ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

ВЫПУСК

С.С. МАРЧЕНКОВ

БУЛЕВЫ ФУНКЦИИ

МОСКВА, 2002

УДК 519.7
ББК 22.176
М25

Марченков С. С. **Булевы функции.**— М.: ФИЗМАТЛИТ, 2002.— 68 с.— ISBN 5-9221-0253-2.

Брошюра знакомит читателя с булевыми функциями — одним из важнейших классов дискретных функций. В ней излагаются основные понятия теории булевых функций, доказывается критерий функциональной полноты и рассматриваются вопросы сложности реализации булевых функций.

Брошюра предназначена для школьников старших классов и студентов первых курсов.

Табл. 4. Ил. 11.

ISBN 5-9221-0253-2

ПРЕДИСЛОВИЕ

С понятием функции сегодня знаком каждый выпускник средней школы. И это закономерно — понятие функции относится к тем немногим понятиям, которые пронизывают все разделы математики.

В математике имеется огромное число различных типов функций. Однако есть в ней такие функции, которые по праву должны быть названы самыми простыми. Речь идет о булевых функциях [1]) — функциях, которые определены на множестве, состоящем из двух элементов. Уменьшить это множество до одного элемента невозможно — происходит вырождение понятия функции. Поэтому булевы функции занимают первую ступень в иерархии функций, ниже которой располагаются только константы.

Как математический объект булевы функции начали интенсивно изучаться лишь около 50 лет назад. Примерно в то же время появились и первые электронные цифровые вычислительные машины. Совпадение этих двух событий неслучайно. Дело в том, что по ряду причин технического и математического характера язык, на котором "говорят" ЭВМ, есть язык двух символов: да–нет, 0–1. Поэтому описывать работу ЭВМ и программировать на ЭВМ удобно с использованием булевых функций. Булевы функции оказались также подходящим инструментом для описания функционирования широкого круга дискретных преобразователей информации, которые не относятся к универсальным вычислительным машинам: переключателей, коммутаторов, простейших сумматоров и некоторых других.

Бурное развитие вычислительной техники, а также запросы со стороны смежных разделов математики поставили перед специалистами по булевым функциям целый ряд серьезных математических проблем: анализ различных форм и возможностей представления булевых функций, оценки сложности реализации булевых функций формулами и схемами, оценки сложности построения оптимальных формул и схем и некоторые другие. Эти проблемы и направления исследований и по сей день остаются центральными в теории булевых функций.

---

[1]) Свое название булевы функции получили по имени английского математика Дж. Буля (G. Boole, 1815–1864).

Основные цели предлагаемой брошюры состоят в том, чтобы научить читателя языку булевых функций, познакомить его с основными фактами из теории булевых функций, показать, как решаются простейшие из перечисленных выше задач и в какой-то степени обрисовать трудности и перспективы на пути решения более сложных проблем. Мы полагаем, что потребность в подобном знакомстве с элементами теории булевых функций давно назрела, тем более, что компьютерная грамотность предполагает умение оперировать с простейшими булевыми функциями.

Книга предназначена в первую очередь для учеников старших классов средней школы. Она может быть также полезна студентам младших курсов университетов и технических вузов, изучающим дискретную математику.

Глава I

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ

§ 1. Табличное задание булевых функций

Булевы функции определяются на множестве, состоящем из двух элементов. В качестве этих элементов обычно берутся числа 0 и 1. Будем обозначать множество, состоящее из 0 и 1, через B. Булеву функцию определим как функцию, аргументы которой принимают значения из B со значениями, также принадлежащими B.

Булеву функцию f (от) n аргументов обозначают через $f(x_1, \ldots, x_n)$ и называют также булевой функцией (от) n переменных. Иногда в обозначениях булевых функций вместо переменных $x_1, x_2, \ldots$ используют переменные $y, z, w, \ldots$, возможно, с индексами.

Булева функция $f(x_1, \ldots, x_n)$ ставит в соответствие каждому упорядоченному набору $(a_1, \ldots, a_n)$, состоящему из элементов 0 и 1, единственный элемент множества B — значение $f(a_1, \ldots, a_n)$. Как же задают функцию $f(x_1, \ldots, x_n)$?

Чтобы ответить на этот вопрос, найдем предварительно число элементов множества B^n, состоящего из всех упорядоченных двоичных (имеются в виду элементы 0 и 1) наборов $(a_1, \ldots, a_n)$ длины n. Докажем, что это число равно 2^n. Доказательство проведем с использованием принципа полной математической индукции.

Очевидно, что множество B^1 состоит ровно из двух наборов. Предположим по индукции, что для данного n $(n \geqslant 1)$ множество B^n состоит из 2^n наборов, и рассмотрим множество B^{n+1}. Каждый двоичный набор $(a_1, \ldots, a_n)$ длины n порождает два различных набора $(a_1, \ldots, a_n, 0)$, $(a_1, \ldots, a_n, 1)$ из множества B^{n+1}. При этом если наборы $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$ из B^n различны, то при любом выборе элементов a_{n+1} и b_{n+1} из множества B будут различными и наборы

$$(a_1, \ldots, a_n, a_{n+1}), \quad (b_1, \ldots, b_n, b_{n+1}).$$

Следовательно, число наборов в множестве B^{n+1} в два раза больше числа наборов в множестве B^n. Поскольку последнее число по предположению индукции есть 2^n, первое число будет равно $2^n \cdot 2 = 2^{n+1}$.

Определив число наборов в множестве B^n, вернемся к вопросу о задании булевой функции $f(x_1, \ldots, x_n)$. Проще всего ее можно задать так называемым табличным способом: перечислить в некотором порядке все наборы из множества B^n и вслед за каждым набором записать значение функции f на этом наборе. Наиболее наглядно реа-

лизовать этот способ задания булевой функции можно действительно в виде таблицы (табл. 1).

В левой части этой таблицы выписаны по строкам все 2^n двоичных наборов длины n. Порядок, в котором они расположены в таблице (сверху вниз), носит название лексикографический порядок.

Таблица 1

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

Первым относительно этого порядка является нулевой набор, а каждый следующий набор получается из предыдущего прибавлением 1. При этом мы считаем, что каждый набор является записью подходящего неотрицательного целого числа в двоичной системе счисления, а имеющиеся слева нулевые разряды поставлены лишь для того, чтобы все наборы имели одну и ту же длину n.

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 табл. 1 будет одной и той же. Поэтому потребность в ее воспроизведении, вообще говоря, отпадает. Тогда от табл. 1 остается только столбец значений функции f высоты 2^n.

Таким образом, мы приходим к выводу, что 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. При этом первый элемент столбца становится первым элементом строки, второй элемент столбца — вторым элементом строки и т.д. В результате для булевой функции $f(x_1, \ldots, x_n)$ получаем двоичную строку вида

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

Итак, каждую булеву функцию $f(x_1, \ldots, x_n)$ можно представить двоичным набором (1) ее значений длины 2^n и всякий двоичный набор длины 2^n определяет некоторую булеву функцию от n переменных. Нетрудно заметить, что данное соответствие, как говорят, взаимно однозначно: различным булевым функциям от n переменных (различным двоичным наборам длины n) отвечают различные двоичные

наборы длины 2^n (различные булевы функции от n переменных). Это позволяет найти число всех булевых функций от n переменных. Действительно, оно равно числу всех двоичных наборов длины 2^n, т.е. числу всех элементов множества B^{2^n}. Как мы установили выше, данное число равно 2^{2^n}.

