функция из P_2 сохраняет любую диагональ, т. е. перестановочна с любой функцией из U_{01}. Это доказывает первое из равенств. Для доказательства второго равенства следует заметить, что всякий предикат можно получить из графиков подходящих функций с помощью операций конъюнкции и проектирования. Используя результаты гл. IV, приходим к выводу, что функции из $\langle P_2 \rangle$ должны сохранять любой предикат. Это возможно только для селекторных функций.

Рассмотрим классы U_0 и T_0 и покажем, что каждый из них является централизатором другого. Напомним, что базисами (по суперпозиции) данных классов служат множества $\{0\}$ и $\{x \oplus y, xy\}$. Легко убедиться, что функция 0 перестановочна с каждой из функций $x \oplus y$, xy. Значит, в силу следствия 2 каждая из функций класса U_0 перестановочна с каждой из функций класса T_0. Иными словами, $T_0 \subseteq \langle U_0 \rangle$ и $U_0 \subseteq \langle T_0 \rangle$. Если бы равенство $T_0 = \langle U_0 \rangle$ не выполнялось, то ввиду предполноты класса T_0 и следствия 1 класс $\langle U_0 \rangle$ совпадал бы с P_2. Однако, очевидно, функция 1 не перестановочна с функцией 0. Значит, равенство $T_0 = \langle U_0 \rangle$ справедливо.

Предположим, что $U_0 \neq \langle T_0 \rangle$. Тогда в силу следствия 1 и результатов главы III класс $\langle T_0 \rangle$ содержит хотя бы одну из функций $x \vee y$, xy, $x \oplus y$, 1. Очевидно, что функций 1 не перестановочна с функций 0 из класса T_0. Далее, функция $x \oplus y$ не перестановочна с функциями $x \vee y$ и xy; чтобы установить это, достаточно рассмотреть (2×2)-матрицу со строками (01) и (10). Следовательно, если $(x \vee y) \in \langle T_0 \rangle$ либо $xy \in \langle T_0 \rangle$,

то необходимо (для проверки перестановочности) взять в классе T_0 функцию $x \oplus y$, а при $x \oplus y \in \langle T_0 \rangle$, например, функцию $x \vee y$. В результате полученного противоречия приходим к равенству $U_0 = \langle T_0 \rangle$.

Покажем, что каждый из классов SU и S является централизатором другого. В целом, доказательство аналогично доказательству для предыдущей пары классов. Напомним, во-первых, что $SU = [\overline{x}]$ и $S = [m(x, \overline{y}, \overline{z})]$. Проверяем, что функции $\overline{x}$ и $m(x, \overline{y}, \overline{z})$ перестановочны. Для этого следует взять (1×3)-матрицу (xyz) и получить тождество

$$\overline{m(x, \overline{y}, \overline{z})} = m(\overline{x}, y, z).$$

Таким образом, приходим к включениям $S \subseteq \langle SU \rangle$ и $SU \subseteq \langle S \rangle$. В случае выполнения неравенства $S \neq \langle SU \rangle$ ввиду предполноты S в P_2 должно быть $\langle SU \rangle = P_2$. Однако функция 0 очевидным образом не перестановочна с функций $\overline{x}$. В случае отличия класса $\langle S \rangle$ от класса SU в класс $\langle S \rangle$ должна входить (см., например, рис. 2) хотя бы одна из функций 0 или $x \oplus y \oplus z$. Функция 0 не перестановочна с функций $\overline{x}$ из класса S, а функция $x \oplus y \oplus z$ — с функцией $m(x, y, z)$. Для обоснования последнего утверждения достаточно рассмотреть (3×3)-матрицу, по строкам которой расположены наборы (001), (010), (100).

Перейдем к паре классов K_{01} и K. Легко проверяется, что конъюнкция xy, образующая базис класса K_{01}, перестановочна с функциями $0, 1, xy$, образующими базис класса K. Поэтому справедливы включения $K \subseteq \langle K_{01} \rangle$ и $K_{01} \subseteq \langle K \rangle$. Если $K \neq \langle K_{01} \rangle$, то (см. рис. 2) класс $\langle K_{01} \rangle$ содержит функцию $x \vee y$. Однако функции xy и $x \vee y$ не перестановочны — достаточно вновь рассмотреть (2×2)-матрицу, по строкам которой стоят наборы (01) и (10). Если же $K_{01} \neq \langle K \rangle$, то в класс $\langle K \rangle$ входит хотя бы одна из функций $0, 1, x(y \vee z)$. Однако функции 0 и 1 очевидным образом не перестановочны, а функция $x(y \vee z)$ не перестановочна с функций xy: здесь можно рассмотреть (2×3)-матрицу, по строкам которой расположены наборы (101) и (110).

Рассмотрим пару классов L_{01} и L. Проверяем, что функция $x \oplus y \oplus z$, образующая базис класса L_{01}, перестанановочна с функциями 1, $x \oplus y$, образующими базис класса L. Значит, $L \subseteq \langle L_{01} \rangle$ и $L_{01} \subseteq \langle L \rangle$. Класс L предполон в P_2. Поэтому при $L \neq \langle L_{01} \rangle$ класс $\langle L_{01} \rangle$ должен совпадать с P_2. Однако, как было установлено выше, функция xy не перестановочна с функцией $x \oplus y \oplus z$. Значит, на самом деле $L = \langle L_{01} \rangle$. Если $L_{01} \neq \langle L \rangle$, то класс $\langle L \rangle$ содержит хотя бы одну из функций $0, 1, \overline{x}, m(x, y, z)$. Линейная функция $\overline{x}$ не перестановочна

с функциями $0, 1$, а функция $x \oplus y$ — с функцией $m(x, y, z)$ (достаточно рассмотреть (2×3)-матрицу, по строкам которой расположены наборы (010) и (100)). Таким образом, приходим к равенству $L_{01} = \langle L \rangle$.

Рассмотрим классы MU и T_{01}. Легко проверить, что функции $0, 1, x$, образующие базис класса MU, перестановочны с функциями $xy, x \oplus y \oplus z$, образующими базис класса T_{01}. Поэтому $T_{01} \subseteq \langle MU \rangle$ и $MU \subseteq \langle T_{01} \rangle$. При $T_{01} \neq \langle MU \rangle$ класс $\langle MU \rangle$ содержит одну из констант 0 или 1. Поскольку функции $0, 1$ не перестановочны, приходим к равенству $T_{01} = \langle MU \rangle$. Далее, при $MU \neq \langle T_{01} \rangle$ класс $\langle T_{01} \rangle$ содержит хотя бы одну из функций $\overline{x}, x \vee y, xy$. Функция $x \vee y$ (из класса T_{01}) не перестановочна с функциями $\overline{x}, xy$, а функция xy (из класса T_{01}) с функцией $x \vee y$. Отсюда следует, что $MU = \langle T_{01} \rangle$.

Для пары классов $U = [0, \overline{x}]$ и $S_{01} = [m(x, y, \overline{z})]$ мы наметим лишь основные моменты доказательства. Функции $0, \overline{x}$ перестановочны с функцией $m(x, y, \overline{z})$; всякий замкнутый класс, строго содержащий класс S_{01}, включает в себя хотя бы одну из функций $\overline{x}, xy$; всякий замкнутый класс, строго содержащий класс U, включает функцию $x \oplus y$; функции из пар $0, \overline{x}$ и $\overline{x}, xy$ не перестановочны; функция $x \oplus y$ не перестановочна с функцией $m(x, y, z)$.

Оставшиеся параметрически замкнутые классы (не считая классов, двойственных к уже рассмотренным) обладают тем свойством, что централизатор класса совпадает с самим классом. Возьмем класс K_0. Легко видеть, что функции $0, xy$, образующие базис класса K_0, перестановочны и каждая из данных функций перестановочна сама с собой. Отсюда следует, что $K_0 \subseteq \langle K_0 \rangle$. Всякий замкнутый класс, строго содержащий класс K_0, включает в себя хотя бы одну из функций $1, x(y \vee z)$. Однако функция 1 не перестановочна с функцией 0, а функция $x(y \vee z)$ с функцией xy (последнее мы уже установили выше). Значит, $K_0 = \langle K_0 \rangle$.

Класс K_1 рассматривается аналогично классу K_0.

Рассмотрим класс L_0, базисом которого является функция $x \oplus y$. Очевидно, что функция $x \oplus y$ перестановочна с собой. Это дает включение $L_0 \subseteq \langle L_0 \rangle$. Класс L_0 непосредственно содержится (см. рис. 2) только в классах L и T_0. В эти классы входят функции 1 и xy, которые не перестановочны с функцией $x \oplus y$. Следовательно, приходим к равенству $L_0 = \langle L_0 \rangle$.