Множество всех булевых функций принято обозначать через P_2.

УПРАЖНЕНИЯ

1. Каково число булевых функций от n переменных, которые на фиксированных k двоичных наборах ($k \leqslant 2^n$) принимают фиксированные k значений?

§ 2. Некоторые элементарные булевы функции

Составим таблицу для всех четырех булевых функций 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 $\overline{x}$ (читается: не икс).

Обратимся далее к функциям от двух переменных. Как мы знаем, их насчитывается ровно $2^{2^2} = 16$. Мы могли бы поступить так же,

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 с функциями от одной переменной, и представить в одной таблице значения всех 16 функций. Однако на первых порах нам будет достаточно познакомиться с одиннадцатью функциями (по техническим причинам в табл. 3 после символов функций опущены символы переменных x_1, x_2).

Как видно из табл. 3, функции $f_1(x_1, x_2)$ и $f_2(x_1, x_2)$ являются константами 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. Аналогично обстоит дело с функцией $f_4(x_1, x_2)$, которая представляет собой функцию выбора (второго аргумента) и обозначается $e_2^2(x_1, x_2)$. 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 логике и 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 $x_1 x_2$ (читается: x_1 и 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 логике и теории булевых функций. Функцию $f_8(x_1, x_2)$ называют *дизъюнкцией* (или логической суммой) и обозначают $x_1 \vee x_2$ (читается: x_1 или 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 *импликация* и обозначается $x_1 \to x_2$. Название "импликация" пришло из логики, где имеется соответствующая логическая связка импликация.

Наконец, функция $f_{11}(x_1, x_2)$ называется *штрихом Шеффера* (или антиконъюнкцией) и обозначается $x_1 \mid x_2$.

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 (или 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.

УПРАЖНЕНИЯ

2. Достройте табл. 3, выписав столбцы значений остальных пяти булевых функций. Используя приведенные выше названия функций от двух переменных, попытайтесь дать подходящие названия этим пяти функциям.

§ 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 $f_1(x_1, x_2)$. Аналогичное замечание следует сделать и 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.

Проверьте, что оставшиеся функции $f_8(x_1, x_2), \ldots, f_{11}(x_1, x_2)$ также существенно зависят от обеих переменных.

Приведем 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 имеются 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 имеются 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

$$f(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = g(x_1, \ldots, x_m), \tag{2}$$

которое выполняется при любых значениях переменных $x_1, \ldots, x_n$. Вообще, этот прием показывает, что функцию $g(x_1, \ldots, x_m)$ можно считать зависящей от любого числа дополнительных фиктивных переменных. При этом важно лишь помнить, что с функциональной

точки зрения переход от функции g к функции f, даваемый равенством (2), приводит к появлению нового объекта: функция f определена на множестве B^n, тогда как функция g — на множестве B^m.

Приведенные рассуждения показывают, что введение и удаление фиктивных переменных можно осуществить сравнительно простыми средствами, практически "даром". Это особенно важно при введении фиктивных переменных. В связи с этим в теории булевых функций иногда для функции указывают лишь те переменные, от которых она зависит существенно. При этом предполагается, что от всех остальных переменных, которые встречаются в дальнейших построениях, данная функция зависит фиктивно.

Следует отметить, что при введении и удалении фиктивных переменных необходимо проявлять известную осторожность. Пусть, например, имеется булева функция $g(x_1, x_2, x_3)$ и мы хотим введением фиктивных переменных получить из нее булеву функцию, зависящую от переменных $x_1, \ldots, x_5$. Довольно просто сообразить, что достичь этого можно различными способами. Прежде всего, напрашивается "естественный" способ введения: добавляемые переменные x_4, x_5 фиктивны, а искомая функция $f_1(x_1, \ldots, x_5)$ определяется равенством

$$f_1(x_1, x_2, x_3, x_4, x_5) = g(x_1, x_2, x_3). \tag{3}$$

Однако можно поступить иначе: к переменным функции g добавить две новые переменные так, чтобы "старые" переменные x_1, x_2, x_3 функции g для вновь определяемой функции $f_2(x_1, \ldots, x_5)$ оказались соответственно второй, четвертой и пятой переменными. Этот вариант введения фиктивных переменных дается равенством

$$f_2(x_1, x_2, x_3, x_4, x_5) = g(x_2, x_4, x_5). \tag{4}$$

Разумеется, на этом пути введения фиктивных переменных существует еще несколько различных функций $f_i(x_1, \ldots, x_5)$, каждая из которых определяется выбором трех различных переменных x_p, x_q, x_r из множества $\{x_1, \ldots, x_5\}$ и использованием в равенствах (3), (4) соответствующей функции $g(x_p, x_q, x_r)$.

По традиции, сложившейся в отечественной школе дискретной математики, булевы функции рассматриваются с точностью до несущественных переменных. Это означает, что наряду с любой булевой функцией f считаются одновременно заданными все функции, которые получаются из f введением или удалением несущественных переменных. Иногда такие функции называют равными, хотя, строго говоря, они различаются уже как функции, имеющие различные количества переменных. Мы в дальнейшем не будем употреблять термин "равные" в этом смысле. Тем не менее равенства типа (3) или (4) будут использоваться.

Весьма распространенным способом введения фиктивных переменных является способ введения с помощью селекторных функций.

Пусть мы имеем булеву функцию g от m переменных и хотим получить из нее функцию f, удовлетворяющую тождеству (2). Тогда функцию f можно определить так:

$$f(x_1, \ldots, x_n) = g(e_1^n(x_1, \ldots, x_n), \ldots, e_m^n(x_1, \ldots, x_n)). \qquad (5)$$

Преимущество этого способа состоит в том, что переменные $x_{m+1}, \ldots, x_n$ не появляются "ниоткуда", как это происходит при переходе от правой к левой части равенства (2). Наряду с переменными $x_1, \ldots, x_m$ они изначально присутствуют в правой части равенства (5). Поэтому данный способ введения фиктивных переменных с математической точки зрения представляется более корректным. К недостаткам его можно отнести то, что среди "исходных" булевых функций селекторные функции присутствуют далеко не всегда.

УПРАЖНЕНИЯ

3. Найдите существенные и фиктивные переменные функций $g_1(x_1, x_2, x_3)$ и $g_2(x_1, x_2, x_3)$, заданных двоичными наборами (10100101) и (00010111).

4. Пусть функция $f(x_1, \ldots, x_n)$ задана двоичным набором $(a_1 \ldots a_{2^{n-1}} a_{2^{n-1}+1} \ldots a_{2^n})$, а функция $g(x_1, \ldots, x_n)$ — набором $(a_{2^n} \ldots a_{2^{n-1}+1} a_{2^{n-1}} \ldots a_1)$. Как соотносятся существенные и фиктивные переменные функций f и g?

5. Назовем булеву функцию *симметрической*, если она принимает одинаковые значения на любых двух наборах, содержащих одинаковое количество единичных компонент. Докажите, что всякая симметрическая булева функция, отличная от константы, существенно зависит от всех своих переменных.

§ 4. Представление 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. Так, например, обращаясь к элементарной алгебре, видим, что формула

$$(x_1 + x_2) \cdot x_2 + x_1 \cdot x_3, \qquad (6)$$

составленная из символов переменных x_1, x_2, x_3 и символов функций $+$ и $\cdot$, указывает на определенную последовательность при вычислении функции, представленной этой формулой: например, 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 (6) считаем известными, "элементарными", а формула (6) 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 некоторое непустое множество F булевых функций. 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.

С помощью индукции (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 уже определенные формулы над F, либо символы переменных (не обязательно различные). Тогда выражение $g(A_1, \ldots, A_m)$ считаем формулой над F.

Пусть, например, F есть множество булевых функций, состоящее из функций $\overline{}$ (отрицание), $\cdot$ (конъюнкция), $\vee$ (дизъюнкция), $\oplus$ (сложение по модулю 2), $\to$ (импликация), $|$ (штрих Шеффера). Тогда согласно приведенному выше определению следующие выражения будут являться формулами над F:

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

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

(чтобы не усложнять вид формул, мы не пишем скобок при использовании отрицаний от переменных).

Понятно, что формулы предназначены для задания булевых функций. Как же определить функцию, задаваемую (или, как говорят, реализуемую) конкретной формулой? Для этого надо вновь обратиться к определению понятия формулы над F и параллельно этому определению ввести определение *функции, реализуемой формулой над* F.

Если f есть обозначение функции от n переменных из F, то формула $f(x_1, \ldots, x_n)$ реализует ту самую функцию от n переменных, 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 A_i. Если же выражение A_i представляет собой символ переменной x_j, то сопоставим ему тождественную функцию $h_i(x_j)$, значения которой совпадают со значениями переменной x_j. Тогда формула $g(A_1, \ldots, A_m)$ *реализует* функцию

$$g(h_1, \ldots, h_m). \tag{7}$$

Сделаем несколько замечаний по поводу определения функции (7). 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.

Во-вторых, мы оставили в стороне вопрос о том, что же представляет собой функция (7). Мы не хотели бы приводить здесь точные, но громоздкие определения. Вместо этого обратимся к примерам.

По-видимому, все читатели представляют себе, как вычисляются значения функции

$$g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)),$$

если функции $g, h_1, \ldots, h_m$ предполагаются известными: для любого двоичного набора $(a_1, \ldots, a_n)$ вычисляем значения

$$h_1(a_1, \ldots, a_n), \ \ldots, \ h_m(a_1, \ldots, a_n),$$

образуем двоичный набор

$$(h_1(a_1, \ldots, a_n), \ldots, h_m(a_1, \ldots, a_n))$$

и, используя функцию g, вычисляем ее значение на этом наборе.

Чуть более сложной является формула

$$g(h_1(x_4, x_1), x_3, h_2(x_3, x_2, x_1)).$$

Здесь по заданному двоичному набору (a_1, a_2, a_3, a_4) необходимо сначала вычислить значения $h_1(a_4, a_1)$ и $h_2(a_3, a_2, a_1)$, затем образовать двоичный набор

$$(h_1(a_4, a_1), a_3, h_2(a_3, a_2, a_1))$$

и найти значение функции g на этом наборе.

На этом примере уже хорошо видны те трудности, которые поджидают нас при определении функции (7): все они связаны с тем, что переменные в функциях $h_1, \ldots, h_m$ могут быть "перемешаны" каким угодно образом.

Чтобы облегчить изложение некоторых результатов, требующих для своего доказательства анализа сложных формул, нередко поступают следующим образом. Пусть, к примеру, требуется проанализировать формулу (7), в которой функции $h_1, \ldots, h_m$ зависят от различных переменных. Допустим, что $x_1, \ldots, x_n$ суть все переменные, от которых зависит хотя бы одна из функций $h_1, \ldots, h_m$. Если функция h_i зависит от переменных $x_{k_1}, \ldots, x_{k_i}$, то рассмотрим функцию $h'_i(x_1, \ldots, x_n)$, которая получается из функции $h_i(x_{k_1}, \ldots, x_{k_i})$ введением недостающих фиктивных переменных из множества $\{x_1, \ldots, x_n\}$:

$$h'_i(x_1, \ldots, x_n) = h_i(x_{k_1}, \ldots, x_{k_i}).$$

Понятно, что формулы (7) и

$$g(h'_1(x_1, \ldots, x_n), \ldots, h'_m(x_1, \ldots, x_n)) \tag{8}$$

реализуют одну и ту же функцию. Вместе с тем гораздо предпочтительнее рассматривать формулу (8), нежели исходную формулу (7).

Формально при совершении подобных замен мы отказываемся от функций $h_1, \ldots, h_m$, переходя, вообще говоря, к другим функциям $h'_1, \ldots, h'_m$. Однако вспомним, что мы условились рассматривать функции с точностью до фиктивных переменных. В частности, наряду с функциями $h_1, \ldots, h_m$ можно считать заданными и функции $h'_1, \ldots, h'_m$. Собственно, именно подобные технические трудности, возникающие при анализе сложных формул, и являются одной из основных причин для принятия нами соглашения о возможности рассмотрения функций с произвольным числом фиктивных переменных.

УПРАЖНЕНИЯ

6. Пусть функция $f(x_1, x_2, x_3)$ задается двоичным набором (01101001), $g_1(x_1, x_2) = x_1 \to x_2$, $g_2(x_1, x_2) = x_1 \vee x_2$. Определите, чему равны функции

$$h_1(x_1, x_2) = f(g_1(x_1, x_2), g_2(x_1, x_2), x_2),$$
$$h_2(x_1, x_2, x_3) = f(g_2(x_1, x_2), x_3, g_1(x_2, x_1)).$$

§ 5. Эквивалентность формул

Из элементарной алгебры известно, что одну и ту же функцию можно задать различными формулами. Так, например, формула (6) задает ту же функцию, что и формула

$$x_1 \cdot (x_2 + x_3) + x_2^2. \tag{9}$$

Этот факт обычно выражают в виде высказывания “формула (6) эквивалентна формуле (9)”.

Аналогично 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. $x \oplus 1 = x \to 0 = x \mid x = \overline{x}$.

5. $x \circ y = y \circ x$, где $\circ$ есть любая из функций $\cdot$, $\vee$, $\oplus$, $\mid$ (*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. $x \oplus y = (\overline{x} \cdot y) \vee (x \cdot \overline{y}) = (x \vee y) \cdot (\overline{x} \vee \overline{y})$,
$x \vee y = ((x \cdot y) \oplus x) \oplus y = \overline{x} \to y$,
$x \to y = \overline{x} \vee y = ((x \cdot y) \oplus x) \oplus 1$,
$x \mid y = \overline{x \cdot y}$.