Остается рассмотреть класс $SL = [x \oplus y \oplus z \oplus 1]$. Проверяем, что функция $x \oplus y \oplus z \oplus 1$ перестановочна с собой. Далее,

класс SL непосредственно содержится только в классах L и S, которым принадлежат функции 1 и $m(x, y, z)$. Очевидно, что функции $x \oplus y \oplus z \oplus 1$ и 1 не перестановочны. Чтобы убедиться в неперестановочности функций $x \oplus y \oplus z \oplus 1$ и $m(x, y, z)$, следует рассмотреть, например, диагональную (3×3)-матрицу, по строкам которой расположены наборы (001), (010), (100). Таким образом, $SL = \langle SL \rangle$.

Классы D_0, D_1, L_1 двойственны классам K_0, K_1, L_0.

Обращаясь к рис. 3, можно заметить, что диаграмма включений параметрически замкнутых классов булевых функций имеет две «оси симметрии»: вертикальная ось соответствует переходу к двойственному классу, горизонтальная ось — переходу к централизатору.

§ 3. Позитивное замыкание

Язык Pos позитивного замыкания получается из языка Par параметрического замыкания добавлением логической связки дизъюнкции $\vee$. Понятие терма в языке Pos совпадает с понятием терма в языке Par. Понятие формулы в языке Pos расширяется новым пунктом: если Φ_1, Φ_2 — формулы языка Pos, то $(\Phi_1 \vee \Phi_2)$ — также формула языка Pos. По аналогии с языком Par на основе формул языка Pos вводим понятия *отношения*, *позитивно выразимого через функции множества* Q, *функции*, *позитивно выразимой через функции множества* Q, *позитивного замыкания множества* Q и *позитивно замкнутого класса*. Позитивное замыкание множества функций $Q \subseteq P_k$ обозначаем $\mathrm{Pos}[Q]$. Так же, как для параметрического замыкания, можно убедиться, что $\mathrm{Pos}[\ ]$ является оператором замыкания на множестве P_2.

Понятно, что всякий позитивно замкнутый класс является также параметрически замкнутым. Поэтому каждый позитивно замкнутый класс состоит, вообще говоря, из нескольких параметрически замкнутых классов. Отсюда и из утверждений 5.2, 5.3 вытекает следующее утверждение.

Утверждение 5.10. *Всякий позитивно замкнутый класс содержит все селекторные функции и замкнут относительно операции суперпозиции, т. е. является клоном.*

Практически без изменения переносится с параметрической выразимости на позитивную выразимость принцип двойственности.

Утверждение 5.11 (принцип двойственности для позитивной выразимости). *Пусть формула* Φ *языка* Pos *позитивно выражает функцию* g *через функции* $g_1, \ldots, g_m$. *Тогда функция* g^* *позитивно выразима формулой* Φ^*, *которая получается из формулы* Φ *заменой всех символов функций* $g_1, \ldots, g_m$, *соответственно, символами двойственных функций* $g_1^*, \ldots, g_m^*$.

Как следствие получаем, что класс S всех самодвойственных булевых функций является позитивно замкнутым. Так же, как в случае параметрического замыкания, устанавливаем, что позитивно замкнуты классы T_0 и T_1.

Утверждение 5.12. *Система* $\{0, 1\}$ *позитивно полна в классе* P_2.

Доказательство. Пусть $f(x_1, \ldots, x_n) \in P_2$. Позитивная формула

$$\bigvee_{(a_1,\ldots,a_n)\in E_2^n} (x_1 = a_1) \,\&\, \ldots \,\&\, (x_n = a_n) \,\&\, (y = f(a_1, \ldots, a_n))$$

определяет отношение $f(x_1, \ldots, x_n) = y$ через функции-константы 0, 1.

Теорема 5.2. *Существует ровно* 6 *позитивно замкнутых классов булевых функций*:

$$P_2, \quad T_0, \quad T_1, \quad S, \quad T_{01}, \quad S_{01}. \tag{5.12}$$

Доказательство. Заметим, что классы T_{01}, S_{01} позитивно замкнуты как пересечения позитивно замкнутых классов T_0, T_1, S. Далее, позитивная формула

$$(x = y) \,\&\, (w = z) \vee (x = z) \,\&\, (w = y) \vee (y = z) \,\&\, (w = y)$$

определяет отношение $w = \overline{x}y \vee \overline{x}z \vee yz$ (через пустое множество функций). Как установлено в гл. III, функция $\overline{x}y \vee \overline{x}z \vee yz$ образует базис по суперпозиции в классе S_{01}. Следовательно, всякий позитивно замкнутый класс булевых функций содержит класс S_{01}. Вместе с тем все замкнутые (относительно операции суперпозиции) классы булевых функций, содержащие класс S_{01}, исчерпываются классами (5.12). Таким образом, не существует позитивно замкнутых классов булевых функций, отличных от классов (5.12). Теорема доказана.

Следствие (критерий позитивной полноты в классе P_2). *Система булевых функций позитивно полна в классе* P_2 *тогда и только тогда, когда она целиком не содержится ни в одном из классов* T_0, T_1, S.

Укажем позитивные базисы в классах (5.12). В силу утверждения 5.12 (а также теоремы 5.2) позитивный базис в классе P_2 образуют функции-константы $0, 1$. По теореме 5.2 позитивные базисы в классах T_0, T_1, S будут состоять, соответственно, из функций $0, 1, \overline{x}$. Позитивный базис класса T_{01} образует, например, любая из функций $x \vee y, xy$. Чтобы в этом убедиться, достаточно заметить, что класс T_{01} собственно содержит только один позитивно замкнутый класс — класс S_{01}. Поскольку ни одна из функций $x \vee y, xy$ не входит в класс S_{01}, приходим к заключению, что каждая из этих функций позитивно порождает класс T_{01}. Наконец, позитивным базисом класса S_{01} может считаться пустое множество, поскольку функция $\overline{x}y \vee \overline{x}z \vee yz$ позитивно определяется через пустое множество функций.

Позитивно замкнутые классы — это часть параметрически замкнутых классов. Поэтому для них также справедливы представления с использованием централизаторов и бицентрализаторов. В частности, централизаторами позитивно замкнутых классов (5.12) являются, соответственно, классы

$$U_{01}, \quad U_0, \quad U_1, \quad SU, \quad MU, \quad U. \tag{5.13}$$

Каждая функция из классов (5.13) зависит существенно не более чем от одной переменной. Поскольку несущественные переменные здесь не играют роли, далее рассматриваем только одноместные функции из классов (5.13). В этом случае каждый из классов (5.13) можно рассматривать как полугруппу с операцией композиции (суперпозиции) и единицей — тождественной функцией x. Кроме того, из определения централизатора следует, что если Q — один из классов (5.13), $f(x_1, \ldots, x_n) \in Q$ и $g(x) \in \langle Q \rangle$, то справедливо тождество

$$f(g(x_1), \ldots, g(x_n)) = g(f(x_1, \ldots, x_n)).$$

Это тождество показывает, что g есть *эндоморфизм* функции f (точнее говоря, g есть эндоморфизм алгебры с носителем E_2 и единственной операцией f). Таким образом, каждый из классов (5.12) можно определить полугруппой эндоморфизмов. Перечислим эти полугруппы в порядке следования классов (5.13):

$$\{x\}, \quad \{0, x\}, \quad \{1, x\}, \quad \{x, \overline{x}\}, \quad \{0, 1, x\}, \quad \{0, 1, x, \overline{x}\}.$$

Комментарии. Определение параметрической выразимости и список всех параметрически замкнутых классов булевых функций были изложены А. В. Кузнецовым в 1967 г. на VIII Всесоюзном коллоквиуме по общей алгебре в Риге (доклад не публиковался). Позже это вошло в виде небольшой

части в обзорную статью [11]. Однако несколько ранее А. Ф. Данильченко [7] сформулировала в иной форме основные результаты А. В. Кузнецова. Дальнейшее развитие и обобщение идей А. В. Кузнецова по параметрической выразимости имеется в работах [52, 53]. Впервые перечисление всех параметрически замкнутых классов булевых функций с подробными доказательствами приведено в книге [19]. Доказательства, использующие понятие централизатора, даны в статье [43]. На возможность введения понятия позитивной выразимости указано А. В. Кузнецовым в статье [11] (в терминах А. В. Кузнецова — экзистенциальная выразимость). Понятие позитивной выразимости и позитивного замыкания введены в работе [18].

Глава VI

ЧАСТИЧНЫЕ БУЛЕВЫ ФУНКЦИИ

Понятие частичной булевой функции естественно возникает в ситуациях, когда значения булевой функции $f(x_1, \ldots, x_n)$ известны не на всем множестве E_2^n, а только на некотором его собственном подмножестве E, и отсутствует информация о возможном поведении функции f на множестве $E_2^n \setminus E$. Удобно считать, что в случае, когда функция f не определена на наборе $(a_1, \ldots, a_n)$, она «принимает» значение «неопределенность». Для обозначения неопределенности будем использовать символ $*$. Таким образом, тот факт, что функция f не определена на наборе $(a_1, \ldots, a_n)$, будем записывать в виде $f(a_1, \ldots, a_n) = *$.

Итак, под *частичной булевой функцией* будем понимать функцию, аргументы которой принимают значения из множества E_2, а сама функция — значения из множества $E_2 \cup \{*\}$.

Множество всех частичных булевых функций обозначим через P_2^*. Отметим, что при любом $n \geqslant 1$ множеству P_2^* принадлежит n-местная *нигде не определенная функция* — функция, которая принимает значение $*$ на всем множестве E_2^n. Все такие функции будем также обозначать символом $*$.

По аналогии с обычными булевыми функциями для частичных булевых функций можно ввести понятия существенной и фиктивной переменных. Мы дадим определение только фиктивной переменной. Будем говорить, что частичная булева функция $g(x_1, \ldots, x_n, x_{n+1})$ получена из частичной булевой функции функции $f(x_1, \ldots, x_n)$ с помощью *введения фиктивной переменной* x_{n+1}, если для любых значений переменных $x_1, \ldots, x_n, x_{n+1}$ справедливо равенство

$$g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n).$$

Отметим, что данное равенство понимается абсолютно: как обычное отношение равенства на трехэлементном множестве $\{0, 1, *\}$.

Определение операции суперпозиции на множестве частичных булевых функций можно дать различными способами. Мы остановимся на следующем наиболее распространенном способе. Чтобы не отягощать определение мелкими техническими деталями, рассмотрим лишь «регулярную» суперпозицию вида

$$f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

Считаем, что функция, задаваемая данной суперпозицией, определена на наборе $(a_1, \ldots, a_n)$ в том и только том случае, когда на наборе $(a_1, \ldots, a_n)$ определены все функции $f_1, \ldots, f_m$, а на наборе

$$(f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n))$$

— функция f_0.

Как и для обычных булевых функций, для частичных булевых функций на основе понятий формулы и функции, реализуемой формулой, можно ввести понятия замыкания, замкнутого класса, полноты, порождающей системы и базиса.

Положим

$$e(x, y) = \begin{cases} x, & \text{если } x = y, \\ * & \text{в противном случае.} \end{cases}$$

Теорема 6.1. *Система функций* $\{\overline{x}, x \vee y, e(x, y)\}$ *полна в классе* P_2^*.

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из P_2^*. Суперпозициями функций $\overline{x}, x \vee y$ определим такие (всюду определенные) функции $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n)$, что для любого набора $(a_1, \ldots, a_n)$ из E_2^n

$$f_1(a_1, \ldots, a_n) = f_2(a_1, \ldots, a_n) = f(a_1, \ldots, a_n),$$

если значение $f(a_1, \ldots, a_n)$ определено, и $f_1(a_1, \ldots, a_n) \neq \neq f_2(a_1, \ldots, a_n)$ — в противном случае. Тогда будем иметь

$$f(x_1, \ldots, x_n) = e(f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n)).$$

Теорема доказана.

Следствие. *Пусть* $g(x)$ *— функция из* P_2^*, *которая определена только в одной точке. Тогда система* $\{\overline{x}, x \vee y, g(x)\}$ *полна в классе* P_2^*.

Доказательство. Легко видеть, что одна из функций

$$g(x), \quad g(\overline{x}), \quad \overline{g}(x), \quad \overline{g}(\overline{x})$$

совпадает с функцией $h(x)$, где $h(0) = 0$ и $h(1) = *$. Далее получаем

$$e(x, y) = x \vee h(x \oplus y).$$

Следствие доказано.

Наша следующая цель — сформулировать для класса P_2^* критерий функциональной полноты. Для этого определим в P_2^* следующие 8 классов:

$P_2 \cup \{*\}$;

$T_0^* = \{f\colon f$ можно доопределить до функции из $T_0\}$;

$T_1^* = \{f\colon f$ можно доопределить до функции из $T_1\}$;

$S^* = \{f\colon f$ можно доопределить до функции из $S\}$;

$M^* = \{f\colon f$ можно доопределить до функции из $M\}$;

$L^* = \{f\colon$ при подстановке в функцию f на места всех переменных любых функций из множества $\{0, 1, x, \overline{x}, y, \overline{y}, x \oplus y, x \oplus y \oplus 1\}$ получается либо функция из этого множества, либо не всюду определенная функция$\}$;

$T_{01}^* = \{f\colon$ или $f(0, \ldots, 0) = 0$ и $f(1, \ldots, 1) = 1$ либо $f(0, \ldots, 0) = *$, либо $f(1, \ldots, 1) = *\}$;

$U^* = \{f\colon$ при подстановке в функцию f на места всех переменных любых функций из множества $\{0, 1, x, \overline{x}, y, \overline{y}\}$ получается либо функция из этого множества, либо не всюду определенная функция$\}$.

Исходя непосредственно из определения суперпозиции нетрудно доказать замкнутость всех классов

$$P_2 \cup \{*\}, \quad T_0^*, \quad T_1^*, \quad S^*, \quad M^*, \quad L^*, \quad T_{01}^*, \quad U^*. \qquad (6.1)$$

Отметим, что имеют место строгие включения

$$T_0 \subset T_0^*, \quad T_1 \subset T_1^*, \quad S \subset S^*, \quad M \subset M^*,$$
$$L \subset L^*, \quad T_{01} \subset T_{01}^*, \quad U \subset U^*.$$

Можно показать также, что ни один из классов (6.1) целиком не содержится в другом. Выделим здесь только два случая: функция $g(x, y, z)$ из класса $S^* \cap U^*$, которая определена лишь на четырех наборах,

$$g(0, 0, 0) = g(0, 1, 1) = g(1, 0, 1) = 0, \quad g(1, 1, 0) = 1,$$

не принадлежит классу L^*.

Теорема 6.2 (критерий функциональной полноты в классе P_2^*). *Система частичных булевых функций полна в классе P_2^* тогда и только тогда, когда она целиком не содержится ни в одном из классов* (6.1).

Доказательство. Необходимость условия теоремы следует из замкнутости классов (6.1) и несовпадении их с классом P_2^*. Установим достаточность условия теоремы.

Пусть система функций из P_2^* целиком не содержится ни в одном из классов (6.1). Выберем в ней функции $f_1, \ldots, f_8$,

которые не принадлежат, соответственно, классам $P_2 \cup \{*\}, \ldots$ $\ldots, U^*$. Докажем, что система функций $\{f_1, \ldots, f_8\}$ полна в классе P_2^*.

Сначала с помощью функций f_2, f_3, f_4, f_7 получим константы. Очевидно, что функция $f_7(x, \ldots, x)$ (не входящая в класс T_{01}^*) совпадает с одной из функций $0, 1, \overline{x}$. Поскольку $f_2(0, \ldots, 0) = 1$ и $f_3(1, \ldots, 1) = 0$, в первых двух случаях из одной константы с помощью функций f_2 или f_3 образуем другую константу. В третьем случае рассмотрим функцию $f_4(x_1, \ldots, x_m)$ (не входящую в класс S^*), которая, очевидно, обладает следующим свойством: существует такой набор $(a_1, \ldots, a_m) \in E_2^m$, что

$$f_4(a_1, \ldots, a_m) = f_4(\overline{a}_1, \ldots, \overline{a}_m) \neq *.$$

Из него следует, что функция $f_4(x \oplus a_1, \ldots, x \oplus a_m)$ будет константой. Другую константу, как и выше, получаем с помощью функций f_2, f_3.

Далее построим функцию $\overline{x}$. Из условия $f_5(x_1, \ldots, x_n) \notin M^*$ вытекает, что найдутся такие два набора $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$, что

$$(a_1, \ldots, a_n) \leqslant (b_1, \ldots, b_n)$$

и

$$f_5(a_1, \ldots, a_n) = 1, \ f_5(b_1, \ldots, b_n) = 0.$$

Как и в лемме о немонотонной функции, заменим в функции $f_5(x_1, \ldots, x_n)$ переменную x_i $(1 \leqslant i \leqslant n)$ константой a_i, если $a_i = b_i$, и переменной x, если $a_i \neq b_i$ (в этом случае непременно $a_i = 0$ и $b_i = 1$). В результате этой замены образуется функция $\overline{x}$.

Перейдем к функции $f_8(x_1, \ldots, x_k)$ (она не входит в класс U^*). Согласно определению класса U^* существуют такие функции $g_1(x, y), \ldots, g_k(x, y)$ из множества $\{0, 1, x, \overline{x}, y, \overline{y}\}$, что функция

$$g(x, y) = f_8(g_1(x, y), \ldots, g_k(x, y))$$

не входит в множество $\{0, 1, x, \overline{x}, y, \overline{y}\}$. Если функция $g(x, y)$ нелинейна (а все нелинейные функции от переменных x, y суть

$$x \vee y, \ x \vee \overline{y}, \ \overline{x} \vee y, \ \overline{x} \vee \overline{y}, \ xy, \ x\overline{y}, \ \overline{x}y, \ \overline{xy}),$$

то вместе с функцией $\overline{x}$ она образует полную в P_2 систему.