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 правилами. Внешние скобки у формул не ставятся. При использовании отрицания скобки также не ставятся (читатель мог заметить, что мы уже применяли эти правила). 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 $\cdot$, $\oplus$, $\vee$, $\to$, $\mid$, 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:

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

Применяя подходящие эквивалентности 1–12, докажем эквивалентность формул

$$(x\overline{y}\vee\overline{x}z)\oplus((y\to z)\to\overline{x}y)\quad\text{и}\quad x\overline{y}\overline{z}\oplus y\oplus z.$$

Подформулу $x\overline{y}\vee\overline{x}z$ первой формулы преобразуем с использованием второй из эквивалентностей 12:

$$x\overline{y}\vee\overline{x}z=x\overline{y}\cdot\overline{x}z\oplus x\overline{y}\oplus\overline{x}z.$$

Применяя коммутативность конъюнкции и свойство $x\cdot\overline{x}=0$, получаем

$$x\overline{y}\cdot\overline{x}z\oplus x\overline{y}\oplus\overline{x}z=x\overline{y}\oplus\overline{x}z.$$

Таким образом,

$$x\overline{y}\vee\overline{x}z=x\overline{y}\oplus\overline{x}z. \tag{10}$$

При рассмотрении второй части $(y\to z)\to\overline{x}y$ первой из исходных формул дважды применяем третью из эквивалентностей 12:

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

Формулу $\overline{\overline{y}\vee z}$ упрощаем с помощью правила де Моргана и первой из эквивалентностей 3:

$$\overline{\overline{y}\vee z}=y\overline{z}.$$

Следовательно, получаем

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

В правой части этой эквивалентности меняем местами $\overline{x}$ и y (коммутативность конъюнкции), “выносим за скобку” y (применяем эквивалентность 7 справа налево), меняем местами $\overline{z}$ и $\overline{x}$ (коммутативность дизъюнкции) и используем затем вторую из эквивалентностей 12:

$$y\overline{z}\vee\overline{x}y=(\overline{x}\vee\overline{z})y=(\overline{x}\overline{z}\oplus\overline{x}\oplus\overline{z})y. \tag{11}$$

Пользуясь дистрибутивностью конъюнкции относительно сложения по модулю 2 и складывая по модулю 2 выражения (10) и (11), получаем, что первая формула эквивалентна формуле

$$x\overline{y}\oplus\overline{x}z\oplus\overline{x}y\overline{z}\oplus\overline{x}y\oplus y\overline{z}.$$

Заменяя в ней $\overline{x}$, $\overline{y}$, $\overline{z}$ на $x\oplus1$, $y\oplus1$, $z\oplus1$ и применяя дистрибутивность конъюнкции относительно сложения по модулю 2, приходим к формуле

$$\begin{aligned}x\overline{y}\oplus\overline{x}z\oplus\overline{x}y\overline{z}\oplus\overline{x}y\oplus y\overline{z}=xy\oplus x\oplus xz\oplus z\oplus xyz\oplus xy\oplus\\ \oplus yz\oplus y\oplus xy\oplus y\oplus yz\oplus y=xyz\oplus xy\oplus xz\oplus x\oplus y\oplus z.\end{aligned}\tag{12}$$

Нетрудно убедиться в том, что вторая формула, $x\overline{y}\overline{z}\oplus y\oplus z$, также приводится к виду (12).

УПРАЖНЕНИЯ

7. Используя эквивалентности 1–12, докажите эквивалентность следующих формул:

$$(x \oplus yz) \to (\overline{x} \to (y \to z)) \quad \text{и} \quad x \to ((y \to z) \to x);$$
$$(\overline{x} \vee \overline{y}z) \to ((x \to y) \to ((y \vee z) \to \overline{x})) \quad \text{и} \quad (x \to y) \to (\overline{y} \to \overline{x}).$$

8. Выясните, при каких n $(n \geqslant 3)$ эквивалентны формулы

$$x_1 \to (x_2 \to (x_3 \to \ldots \to (x_{n-1} \to x_n)\ldots)),$$
$$(\ldots((x_1 \to x_2) \to x_3) \to \ldots \to x_{n-1}) \to x_n.$$

§ 6. Замыкание. Замкнутые классы

Одной из центральных проблем в теории булевых функций является проблема выразимости. В общем виде ее можно сформулировать следующим образом. 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 другими с помощью формул называют операцией *суперпозиции* функций. Соответственно этому множество $[F]$ называют *замыканием* множества F относительно (операции) суперпозиции или просто замыканием F. Из определения легко усматриваются следующие свойства замыкания.

1. F содержится в $[F]$.
2. $[[F]] = [F]$.
3. Если F_1 содержится в F_2, то $[F_1]$ содержится в $[F_2]$.

Если для множества булевых функций F выполняется равенство $F = [F]$, то F называют *замкнутым множеством* или *замкнутым классом*.

Рассмотрим некоторые примеры замкнутых классов. Прежде всего, очевидно, что замкнутым классом является множество P_2 всех булевых функций. Следующий наш пример связан с селекторными функциями. Обозначим через U_{01} множество всех селекторных функ-

ций $e_i^n(x_1, \ldots, x_n)$ $(1 \leqslant i \leqslant n,\ n = 1, 2, \ldots)$. 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, тождественно равных 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, как говорят, *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 переменную можно рассматривать как тождественную функцию (из класса T_0), то так же, как и в § 4, все выражения $A_1, \ldots, A_n$ можно считать функциями 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 имеем

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

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 $\bar{e}_i^n(x_1, \ldots, x_n)$, где

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

В самом деле, 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.

С понятием замыкания тесно связано понятие полноты. Пусть 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. *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 (конечный) способ описания замкнутых классов. Один из таких способов подсказывается понятием 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 различные количества функций.

УПРАЖНЕНИЯ

9. Покажите, что замкнутыми классами являются объединение C классов C_0 и C_1, объединение U_0 классов U_{01} и C_0, объединение U_1 классов U_{01} и C_1.

10. Выясните, являются ли замкнутыми классами следующие множества функций:

а) $\{x_1 \cdot \ldots \cdot x_n,\ n = 1, 2, \ldots\}$;

б) $\{x_1 \oplus \ldots \oplus x_n,\ n = 1, 2, \ldots\}$;

в) $\{0, x_1 \vee \ldots \vee x_n,\ n = 1, 2, \ldots\}$.

11. Верно ли, что объединение двух замкнутых классов всегда является замкнутым классом?

§ 7. Разложение булевой функции по переменной

Следующее утверждение имеет фундаментальное значение для всей теории булевых функций.

Т е о р е м а 2 (о разложении функции по первой переменной). *Для любой булевой функции $f(x_1, \ldots, x_n)$ справедливо представление*

$$f(x_1, \ldots, x_n) = x_1 \cdot f(1, x_2, \ldots, x_n) \vee \overline{x}_1 \cdot f(0, x_2, \ldots, x_n). \qquad (13)$$

Д о к а з а т е л ь с т в о. Возьмем произвольный двоичный набор $a = (a_1, \ldots, a_n)$ и сравним значения левой и правой частей равенства (13) 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.

Разумеется, в теореме 2 вместо первой переменной с равным успехом можно выбрать любую другую переменную.

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

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

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

С л е д с т в и е 1 (о разложении функции по первым m переменным). *Для любой булевой функции $f(x_1, \ldots, x_n)$ и любого m $(1 \leqslant$*

$\leqslant m \leqslant n$) *имеет место представление*

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_m)} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n). \tag{14}$$

Выражение $(\sigma_1, \ldots, \sigma_m)$ под знаком дизъюнкции в формуле (14) 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 (14) имеет вид

$$x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma_1, \ldots, \sigma_n). \tag{15}$$

Если $f(\sigma_1, \ldots, \sigma_n) = 0$, то слагаемое (15) равно 0. Поэтому в формуле (14) его можно опустить (исключение составляет единственный случай, когда функция f тождественно равна 0; тогда формула (14) вырождается в константу 0). Если же $f(\sigma_1, \ldots, \sigma_n) = 1$, то вместо формулы (15) 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*

$$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}. \tag{16}$$

Равенство $f(\sigma_1, \ldots, \sigma_n) = 1$ в формуле (16) говорит о том, что в формуле (16) 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 (16) 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 конъюнкий, конъюнкции могут состоять из различных переменных и иметь различную

длину. Так, первая из формул

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

есть СДНФ, вторая — ДНФ. Обе формулы реализуют одну и ту же функцию $x \to y$. На этом 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 (16) 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 2.

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

Используя следствие 3 и теорему 1, докажем полноту следующих систем функций:

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

Полнота первых двух систем вытекает из полноты системы $\{\overline{x},\ xy,\ x \vee y\}$, теоремы 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 и соотношения $\overline{x} = x \oplus 1$. Полнота четвертой системы следует из полноты системы $\{\overline{x}, xy\}$ и соотношений

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

УПРАЖНЕНИЯ

12. Разложите по переменным x, z функцию $xyz \oplus xz \oplus y \oplus z \oplus 1$.

13. Постройте СДНФ для функции $\overline{x} \vee y\overline{z}$.

14. Докажите полноту систем функций

$$\{\overline{x}, x \to y\}, \quad \{0, x \to y\}, \quad \{0, x \oplus y \oplus 1, x \vee y\}, \quad \{1, \overline{x}, xy \vee xz \vee yz\}.$$

§ 8. Двойственность. Принцип двойственности

Каждому, кто знакомится с булевыми функциями, довольно быстро приходит в голову следующая мысль. Элементы 0, 1 множества B 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

$$g(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n). \tag{17}$$

Это равенство следует понимать так. Чтобы найти значение функции g на наборе $(a_1, \ldots, a_n)$, необходимо сначала образовать "противоположный" набор $(\overline{a}_1, \ldots, \overline{a}_n)$, затем найти значение $f(\overline{a}_1, \ldots, \overline{a}_n)$ и в заключение инвертировать его с помощью отрицания.

Функция, двойственная к функции $f(x_1, \ldots, x_n)$, обозначается через $f^*(x_1, \ldots, x_n)$. Из определения (17) двойственной функции и тождества $\overline{\overline{x}} = x$ нетрудно вывести, 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	$x \vee y$
$x \oplus y$	$x \oplus y \oplus 1 = \overline{x \oplus y}$
$x \to y$	$\overline{x \vee \overline{y}} = \overline{x}y = \overline{y \to x}$
$x \mid y$	$\overline{x \vee y} = \overline{x}\,\overline{y}$

Важную роль в теории булевых функций играет следующий принцип двойственности.

Если функция f реализуется формулой Φ, составленной из функций $g_1, \ldots, g_m$, то двойственная функция f^* реализуется формулой Φ^*, которая получается из формулы Φ заменой каждого вхождения функции g_i $(1 \leqslant i \leqslant m)$ соответствующей двойственной функцией g_i^*.

Чтобы убедиться в справедливости принципа двойственности, достаточно рассмотреть самый простой этап в определении формул, когда

$$f(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)). \tag{18}$$

Согласно исходному определению двойственной функции имеем

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

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

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

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

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

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

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

Покажем на примерах, как работает принцип двойственности. При этом будем пользоваться двойственными функциями из табл. 4:

$$(x\overline{y}z \vee \overline{x}y\overline{z} \vee \overline{x}\overline{y}z)^* = (x \vee \overline{y} \vee z)(\overline{x} \vee y \vee \overline{z})(\overline{x} \vee \overline{y} \vee z),$$

$$(\overline{x}y\overline{z} \oplus (\overline{y}z \vee xy\overline{z}))^* = (\overline{x} \vee y \vee \overline{z}) \oplus (\overline{y} \vee z)(x \vee y \vee \overline{z}) \oplus 1,$$

$$((x \to \overline{y})(\overline{x} \to z) \oplus (\overline{y}z \to x\overline{z}))^* =$$
$$= (\overline{\overline{y} \to x} \vee \overline{z \to \overline{x}}) \oplus \overline{(x \vee \overline{z}) \to (\overline{y} \vee z)} \oplus 1.$$

На практике принцип двойственности чаще всего применяют следующим образом. Если уже установлено некоторое утверждение о булевых функциях $f, g, \ldots$ и множествах булевых функций $F, G, \ldots$, в котором фигурируют лишь понятия, базирующиеся на формулах, то по принципу двойственности будет справедливо аналогичное утверждение о булевых функциях $f^*, g^*, \ldots$ и множествах булевых функций $F^*, G^*, \ldots$. 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), на основании принципа двойственности мы 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 2 и ее следствий можно доказать несколько интересных утверждений. Во-первых, имеет место следующий аналог теоремы 2.

Т е о р е м а $2'$. *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.

УПРАЖНЕНИЯ

15. Докажите, что функция $f(x_1, \ldots, x_n)$ существенно зависит от переменной x_i в том и только том случае, когда от переменной x_i существенно зависит функция $f^*(x_1, \ldots, x_n)$.

16. Выясните, верно ли, что СКНФ для булевой функции f можно построить следующим образом: сначала построить СДНФ для функции f^*, а затем в полученной СДНФ заменить $\vee$ на $\cdot$ и $\cdot$ на $\vee$.

§ 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*. Общий вид полинома Жегалкина для функции от n переменных может быть записан следующим образом:

$$\sum a_{i_1 \ldots i_s} \cdot x_{i_1} \cdot \ldots \cdot x_{i_s}. \tag{19}$$

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 $a_{i_1\dots i_s}$ принимают значения 0 или 1; при $a_{i_1\dots i_s}=0$ соответствующее слагаемое в полиноме (19) опускают. Наконец, если все коэффициенты $a_{i_1\dots i_s}$, включая коэффициент $a_\varnothing$, равны 0, то полином (19) записывают просто как 0.