Пусть функция $g(x, y)$ линейна (т. е. $g(x, y) \in \{x \oplus y,$ $x \oplus y \oplus 1\}$). Поскольку функция $\overline{x}$ уже построена, можно считать, что в этом случае имеются обе функции $x \oplus y$ и $x \oplus y \oplus 1$. Теперь рассматриваем функцию f_6 (не входящую в класс L^*) и так же, как для функции f_8, подстановкой

в функцию f_6 на места всех переменных подходящих функций из множества $\{0, 1, x, \overline{x}, y, \overline{y}, x \oplus y, x \oplus y \oplus 1\}$ получаем нелинейную функцию от двух переменных. В результате вновь приходим к полной в P_2 системе.

Рассмотрим, наконец, функцию f_1. Очевидно, что можно найти такую пару соседних (отличающихся только в одной координате) наборов $\widetilde{a}$ и $\widetilde{b}$, что функция f_1 определена только на одном из этих наборов. Подставим в функцию f_1 константы 0,1 вместо всех тех переменных, которым в наборах $\widetilde{a}, \widetilde{b}$ отвечают равные значения, и переменную x вместо единственной оставшейся переменной. Получим функцию $g_1(x)$, которая определена только в одной точке. Далее применяем следствие из теоремы 6.1. Теорема доказана.

Следующая теорема показывает, что с точки зрения функциональной выразимости случай частичных булевых функций кардинально отличается от случая обычных булевых функций.

Теорема 6.3. *В P_2^* имеется континуальное число различных замкнутых классов.*

Доказательство. Определим последовательность $\{f_i(x_1, \ldots, x_i);\ i = 2, 3, \ldots\}$ функций из P_2^*: для любого набора $(a_1, \ldots, a_i)$ из E_2^i пусть

$$f_i(a_1, \ldots, a_i) = \begin{cases} 0, & \text{если набор } (a_1, \ldots, a_i) \text{ содержит ровно} \\ & \text{одну единицу,} \\ * & \text{в остальных случаях.} \end{cases}$$

Покажем, что никакая функция f_i не выражается формулой над множеством функций $\{f_2, \ldots, f_{i-1}, f_{i+1}, \ldots\}$. В силу стандартных рассуждений отсюда будет следовать требуемое в теореме утверждение.

Доказательство будет от противного. Предположим, что Φ — формула над множеством функций $\{f_2, \ldots, f_{i-1}, f_{i+1}, \ldots, \}$, которая реализует функцию f_i. В формулу Φ непременно входит подформула вида $f_j(x_{k_1}, \ldots, x_{k_j})$, где

$$\{k_1, \ldots, k_j\} \subseteq \{1, 2, \ldots, i\} \quad \text{и} \quad j \neq i.$$

Если $j < i$, то рассмотрим набор $(a_1, \ldots, a_i)$, который содержит ровно одну единицу и в котором $a_{k_1} = \ldots = a_{k_j} = 0$. Функция $f_j(x_{k_1}, \ldots, x_{k_j})$ не определена на этом наборе. Значит, (согласно определению суперпозиции частичных булевых функций) на данном наборе будет не определена и вся функция, реализуемая формулой Φ. Получили противоречие.

Допустим, что $j > i$. Тогда среди чисел $k_1, \ldots, k_j$ есть хотя бы два одинаковых. Пусть например, $k_1 = k_2$. Рассмотрим набор $(a_1, \ldots, a_i)$, в котором равна 1 только компонента a_{k_1}. Тогда значение функции $f_j(x_{k_1}, \ldots, x_{k_j})$ на наборе $(a_1, \ldots, a_i)$ не определено и, как и выше, получаем противоречие. Теорема доказана.

Комментарии. Критерий функциональной полноты в классе P_2^* установлен Р. В. Фрейвалдом [32, 33]. Континуальность числа замкнутых классов в P_2^* следует из работы [2]. Доказательство теоремы 6.3 взято из [21].

Глава VII

РЕАЛИЗАЦИЯ БУЛЕВЫХ ФУНКЦИЙ СХЕМАМИ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

Универсальные способы представления булевых функций в виде (совершенной) ДНФ, (совершенной) КНФ или полинома Жегалкина обладают одной особенностью, на которую поначалу можно и не обратить внимание. Дело в том, что при построении формул данных типов, а это построение необходимо выполнять последовательно, отправляясь от символов переменных и используя на промежуточных этапах уже построенные части формул, любая подформула, образованная в процессе построения, используется далее только один раз. Однако понятно, что можно отказаться от этого ограничения и получить в результате определенный выигрыш в сложности получаемых формул (в нашем случае — по числу символов переменных и числу символов базисных функций). В практической реализации этого подхода приходится отказываться от привычного понятия формулы, которым мы пользовались ранее. Здесь, скорее, более уместным представляется термин «схема», тем более что реальные схемы (например, в микроэлектронике) действительно напоминают те схемы, которые будут определены в дальнейшем.

§ 1. Системы булевых уравнений и схемы из функциональных элементов

Мы начнем со «схем», которые все же сохраняют основные черты формул. Будем рассматривать системы булевых уравнений специального вида. Для простоты ограничимся уравнениями в «базисе» $B = \{-, \vee, \&\}$ (система функций B не является базисом согласно приведенному ранее определению, однако в данной области исследований множество B традиционно называется базисом). Система уравнений Σ в базисе B имеет *входные переменные* $x_1, \ldots, x_n$, *рабочие переменные* $y_1, \ldots, y_m$ и состоит из m уравнений, левые части которых суть переменные $y_1, \ldots, y_m$. Уравнение с номером i системы Σ может быть одного из следующих трех типов:

$$y_i = \overline{z}_j, \quad y_i = z_j \vee z_l, \quad y_i = z_j \,\&\, z_l,$$

где переменные z_j, z_l принадлежат множеству $\{x_1, \ldots, x_n, y_1, \ldots, y_{i-1}\}$. Среди переменных множества $\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$ выделяются некоторые переменные, которые называются *выходными переменными* системы Σ.

Легко видеть, что для любых значений входных переменных $x_1, \ldots, x_n$ системы Σ существует единственный набор значений переменных $y_1, \ldots, y_m$, удовлетворяющий данной системе уравнений. Таким образом, каждой переменной y_i системы Σ можно сопоставить булеву функцию $f_i(x_1, \ldots, x_n)$, которая рекуррентно вычисляется согласно системе уравнений Σ с использованием только рабочих переменных $y_1, \ldots, y_{i-1}$. Допуская некоторую вольность речи, будем говорить, что переменная y_i *реализует функцию* f_i.

В качестве примера рассмотрим систему уравнений

$$y_1 = x_1 \,\&\, x_2, \quad y_2 = x_1 \vee x_2, \quad y_3 = \overline{y}_1, \quad y_4 = y_2 \,\&\, y_3.$$

В ней переменные $y_1, \ldots, y_4$ реализуют, соответственно, функции

$$x_1 \,\&\, x_2, \quad x_1 \vee x_2, \quad \overline{x_1 \,\&\, x_2}, \quad \overline{(x_1 \,\&\, x_2)} \,\&\, (x_1 \vee x_2).$$

Нетрудно видеть, что переменная y_4 реализует функцию $x_1 \oplus x_2$.

Под сложностью системы булевых уравнений обычно понимают число уравнений, составляющих данную систему.

В общем случае системы булевых уравнений строятся для реализации нескольких булевых функций. Однако если мы хотим построить систему уравнений для реализации только одной булевой функции, то в качестве выходной переменной системы естественно рассматривать последнюю из рабочих переменных.

Несмотря на достаточную логическую простоту систем булевых уравнений, существенно большее распространение получили другие схемы для реализации булевых функций — схемы из функциональных элементов (СФЭ). Мы будем рассматривать СФЭ только в базисе B. В определении СФЭ используются некоторые простые понятия из теории графов.

Начнем с ориентированных ациклических (т. е. не имеющих ориентированных циклов, в том числе петель) графов. Пусть G — конечный граф этого типа. Предполагаем, что в каждую вершину графа G входит не более двух дуг (это ограничение в нашем определении существенно и сязано с выбором базиса B). Нетрудно видеть, что в силу ацикличности графа G в нем обязательно найдутся вершины, в которые не входят никакие дуги. Назовем такие вершины *истоками* графа G.

Схемой из функциональных элементов (в базисе B) будем называть конечный ориентированный ациклический граф, который удовлетворяет следующим дополнительным условиям.

1) Каждому истоку графа приписана некоторая переменная, причем разным истокам графа — различные переменные; истоки графа называются *входами схемы*, а приписанные им переменные — *входными переменными схемы*.

2) Каждой вершине графа, в которую входит ровно одна дуга, приписана булева функция отрицание; каждой вершине графа, в которую входят ровно две дуги, приписана либо функция дизъюнкция, либо функция конъюнкция; вершина с приписанной ей булевой функцией называется *функциональным элементом*.

3) В графе выделены некоторые вершины, называемые *выходами схемы* (истоки могут одновременно являться выходами схемы).

Функциональные элементы, отвечающие функциям $-, \vee, \&$, называются, соответственно, *инвертором*, *дизъюнктором* и *конъюнктором*.