Эквивалентность $x\vee y=\overline{\overline{x}\cdot\overline{y}}$ можно переписать в виде

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

Раскрывая в этом равенстве скобки и пользуясь соотношением $1\oplus 1=0$, получаем полином Жегалкина для функции $x\vee y$:

$$x\vee y=xy\oplus x\oplus y.$$

Аналогичным способом можно построить полиномы Жегалкина для функций $x\to y$ и $x\mid y$:

$$(x\to y)=xy\oplus x\oplus 1,\quad (x\mid y)=xy\oplus 1.$$

Интересно выглядит процесс построения полинома Жегалкина для функции $xy\vee xz\vee yz$:

$$\begin{aligned}xy\vee xz\vee yz&=(xy\cdot xz\oplus xy\oplus xz)\vee yz=(xyz\oplus xy\oplus xz)\vee yz=\\&=(xyz\oplus xy\oplus xz)\cdot yz\oplus xyz\oplus xy\oplus xz\oplus yz=\\&=xyz\cdot yz\oplus xy\cdot yz\oplus xz\cdot yz\oplus xyz\oplus xy\oplus xz\oplus yz=\\&=xyz\oplus xyz\oplus xyz\oplus xyz\oplus xy\oplus xz\oplus yz=xy\oplus xz\oplus yz.\end{aligned}$$

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 $a_0,\dots,a_7$:

$$f(x,y,z)=a_0\oplus a_1x\oplus a_2y\oplus a_3z\oplus a_4xy\oplus a_5xz\oplus a_6yz\oplus a_7xyz. \quad (20)$$

Подставляя в функцию $f(x,y,z)$ последовательно наборы $(0,0,0)$, $(0,0,1),\dots,(1,1,1)$ и пользуясь известными значениями функции f, из (20) получаем следующую систему уравнений для коэффициентов $a_0,\dots,a_7$ (слева в скобках указан набор значений переменных x, y, z, приводящий к данному соотношению):

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

Решим ее, исключая последовательно неизвестные $a_0, \ldots, a_7$. Первое уравнение дает $a_0 = 1$, второе, третье и пятое — $a_1 = 0$, $a_2 = a_3 = 1$. Используя далее найденные значения коэффициентов a_0, a_1, a_2, a_3, рассматриваем четвертое, шестое и седьмое уравнения. Из них находим $a_4 = a_6 = 0$, $a_5 = 1$. Подставляя полученные значения в восьмое уравнение, получаем $a_7 = 0$. Окончательно полином Жегалкина для функциии $f(x, y, z)$ имеет вид $1 \oplus y \oplus z \oplus xz$.

Довольно неожиданно оказывается, что для любой булевой функции имеется единственный полином Жегалкина, если только полиномы Жегалкина рассматривать с точностью до перестановок слагаемых и сомножителей в слагаемых. В самом деле, подсчитаем число коэффициентов $a_{i_1 \ldots i_s}$ в общей формуле (19) полинома Жегалкина для функции от n переменных. Это число равно числу всевозможных подмножеств (включая пустое) множества $\{1, 2, \ldots, n\}$. В свою очередь подмножества множества $\{1, 2, \ldots, n\}$ взаимно однозначным образом соответствуют двоичным наборам длины n: единица, стоящая в наборе на i-м слева месте, свидетельствует о том, что в рассматриваемое подмножество входит число i, нуль — что число i в подмножество не входит.

Понятно, что число различных полиномов Жегалкина вида (19) (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 (19). Поскольку этих коэффициентов имеется 2^n, мы 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 и, 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.

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 $f(x_1, \ldots, x_n)$ (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 Жегал-

кина Ф, 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 $f(x_1, \ldots, x_n)$.

УПРАЖНЕНИЯ

17. Определите при любом n, какую булеву функцию реализует полином Жегалкина (19), если все коэффициенты $a_{i_1 \ldots i_s}$ (включая коэффициент $a_\varnothing$) равны 1.

18. Методом неопределенных коэффициентов постройте полином Жегалкина для функции $f(x, y, z, w)$, заданной набором

(1010101111011000).

Глава II

ЗАМКНУТЫЕ КЛАССЫ И ПОЛНОТА

§ 1. Класс самодвойственных функций

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

$$f(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n). \tag{21}$$

Для самодвойственной функции $f(x_1, \ldots, x_n)$ равенство (21) 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 $e_i^n(x_1, \ldots, x_n)$.

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 (18). Однако это непосредственно следует из принципа двойственности.

На примере самодвойственных функций интересно еще раз проследить идею подсчета функций от n переменных с помощью таблицы. Внимательно 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, необ-

ходимое для ее решения, имеет также и некоторый самостоятельный интерес.

Лемма 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

$$f(a_1, \ldots, a_n) = f(\overline{a}_1, \ldots, \overline{a}_n). \tag{22}$$

Подставим в функцию $f(x_1, \ldots, x_n)$ вместо переменной x_i $(1 \leqslant i \leqslant n)$ функцию x, если $a_i = 1$, и функцию $\overline{x}$, если $a_i = 0$. Полученную после подстановки функцию обозначим через $g(x)$. Согласно определению

$$g(x) = f(x^{a_1}, \ldots, x^{a_n}),$$

где, напомним, через x^1 обозначена функция x, а через x^0 функция $\overline{x}$. Имеем теперь

$$g(0) = f(0^{a_1}, \ldots, 0^{a_n}), \quad g(1) = f(1^{a_1}, \ldots, 1^{a_n}). \tag{23}$$

Поскольку

$$0^0 = \overline{0} = 1^1 = 1, \quad 0^1 = 1^0 = \overline{1} = 0,$$

из равенств (23) заключаем, что

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

Обращение к равенству (22) завершает доказательство леммы.

Пусть функция $f(x_1, x_2, x_3)$ определена формулой $x_1\overline{x}_2 \vee \overline{x}_1 x_3 \vee \vee \overline{x}_2\overline{x}_3$. Из нее видно, что $f(0, 1, 1) = f(1, 0, 0) = 1$. Соответствующие этим противоположным наборам подстановки $f(\overline{x}, x, x)$ и $f(x, \overline{x}, \overline{x})$ дают константу 1.

УПРАЖНЕНИЯ

19. Проверьте, что самодвойственными являются функции

$x \oplus y \oplus z$, $\quad x \oplus y \oplus z \oplus 1$, $\quad xy \vee xz \vee yz$, $\quad xy \vee x\overline{z} \vee y\overline{z}$, $\quad x\overline{y} \vee x\overline{z} \vee \overline{y}\overline{z}$.

Докажите, что не существует самодвойственных функций $f(x_1, x_2)$, существенно зависящих от обеих переменных.

§ 2. Класс линейных функций

Булеву функцию $f(x_1, \ldots, x_n)$ назовем *линейной*, если в ее полиноме Жегалкина (19) отсутствуют нелинейные слагаемые (т.е. слагаемые, содержащие не менее двух сомножителей).

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

$$a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n, \tag{24}$$

где коэффициенты $a_0, a_1, \ldots, a_n$ равны 0 или 1. Представление (24) 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 (проверьте!) линейные функции. Следовательно, число линейных функций, зависящих от переменных $x_1, \ldots, x_n$, равно числу двоичных наборов длины $n+1$. Последнее число, как мы знаем, есть 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.

Множество всех линейных булевых функций обозначим через L. Убедимся, что L является замкнутым классом. Пусть функции

$$g_0(y_1, \ldots, y_m),\ g_1(x_1, \ldots, x_n),\ \ldots,\ g_m(x_1, \ldots, x_n)$$

линейны, т.е.

$$\begin{gathered} g_0(y_1, \ldots, y_m) = b_0 \oplus b_1 y_1 \oplus \ldots \oplus b_m y_m, \\ g_1(x_1, \ldots, x_n) = a_{10} \oplus a_{11} x_1 \oplus \ldots \oplus a_{1n} x_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_m(x_1, \ldots, x_n) = a_{m0} \oplus a_{m1} x_1 \oplus \ldots \oplus a_{mn} x_n, \end{gathered}$$

а функция $f(x_1, \ldots, x_n)$ представима формулой (18). Тогда

$$\begin{aligned} f(x_1, \ldots, x_n) = b_0 \oplus b_1(a_{10} \oplus a_{11} x_1 \oplus \ldots \oplus a_{1n} x_n) \oplus \ldots \\ \ldots \oplus b_m(a_{m0} \oplus a_{m1} x_1 \oplus \ldots \oplus a_{mn} x_n) = \\ = (b_0 \oplus b_1 a_{10} \oplus \ldots \oplus b_m a_{m0}) \oplus (b_1 a_{11} \oplus \ldots \oplus b_m a_{m1})\, x_1 \oplus \ldots \\ \ldots \oplus (b_1 a_{1n} \oplus \ldots \oplus b_m a_{mn})\, x_n. \end{aligned}$$

Если обозначить значения выражений

$$b_0 \oplus b_1 a_{10} \oplus \ldots \oplus b_m a_{m0},\ b_1 a_{11} \oplus \ldots \oplus b_m a_{m1},\ \ldots,\ b_1 a_{1n} \oplus \ldots \oplus b_m a_{mn}$$

(которые являются константами 0 или 1) соответственно через a_0, $a_1, \ldots, a_n$, то мы придем к формуле (24), определяющей функцию $f(x_1, \ldots, x_n)$.

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 $n \geqslant 2$; а поскольку у нас в распоряжении имеются константы 0 и 1 — также и любую функцию вида $x_1 \oplus \ldots \oplus x_{n-1}$ и $x_1 \oplus \ldots \oplus x_{n-1} \oplus 1$.

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 приемом служит разложение функции в полином Жегалкина. Однако в некоторых случаях о нелинейности функции можно судить по виду двоичного набора, задающего функцию. Так, отличная от константы булева функция будет заведомо нелинейной, если значение 1 (или значение 0) она принимает не на половине всех наборов. Это утверждение мы докажем от противного: если булева функция $f(x_1, \ldots, x_n)$ линейна и отлична от константы, то значение 1 (и значение 0) она принимает ровно на 2^{n-1} наборах.

Итак, пусть функция $f(x_1, \ldots, x_n)$ линейна и отлична от константы. Тогда она существенно зависит по крайней мере от одной из переменных $x_1, \ldots, x_n$. Пусть это будет, например, переменная x_n. Тогда функцию $f(x_1, \ldots, x_n)$ можно представить в виде

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_{n-1} x_{n-1} \oplus x_n. \tag{25}$$

При $n = 1$ функция $f(x_1)$ совпадает с одной из функций x_1, $x_1 \oplus 1$ и утверждение проверяется непосредственно. Предположим далее, что $n \geqslant 2$. Опираясь на представление (25), заключаем, что функция $f(x_1, \ldots, x_n)$ принимает значение 1 только в двух случаях: либо линейная функция

$$a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_{n-1} x_{n-1} = f(x_1, \ldots, x_{n-1}, 0) \tag{26}$$

принимает значение 0 и $x_n = 1$, либо линейная функция (26) принимает значение 1 и $x_n = 0$. Отсюда сразу следует, что число наборов, на которых функция f принимает значение 1, равно сумме числа наборов, на которых функция (26) принимает значение 0, и числа наборов, на которых функция (26) принимает значение 1. Очевидно, что указанная сумма равна 2^{n-1} — числу всех двоичных наборов длины $n - 1$.

В дальнейшем при решении проблемы полноты в классе P_2 нам понадобится утверждение о возможности понижения числа переменных в нелинейной функции. Это утверждение носит название *лемма о нелинейной функции.*

Лемма 2. *Из всякой нелинейной булевой функции подстановкой констант* 0 *и* 1 *вместо некоторых переменных можно получить нелинейную функцию от двух переменных.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — нелинейная функция. Поскольку все булевы функции от одной переменной линейны, имеем $n \geqslant 2$. При $n = 2$ утверждение тривиально (можно применить "пустую" подстановку). Пусть $n > 2$. Выберем в полиноме Жегалкина функции $f(x_1, \ldots, x_n)$ нелинейное слагаемое наименьшей степени. Чтобы не применять громоздких обозначений, будем предполагать, что это слагаемое имеет вид $x_1 \cdot \ldots \cdot x_m$ $(2 \leqslant m \leqslant n)$. Подставим в функцию $f(x_1, \ldots, x_n)$ константу 0 вместо всех переменных $x_{m+1}, \ldots, x_n$ (можно считать, что константа 0 зависит от пе-

ременной x_1). Ввиду минимальности степени слагаемого $x_1 \cdot \ldots \cdot x_m$ полином Жегалкина функции $f(x_1, \ldots, x_m, 0, \ldots, 0)$ примет вид

$$x_1 \cdot \ldots \cdot x_m \oplus a_m x_m \oplus \ldots \oplus a_1 x_1 \oplus a_0.$$

Если $m > 2$, то подставим далее константу 1 вместо всех переменных $x_3, \ldots, x_m$. В итоге придем к функции, полином Жегалкина которой имеет вид

$$x_1 x_2 \oplus b_2 x_2 \oplus b_1 x_1 \oplus b_0.$$

Лемма доказана.

УПРАЖНЕНИЯ

20. Покажите, что функция, двойственная к линейной, также будет линейной. Покажите, что линейные функции вида $a \oplus x_1 \oplus \ldots \ldots \oplus x_{2n+1}$ являются самодвойственными.

21. Докажите, что при любом n $(n \geqslant 3)$ существует нелинейная функция от n переменных, которая принимает значение 1 ровно на 2^{n-1} наборах. Существенно ли в этом утверждении ограничение $n \geqslant 3$?

§ 3. Класс монотонных функций

Что такое монотонно не убывающая функция? Это функция, значения которой не убывают с ростом значений аргумента. Если вы дадите такой ответ на поставленный вопрос, то в общем-то будете правы. Трудности с монотонными функциями начинаются тогда, когда основное множество, на котором определена функция, как говорят, не является линейно упорядоченным либо когда рассматриваются функции многих переменных. Обе эти возможности нередко соседствуют друг с другом. Однако в случае булевых функций исходное множество B линейно упорядочено $(0 < 1)$, и потому проблема остается лишь с определением монотонных функций от нескольких переменных.