Отправляясь от входов схемы и продвигаясь по дугам «вглубь» схемы, нетрудно убедиться, что каждой вершине СФЭ можно однозначным образом приписать некоторую булеву функцию от входных переменных схемы — функцию, реализуемую на «выходе» функционального элемента, приписанного рассматриваемой вершине схемы. На входах схемы реализуются (селекторные) функции, совпадающие со значениями переменной, приписанной данной вершине схемы. Таким образом, на выходах СФЭ реализуется система булевых функций, о которой говорят, что она *реализуема* данной СФЭ.

Под *сложнстью* СФЭ Σ будем понимать общее число функциональных элементов, составляющих схему Σ. Сложность схемы Σ обозначается через $L(\Sigma)$. На рис. 4 изображена СФЭ с входными переменными x_1, x_2, которая реализует (помимо других функций) функцию $x_1 \oplus x_2$. (Здесь и далее мы не указываем стрелки на дугах, предполагая, что они всегда задают направление «сверху вниз».)

Можно заметить, что между системами булевых уравнений и схемами из функциональных переменных существует легко обнаружимая связь. Именно: пусть Σ_1 — система уравнений (в базисе B) с входными переменными $x_1, \ldots, x_n$ и рабочими переменными $y_1, \ldots, y_m$. Сопоставим ей СФЭ Σ_2 с входными переменными $x_1, \ldots, x_n$ и m функциональными элементами. Соответствующий схеме Σ_2 ориентированный ациклический граф G имеет $n + m$ вершин; в вершины графа G,

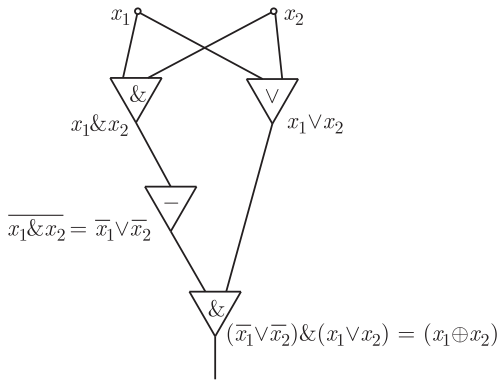


Рис. 4

отвечающие входным переменным $x_1, \ldots, x_n$, не входят никакие дуги. Напротив, если в системе Σ_1 переменная y_i связана (посредством функций $-, \vee, \&$) с переменной z_j либо переменными z_j, z_l, то в вершину v_i графа G, соответствующую переменной y_i, входит либо одна одна дуга, либо две дуги, которые отвечают переменным z_j либо переменным z_j, z_l (напомним, что $z_j, z_l \in \{x_1, \ldots, x_n, y_1, \ldots, y_{i-1}\}$). Понятно, что булева функция, реализуемая на выходе функционального элемента, приписанного в схеме Σ_2 вершине v_i, совпадает с булевой функцией, реализуемой в системе Σ_1 переменной y_i.

Обратно: пусть имеется СФЭ Σ_2 со входами $x_1, \ldots, x_n$ и m функциональными элементами. Ее можно «изобразить» в виде системы булевых уравнений Σ_1, если предварительно занумеровать в схеме Σ_2 все вершины, отличные от входов, числами от 1 до m. При этом должно соблюдаться одно условие: если в схеме Σ_2 в вершину с номером i ведут дуги (дуга) из вершин v, w (вершины v), то каждая из вершин v, w либо является входом, либо имеет номер, меньший i. Нетрудно понять, что ориентированность и ацикличность графа схемы Σ_2 позволяют выполнить такую нумерацию.

Отметим, что схема Σ_2 и система уравнений Σ_1 в приведенных преобразованиях имеют одинаковую сложность.

Пусть f — булева функция. *Сложностью функции* f (обозначение $L(f)$) называется сложность минимальной (по числу функциональных элементов) СФЭ, которая реализует функцию f. *Функцией Шеннона* $L(n)$ называется функция $\max L(f)$, где максимум берется по всем функциям f от n переменных. Таким образом, любую булеву функцию от n переменных можно реализовать СФЭ со сложностью, не превосходящей $L(n)$.

§ 2. Предварительные оценки функции Шеннона

Сначала рассмотрим реализацию булевых функций в виде совершенной ДНФ и верхние оценки функции $L(n)$, вытекающие из этого способа представления булевых функций. Пусть $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_n)$ — булев набор размерности n и $K_{\widetilde{\sigma}} = x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$ — конъюнкция, отвечающая набору $\widetilde{\sigma}$. СФЭ, реализующую конъюнкцию $K_{\widetilde{\sigma}}$, можно получить, используя не более n инверторов (для реализации функций $x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}$) и ровно $n-1$ конъюнкторов, «собирающих» функции $x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}$. Поэтому

$$L(K_{\widetilde{\sigma}}) \leqslant 2n - 1. \tag{7.1}$$

Пусть теперь $f(x_1, \ldots, x_n)$ — произвольная функция от n переменных и $K_1 \vee \ldots \vee K_m$ — ее совершенная ДНФ. СФЭ для реализации функции f строим из m схем, реализующих конъюнкции $K_1, \ldots, K_m$, и $m-1$ дизъюнкторов, последовательно соединяющих выходы схем для этих конъюнкций. Таким образом, учитывая неравенство (7.1), приходим к следующему утверждению.

Если совершенная ДНФ функции f от n переменных состоит из m конъюнкций, то $L(f) \leqslant 2mn$.

Поскольку $m \leqslant 2^n$, для произвольной функции f от n переменных, отличной от константы 0, получаем оценку

$$L(f) \leqslant n2^{n+1}.$$

Константа 0 может быть реализована СФЭ из двух элементов (применяем тождество $0 = x \,\&\, \overline{x}$). Поэтому имеем

$$L(n) \leqslant n2^{n+1}. \tag{7.2}$$

Полученную верхнюю оценку для функции $L(n)$ можно несколько улучшить, если воспользоваться экономным способом реализации системы $Q_n(x_1, \ldots, x_n)$ всех 2^n конъюнкций от n переменных. В лемме 7.1, где предложен такой способ, для обозначения асимптотического равенства используется знак $\sim$.

Лемма 7.1. *Имеет место асимптотическое равенство*

$$L(Q_n) \sim 2^n.$$

Доказательство. Очевидно, что всякую конъюнкцию $x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$ можно представить в виде произведения двух конъюнкций: $x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m}$ из системы $Q_m(x_1, \ldots, x_m)$

и $x_{m+1}^{\sigma_{m+1}} \cdot \ldots \cdot x_n^{\sigma_n}$ из системы $Q_{n-m}(x_{m+1}, \ldots, x_n)$. Поэтому (см. рис. 5), имея схемы из функциональных элементов для реализации систем конъюнкций $Q_m(x_1, \ldots, x_m)$

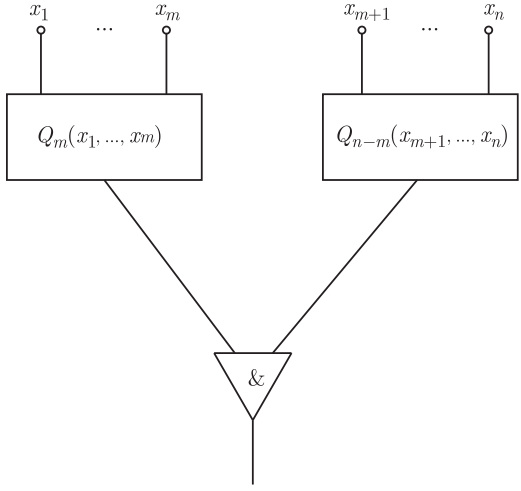


Рис. 5

и $Q_{n-m}(x_{m+1}, \ldots, x_n)$, достаточно добавить 2^n конъюнкторов, чтобы получить СФЭ, реализующую систему конъюнкций $Q_n(x_1, \ldots, x_n)$. Вместе с тем из (7.1) следует, что

$$L(Q_m) \leqslant m2^{m+1}, \quad L(Q_{n-m}) \leqslant (n-m)2^{n-m+1}.$$

Значит, для реализации системы конъюнкций Q_n достаточно не более

$$2^n + m2^{m+1} + (n-m)2^{n-m+1}$$

функциональных элементов.

Положим теперь $m = \left[\frac{n}{2}\right]$. Тогда будем иметь

$$m2^{m+1} \leqslant \left(\frac{n}{2}\right) 2^{n/2+1}, \quad (n-m)2^{n-m+1} \leqslant \left(\frac{n}{2}+1\right) 2^{n/2+2}.$$

Следовательно,

$$L(Q_n) \leqslant 2^n + O(n2^{n/2}) \sim 2^n.$$

С другой стороны, при $n \geqslant 2$ схема, реализующая систему конъюнкций Q_n, имеет не менее 2^n выходов (по числу всех конъюнкций от n переменных). Значит, при $n \geqslant 2$ получаем

$$L(Q_n) \geqslant 2^n.$$

Лемма доказана.

Используя лемму 7.1, можно усовершенствовать метод синтеза СФЭ, основанный на совершенной ДНФ, если заменить «раздельную» реализацию конъюнкций $K_1, \ldots, K_m$ их «совместной» реализацией, указанной в лемме 7.1. При этом для произвольной функции f от n переменных (отличной от константы 0) будем иметь

$$L(f) \leqslant L(Q_n) + 2^n$$

или, применяя лемму 7.1,

$$L(f) \lesssim 2 \cdot 2^n$$

(здесь и далее знаком $\lesssim$ обозначается неравенство «асимптотически не превосходит»). Таким образом,

$$L(n) \lesssim 2 \cdot 2^n.$$

§ 3. Метод Шеннона

Приводимый ниже метод синтеза предложен К. Шенноном для контактных схем. Здесь он излагается применительно к схемам из функциональных элементов.

Теорема 7.1. *Имеет место асимптотическое неравенство*

$$L(n) \lesssim 6 \cdot \frac{2^n}{n}.$$

Доказательство. Возьмем произвольную булеву функцию $f(x_1, \ldots, x_n)$ и разложим ее по первым $n - k$ переменным (параметр k будет выбран позже):

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_{n-k})} x_1^{\sigma_1} \cdot \ldots \cdot x_{n-k}^{\sigma_{n-k}} \cdot f(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n). \tag{7.3}$$

Схема Σ, реализующая функцию f, будет состоять из трех блоков (рис. 6):

1) блока, реализующего систему конъюнкций $Q_{n-k}(x_1, \ldots, x_{n-k})$;

2) блока, реализующего систему $U_k(x_{n-k+1}, \ldots, x_n)$ всех 2^{2^k} функций от переменных $x_{n-k+1}, \ldots, x_n$ (универсальный многополюсник порядка k);

3) блока, осуществляющего соединение первых двух блоков в соответствии с разложением (7.3).

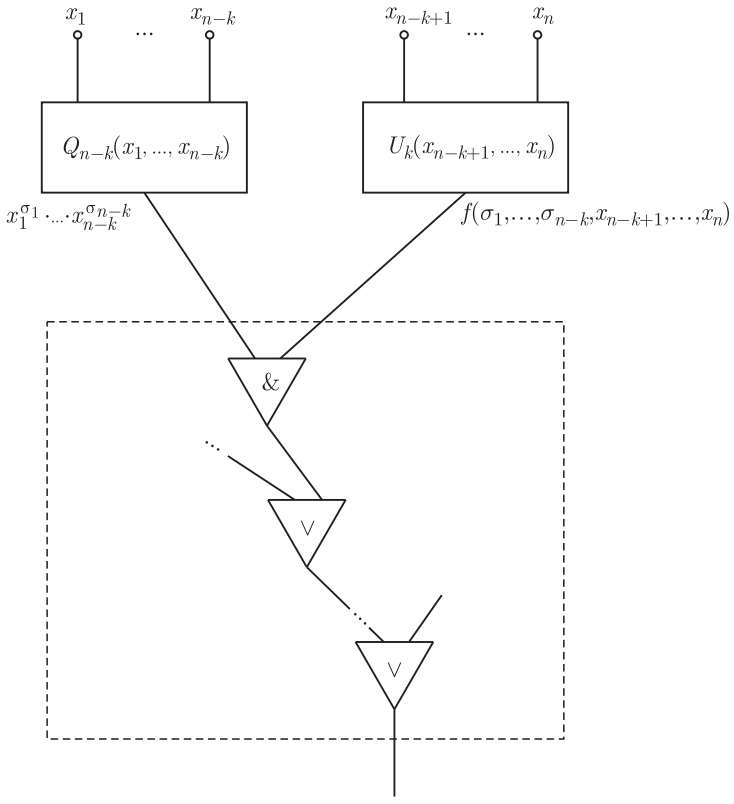


Рис. 6

Заметим, что первые два блока не зависят от реализуемой функции f, а зависят только от разбиения переменных функции f на два подмножества $\{x_1, \ldots, x_{n-k}\}$ и $\{x_{n-k+1}, \ldots, x_n\}$. В третьем блоке на каждое дизъюнктивное слагаемое разложения (7.3) приходится не более одного конъюнктора и не более одного дизъюнктора (некоторые слагаемые разложения могут быть нулевыми). Таким образом, получаем

$$L(\Sigma) \leqslant L(Q_{n-k}) + L(U_k) + 2 \cdot 2^{n-k}. \tag{7.4}$$

Исходя из тривиальной оценки (7.2) для сложности реализации универсального многополюсника U_k, получаем оценку

$$L(U_k) \leqslant k \cdot 2^{k+1} \cdot 2^{2^k} \tag{7.5}$$

(для величины $L(U_k)$ можно получить неулучшаемую оценку $2^{2^k} - k$, однако сейчас для нас это не важно и не влияет на получаемую ниже асимптотическую оценку).

Из леммы 7.1 и неравенств (7.4), (7.5) выводим, что

$$L(\Sigma) \lesssim 3 \cdot 2^{n-k} + k \cdot 2^{k+1} \cdot 2^{2^k}.$$

Положим (при достаточно больших n)

$$k = [\log_2(n - 3\log_2 n)].$$

Тогда будут справедливы неравенства

$$\log_2(n - 3\log_2 n) - 1 < k \leqslant \log_2(n - 3\log_2 n),$$

$$\frac{n - 3\log_2 n}{2} < 2^k \leqslant n - 3\log_2 n, \qquad 2^{2^k} \leqslant \frac{2^n}{n^3}.$$

Поэтому

$$3 \cdot 2^{n-k} + k \cdot 2^{k+1} \cdot 2^{2^k} < \frac{3 \cdot 2^{n+1}}{n - 3\log_2 n} + \frac{2^n}{n^3} \cdot 2n \cdot \log_2 n \lesssim 6 \cdot \frac{2^n}{n},$$

и теорема доказана.

Можно показать, что оценка функции Шеннона, даваемая теоремой 7.1, по порядку неулучшаема. В следующем параграфе мы найдем асимптотику функции Шеннона и, в частности, получим для нее нижнюю оценку, асимптотически равную $2^n/n$.

§ 4. Асимптотически наилучший метод О. Б. Лупанова

Теорема 7.2. *Имеет место асимптотическое неравенство*

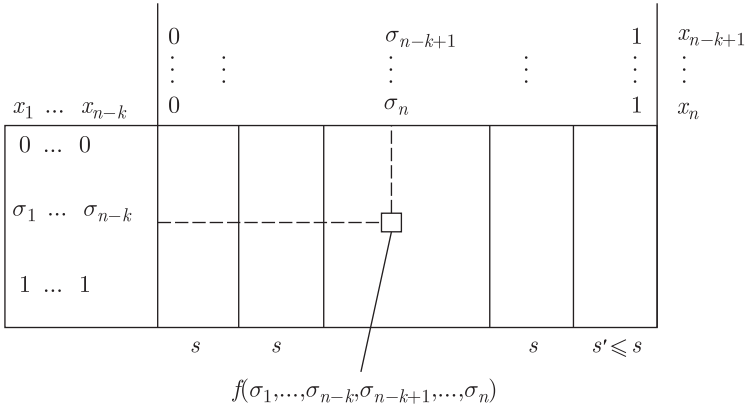
$$L(n) \lesssim \frac{2^n}{n}.$$

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция от n переменных. Ее можно задать таблицей, в которой значение $f(\sigma_1, \ldots, \sigma_{n-k}, \sigma_{n-k+1}, \ldots, \sigma_n)$ стоит на пересечении строки $(\sigma_1, \ldots, \sigma_{n-k})$ и столбца $(\sigma_{n-k+1}, \ldots, \sigma_n)$ (табл. 7).

Разобьем столбцы таблицы на вертикальные полосы $H_1, \ldots, H_p$ по s столбцов в полосе (последняя полоса может содержать меньшее число столбцов). Очевидно, что

$$\frac{2^k}{s} \leqslant p < \frac{2^k}{s} + 1.$$

Таблица 7



Обозначим через f_i функцию, совпадающую с функцией f в полосе H_i и равную 0 вне этой полосы. Из определений следует, что имеют место следующие равенства:

$$f(x_1,\ldots,x_n) = \bigvee_{i=1}^{p} f_i(x_1,\ldots,x_n) =$$

$$= \bigvee_{i=1}^{p} \bigvee_{(\sigma_1,\ldots,\sigma_{n-k})} x_1^{\sigma_1}\cdot\ldots\cdot x_{n-k}^{\sigma_{n-k}}\cdot f_i(\sigma_1,\ldots,\sigma_{n-k},x_{n-k+1},\ldots,x_n) =$$

$$= \bigvee_{(\sigma_1,\ldots,\sigma_{n-k})} x_1^{\sigma_1}\cdot\ldots\cdot x_{n-k}^{\sigma_{n-k}} \bigvee_{i=1}^{p} f_i(\sigma_1,\ldots,\sigma_{n-k},x_{n-k+1},\ldots,x_n).$$

Заметим, что каждая функция $f_i(\sigma_1,\ldots,\sigma_{n-k},x_{n-k+1},\ldots,x_n)$ задается одной строкой таблицы и потому принимает значение 1 не более чем на s наборах. Кроме того, при фиксированном i число различных функций $f_i(\sigma_1,\ldots,\sigma_{n-k},x_{n-k+1},\ldots,x_n)$ не превосходит величины 2^s.

Схема Σ, реализующая функцию f, строится на основе представления (7.3) и состоит из 6 блоков (рис. 7).

1) Блок A реализует систему конъюнкций $Q_{n-k}(x_1,\ldots,x_{n-k})$,

$$L(A) \leqslant (n-k)2^{n-k+1}.$$

2) Блок B реализует систему конъюнкций $Q_k(x_{n-k+1},\ldots,x_n)$,

$$L(B) \leqslant k\cdot 2^{k+1}.$$

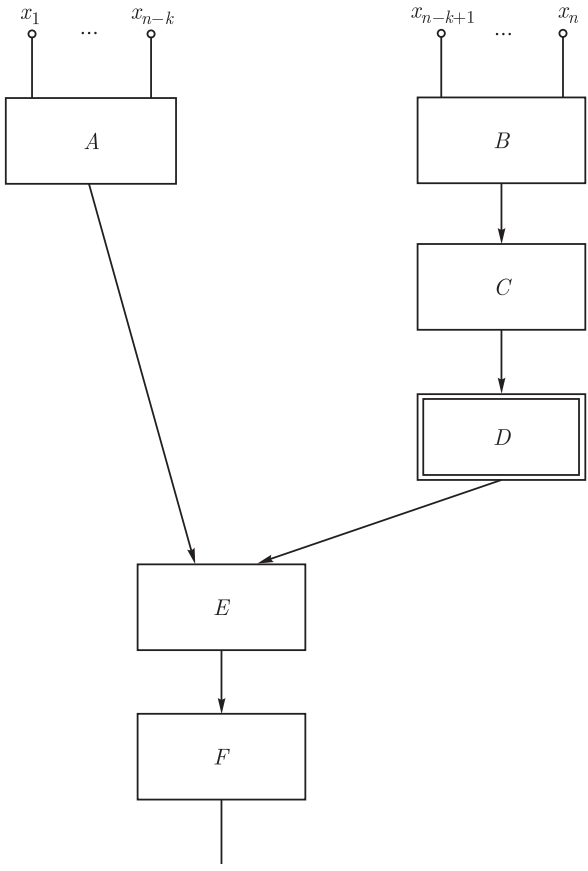


Рис. 7

3) Блок C реализует все различные функции $f_i(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n)$. Из определения функций f_i следует, что для реализации одной такой функции (с использованием конъюнкций, реализованных блоком B) требуется не более s дизъюнкторов, поэтому

$$L(C) \leqslant ps2^s.$$

4) Блок D реализует все функции

$$\bigvee_{i=1}^{p} f_i(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n) = \\ = f(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n).$$

Имеем

$$L(D) \leqslant p2^{n-k}.$$

5) Блок E выполняет умножение

$$x_1^{\sigma_1} \cdot \ldots \cdot x_{n-k}^{\sigma_{n-k}} \cdot f(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n).$$

Очевидно, что

$$L(D) = 2^{n-k}.$$

6) Блок F реализует функцию $f(x_1, \ldots, x_n)$ как дизъюнкцию функций, реализованных блоком E. Имеем

$$L(F) \leqslant 2^{n-k}.$$

Таким образом,

$$L(\Sigma) = L(A) + L(B) + L(C) + L(D) + L(E) + L(F) \leqslant$$
$$\leqslant (n-k)2^{n-k+1} + k2^{k+1} + ps2^s + p2^{n-k} + 2^{n-k+1}.$$

Положим

$$k = [3\log_2 n], \quad s = [n - 5\log_2 n].$$

Тогда будем иметь

$$(n-k)2^{n-k+1} = O\left(\frac{2^n}{n^2}\right) = o\left(\frac{2^n}{n}\right),$$

$$k2^{k+1} = O(n^3 \log_2 n) = o\left(\frac{2^n}{n}\right),$$

$$ps2^s \sim \frac{2^k}{s} s 2^s = 2^{k+s} = O\left(\frac{2^n}{n^2}\right) = o\left(\frac{2^n}{n}\right),$$

$$p2^{n-k} \sim \frac{2^k}{s} 2^{n-k} = \frac{2^n}{s} \sim \frac{2^n}{n},$$

и теорема доказана.

Перейдем к нижней оценке для функции $L(n)$. Для этого сначала оценим сверху число $S(n, m)$ функций от переменных $x_1, \ldots, x_n$, которые реализуются схемами из m элементов. Зафиксируем n входов схемы, которым припишем входные переменные $x_1, \ldots, x_n$. Остальным m вершинам $v_1, \ldots, v_m$ схемы будут приписаны функции базиса B. Любой вершине v_i можно приписать одну из трех функций базиса. Это дает 3^m вариантов «расстановки» булевых функций по вершинам $v_1, \ldots, v_m$ схемы. В каждую вершину v_i может вести одна или две дуги от входов схемы либо от остальных вершин $v_1, \ldots, v_m$. Мы увеличим число возможностей, если будем считать, что в каждую вершину ведут ровно две дуги, причем эти дуги могут исходить из любых вершин схемы (это, разумеется, может привести к конструкциям, которые не являются СФЭ). Для одной вершины эта процедура дает $(n+m)^2$ возможностей, для всех вершин — $(n+m)^{2m}$ возможностей. После того как «схема» создана, необходимо

определить выход схемы. Для этого следует указать одну из $n+m$ вершин схемы. В итоге получим верхнюю оценку вида $3^m(n+m)^{2m+1}$.

Теперь следует заметить, что данную верхнюю оценку $3^m(n+m)^{2m+1}$ можно разделить на $m!$. В самом деле, если мы отобразили множество вершин $\{v_1,\dots,v_m\}$ в базис B с помощью функции V, а затем выполнили некоторую нетождественную перестановку на множестве $\{1,2,\dots,m\}$, то результирующее отображение V' множества $\{v_1,\dots,v_m\}$ в базис B будет нами также учтено. Однако после того, как для отображения V выбраны дуги в графе схемы и выход схемы, соответствующий перестановке, выбор дуг и выхода схемы для отображения V' приведет к реализации той же самой функции, что и для отображения V. Таким образом, окончательно приходим к оценке

$$S(n,m) \leqslant \frac{3^m(n+m)^{2m+1}}{m!}. \tag{7.6}$$

Теорема 7.3. *Имеет место асимптотическое неравенство*

$$L(n) \gtrsim \frac{2^n}{n}.$$

Доказательство. Как установлено выше, число функций от переменных $x_1\dots,x_n$, имеющих схемную сложность минимальной реализации не выше m, ограничено сверху величиной (7.6) (если функция реализуема схемой со сложностью меньше m, то она, конечно, может быть реализована схемой со сложностью, равной m: достаточно ввести в схему требуемое число «фиктивных» элементов). Однако для подходящей константы c и при $m>n$ имеют место следующие соотношения:

$$\frac{3^m(n+m)^{2m+1}}{m!} < \frac{3^m(2m)^{2m+1}}{(m/e)^m} = (6e)^m\cdot m^{m+1} < (cm)^m$$

(здесь e — основание натуральных логарифмов). Поэтому если взять $m=\left[\dfrac{2^n}{n}\right]$ (при этом неравенство $m>n$ будет выполняться для $n\geqslant 5$), то число функций от n переменных, которые реализуются схемами сложности не более m, не превосходит величины

$$\left(\frac{c2^n}{n}\right)^{2^n/n}. \tag{7.7}$$

Разделив эту величину на число 2^{2^n} всех булевых функций от n переменных и взяв взяв двоичный логарифм от частного,

получим (при $n \to \infty$)

$$\frac{2^n}{n}(n + \log_2 c - \log_2 n) - 2^n = \frac{2^n}{n}(\log_2 c - \log_2 n) \to -\infty.$$

Таким образом, при достаточно больших n число (7.7) будет меньше числа 2^{2^n}. Это означает, что схемами сложности не выше $2^n/n$ невозможно реализовать все булевы функции от n переменных. Теорема доказана.

Из теорем 7.2, 7.3 вытекает итоговый результат этой главы.

Теорема 7.4. *Имеет место асимптотическое равенство*

$$L(n) \sim \frac{2^n}{n}.$$

Комментарии. Задача оценки сложности реализации булевых функций некоторыми классами управляющих систем впервые рассмотрена в работах К. Шеннона [50, 51]. Им же найден порядок функции Шеннона при реализации булевых функций контактными схемами [51]. Асимпототически наилучший метод синтеза схем из функциональных элементов в базисе B (а также в любых других полных базисах) предложен О. Б. Лупановым [14–16]. Этот метод широко представлен в ряде учебников и учебных пособий [1, 13, 26, 34, 38].

Список литературы

1. *Алексеев В.Б.* Лекции по дискретной математике. М.: ИНФРА-М, 2012. 89 с.
2. *Алексеев В.Б.*, *Вороненко А.А.* О некоторых замкнутых классах в частичной двузначной логике // Дискретная математика. 1994. Т. 6, № 4. С. 58–79.
3. *Блохина Г.Н.* О предикатном описании классов Поста // Дискретный анализ. 1970. № 16. С. 16–29.
4. *Боднарчук В.Г.*, *Калужнин Л.А.*, *Котов В.Н.*, *Ромов Б.А.* Теория Галуа для алгебр Поста // Кибернетика. 1969. № 3. С. 1–10; № 5. С. 1–9.
5. *Гаврилов Г.П.* Индуктивное представление булевых функций и конечная порождаемость классов Поста // Алгебра и логика. 1984. Т. 23, № 1. С. 3–26.
6. *Гаврилов Г.П.* Функциональные системы дискретной математики. М.: Из-во МГУ, 1985, 39 с.
7. *Данильченко А.Ф.* О параметрической выразимости функций трехзначной логики // Алгебра и логика. 1977. Т. 16, № 4. С. 397–416.
8. *Ершов Ю.Л.*, *Палютин Е.А.* Математическая логика. М.: Наука, 1979. 320 с.
9. *Кузнецов А.В.* Алгебра логики и ее обобщения // Яновская С.А. Математическая логика и основания математики. Математика в СССР за сорок лет, т. 1. М.: Физматгиз, 1959. С. 13–120.
10. *Кузнецов А.В.* Структуры с замыканием и критерии функциональной полноты // Успехи матем. наук. 1961. Т. XVI, № 2(98). С. 201–202.
11. *Кузнецов А.В.* О средствах для обнаружения невыводимости и невыразимости. Логический вывод. М.: Наука, 1979. С. 5–33.
12. *Лавров И.А.* Математическая логика. М.: Академия, 2006. 240 с.
13. *Ложкин С.А.* Лекции по основам кибернетики. Учебное пособие. М.: Издательский отдел факультета Вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, МАКС Пресс, 2004. 253 с.
14. *Лупанов О.Б.* Об одном методе синтеза схем // Известия вузов. Радиофизика. 1958. Т. 1, № 1. С. 120–140.
15. *Лупанов О.Б.* О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. М.: Физматгиз, 1963. С. 63–97.
16. *Лупанов О.Б.* Асимптотические оценки сложности управляющих систем. М.: Издательство Московского университета, 1984. 137 с.

17. *Марченков С.С.* Инварианты классов Поста // Фундаментальная и прикладная математика. 1998. Т. 4, № 4. С. 1385–1404.
18. *Марченков С.С.* О выразимости функций многозначной логики в некоторых логико-функциональных языках // Дискретная математика. 1999. Т. 11, № 4. С. 110–126.
19. *Марченков С.С.* Замкнутые классы булевых функций. М.: Физматлит, 2000. 126 с.
20. *Марченков С.С.* Конечная порождаемость замкнутых классов булевых функций // Дискретный анализ и исследование операций. Серия 1. 2005. Т. 12, № 1. С. 101–118.
21. *Марченков С.С.* Функциональные системы. Учебное пособие. М.: Издательсткий отдел факультета ВМиК МГУ имени М. В. Ломоносова; МАКС Пресс. 48 с.
22. *Марченков С.С.*, *Угольников А.Б.* Замкнутые классы булевых функций. М.: Из-во ИПМ АН СССР, 1990. 147 с.
23. *Нигматуллин Р.Г.* Сложность булевых функций. М.: Наука, 1991. 240 с.
24. *Оре О.* Теория графов. М.: Наука, 1968. 352 с.
25. *Перязев Н.А.*, *Казимиров А.С.* Замкнутые множества булевых функций. Учебная монография. Иркутск, 2010. 52 с.
26. *Редькин Н.П.* Дискретная математика. М: Физматлит, 2009. 262 с.
27. *Риге Ж.* Бинарные отношения, замыкания, соответствия Галуа // Кибернетический сборник, вып. 7. М.: Мир, 1963. С. 129–185.
28. *Сапоженко А.А.* Проблема Дедекинда и метод граничных функционалов // Математические вопросы кибернетики. Вып. 9. М.: Физматлит, 2000. С. 161–220.
29. *Сапоженко А.А.* Проблема Дедекинда и метод граничных функционалов. М.: Физматлит, 2009. 151 с.
30. *Угольников А.Б.* О замкнутых классах Поста // Известия ВУЗов. Математика. 1988. № 7. С. 79–88.
31. *Угольников А.Б.* Классы Поста. М.: Из-во ЦПИ при механико-математическом факультете МГУ им. М.В.Ломоносова, 2008. 62 с.
32. *Фрейвалд Р.В.* Критерий полноты для частичных функций алгебры логики и многозначных логик // Доклады АН СССР. 1966. Т. 167, № 6. С. 1249–1250.
33. *Фрейвалд Р.В.* Функциональная полнота для не всюду определенных функций алгебры логики // Дискретный анализ. 1966. № 8. С. 55–68.
34. *Чашкин А.В.* Дискретная математика. М.: Академия, 2012. 352 с.
35. *Яблонский С.В.* О строении верхней окрестности для предикатно-описуемых классов в P_k // Доклады АН СССР. 1974. Т. 218, № 2. С. 304–307.
36. *Яблонский С.В.* О суперпозициях функций алгебры логики // Матем. сборник. 1952. Т. 30, № 2. С. 329–348.

37. *Яблонский С.В.* Функциональные построения в k-значной логике // Труды матем. ин-та им. В.А.Стеклова АН СССР. 1958. Т. LI. С. 5–142.
38. *Яблонский С.В.* Введение в дискретную математику. М.: Наука, 1986. 384 с.
39. *Яблонский С.В.*, *Гаврилов Г.П.*, *Кудрявцев В.Б.* Функции алгебры логики и классы Поста. М.: Наука, 1966. 119 с.
40. *Benzaken C.* Definitions et proprietes de certains familles de fonctions booleénnes croissantes // C. R. Acad. Sci. Paris. 1964. T. 259, group I. P. 1369–1371.
41. *Benzaken C.* Les familles de fonctions booleénnes deduites de certains familles de fonctions booleénnes croissates. Criteres de determination de l'indice d'une fonction croissante // C. R. Acad. Sci. Paris. 1965. T. 260, group I. P. 1528–1531.
42. *Geiger D.* Closed systems of functions and predicates // Pacific J. Math. 1968. V. 27. P. 95–100.
43. *Hermann M.* On Boolean primitive positive clones // Discrete Math. 2008. V. 308. P. 3151–3162.
44. *Kuntzman J.* Algébre de Boole. Paris, Dunod, 1965. 319 p.
45. *Lau D.* On closed subsets of Boolean functions (A new proof for Post's theorem) // J. Inform. Process. Cybernet. EIK. – 1991. Bd. 27, № 3. S. 167–178.
46. *Ore O.* Galois connections // Trans. Amer. Math. Soc. 1944. V. 55. P. 493–513.
47. *Post E.L.* Introduction to a general theory of elementary propositions // Amer. J. Math. 1921. V. 43, № 4. P. 163–185.
48. *Post E.L.* Two-valued iterative systems of mathematical logic // Annals of Math. Studies. Princeton Univ. Press, 1941. V. 5. P. 1–122.
49. *Reschke M.*, *Denecke K.* Ein neuer Beweis für die Ergebnisse von E.L.Post über abgeschlossene Klassen Boolescher Funktionen // J. Process. Cybern. EIK. 1989. Bd. 7. S. 361–380.
50. *Riordan J.*, *Shannon C.E.* The number of two-terminal series-parallel networks // J. Math. and Phys. 1942. V. 21, № 2. P. 83–93. (Русский перевод: Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 83–93.)
51. *Shennon C.E.* The synthesis of two-terinal switching circuits // Bell Syst. Techn. J. 1949. V. 28, № 1. P. 59–98. (Русский перевод: Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 59–101.)
52. *Szabó L.* Concrete representation of related strucrures of universal algebras I // Acta Sci. Math. 1978. V. 40. P. 175–184.
53. *Szabó L.* On the lattice of clones acting bicenrally // Acta Cybernet. 1984. V. 6. P. 381–388.

Предметный указатель

Учебное издание

МАРЧЕНКОВ Сергей Серафимович

ОСНОВЫ ТЕОРИИ БУЛЕВЫХ ФУНКЦИЙ

Редактор *Е.И. Ворошилова*
Оригинал-макет: *В.В. Затекин*
Оформление переплета: *Д.Б. Белуха*

Подписано в печать 13.05.2014. Формат 60×90/16. Бумага офсетная.
Печать офсетная. Усл. печ. л. 8,5. Уч.-изд. л. 9,35. Тираж 300 экз.
Заказ №

Издательская фирма «Физико-математическая литература»
МАИК «Наука/Интерпериодика»
117997, Москва, ул. Профсоюзная, 90
E-mail: fizmat@maik.ru, fmlsale@maik.ru;
http://www.fml.ru

Отпечатано с электронных носителей издательства
в ОАО «ИПК «Чувашия», 428019
г. Чебоксары, пр-т И. Яковлева, 13

ISBN 978-5-9221-1562-9