Приводимое ниже определение монотонной функции по существу представляет собой определение функции, монотонной по любой из своих переменных.

Начнем с введения (частичного) порядка на множестве B^n всех двоичных наборов длины n. Говорим, 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 $a_i \leqslant b_i$. Если набор $(a_1, \ldots, a_n)$ не превосходит набора $(b_1, \ldots, b_n)$, то этот факт записываем в виде

$$(a_1, \ldots, a_n) \leqslant (b_1, \ldots, b_n). \tag{27}$$

Отметим, что при $n \geqslant 2$ введенное отношение определено не для любых двух наборов длины n. Так, например, наборы $(0,1)$ и $(1,0)$ невозможно сравнить относительно этого отношения. Именно поэтому введенное отношение является частичным.

Булева функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если для любых двух наборов $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ из того, что выполняется неравенство (27), следует, что выполняется неравенство

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

Множество всех монотонных булевых функций обозначим через M. Непосредственная проверка показывает, что множеству M принадлежат функции 0, 1, x, xy, $x \vee y$ и не принадлежат функции $\overline{x}$, $x \oplus y$, $x \to y$, $x \mid y$.

Для проверки монотонности булевых функций от небольшого числа переменных часто используют задание булевых функций с помощью диаграммы, на которой представлен частичный порядок на множестве B^n. Каждому набору из B^n отвечает точка на этой диаграмме, а различные точки соединяются отрезком прямой в том и только том случае, когда эти точки соответствуют наборам, различающимся ровно в одной компоненте (рис. 1). Обычно точки на диаграмме изображают "слоями". При этом каждый "слой" диаграммы состоит из точек, которые отвечают двоичным наборам с одним и тем же числом единичных компонент. Следовательно, если число единиц в наборе $a = (a_1, \ldots, a_n)$ меньше числа единиц в наборе $b = (b_1, \ldots, b_n)$, то набор b расположен в диаграмме выше набора a. Если же еще для наборов a, b выполняется соотношение (27), то от набора a в диаграмме можно "подняться" до набора b по отрезкам прямых.

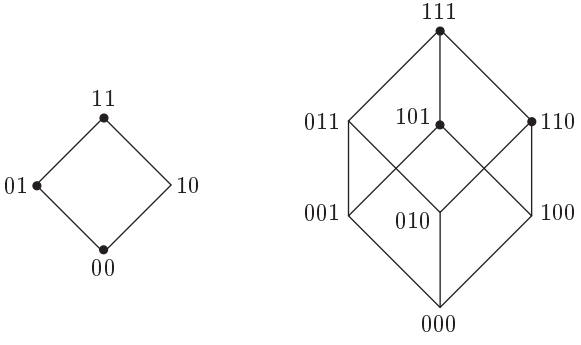

Рис. 1

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 B^2 представлена функция $x \to y$, а на диаграмме множества B^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 B^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 (18). Пусть для наборов $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ выполняется соотношение (27). 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 (18) это означает, что

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

и монотонность функции f установлена.

Любопытный вариант теоремы 2 о разложении имеет место для монотонных функций.

Т е о р е м а 3. *Для любой монотонной булевой функции* $f(x_1, \ldots, x_n)$ *справедливо представление*

$$f(x_1, \ldots, x_n) = x_1 \cdot f(1, x_2, \ldots, x_n) \vee f(0, x_2, \ldots, x_n). \qquad (28)$$

Д о к а з а т е л ь с т в о. Пусть $a = (a_1, \ldots, a_n)$ — произвольный двоичный набор. Для набора a найдем значения левой и правой частей равенства (28). 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 (28) получаем

$$f(1, a_2, \ldots, a_n) \vee f(0, a_2, \ldots, a_n). \qquad (29)$$

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 (29) есть $f(1, a_2, \ldots, a_n)$. Теорема доказана.

Заметим, что в формуле (28) 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 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

$$f(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot f(1, 1, x_3, \ldots, x_n) \vee x_1 \cdot f(1, 0, x_3, \ldots, x_n) \vee \\ \vee x_2 \cdot f(0, 1, x_3, \ldots, x_n) \vee f(0, 0, x_3, \ldots, x_n).$$

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.*

Следствие 1 позволяет сделать важный вывод о системе функций, порождающей класс M.

Следствие 2. *Класс M порождается системой функций* $\{0, 1, xy, x \vee y\}$.

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

Лемма 3. *Из немонотонной функции путем подстановки констант* 0 *и* 1 *на места некоторых 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 (27) и $f(a) = 1$, $f(b) = 0$. Покажем, что наборы a, b можно считать соседними, т.е. различающимися ровно в одной компоненте. В самом деле, предположим, что это не так и наборы a, b различаются в t компонентах, где $t > 1$. Пусть, например, $a_i = 0$, $b_i = 1$ (вариант $a_i = 1$, $b_i = 0$ не может реализоваться в силу неравенства (27)). Рассмотрим набор $c = (a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$. Он отличается от набора a в одной компоненте и от набора b в $t - 1$ компонентах. Кроме того, $a \leqslant c$ и $c \leqslant b$. Если $f(c) = 0$, то вместо набора b можно взять набор c. Если же $f(c) = 1$, то набор a следует заменить на набор c и вновь повторить описанную выше процедуру. Не более чем через $t - 1$ шагов мы придем к паре соседних наборов с требуемыми свойствами.

Итак, считаем, что наборы a и b различаются только в одной компоненте. Пусть это будет первая компонента. Тогда $a_2 = b_2, \ldots, a_n = b_n$ и, следовательно, подстановка констант $a_2, \ldots, a_n$ на места переменных $x_2, \ldots, x_n$ в функцию $f(x_1, \ldots, x_n)$ дает функцию $g(x_1) = f(x_1, a_2, \ldots, a_n)$ такую, что $g(0) = 1$ и $g(1) = 0$. Лемма доказана.

УПРАЖНЕНИЯ

22. Проверьте на монотонность функцию $xyz(x \to y)(x \to z)$. С использованием диаграммы множества B^3 найдите число монотонных функций от трех переменных.

23. Покажите, что из монотонности функции f следует монотонность функции f^*.

24. Найдите все монотонные линейные функции.

§ 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; его предложил американский математик Э. Пост еще в 1921 г. Способ основан на проверке пяти свойств: невхождении системы булевых функций полностью ни в один из замкнутых классов

$$T_0, \quad T_1, \quad S, \quad M, \quad L. \tag{30}$$

Точнее говоря, имеет место следующий критерий полноты в классе P_2.

Теорема 4. *Система булевых функций Q полна в P_2 тогда и только тогда, когда Q целиком не содержится ни в одном из классов* (30).

Доказательство. Необходимость. Пусть система функций Q полна в P_2. Тогда $[Q] = P_2$. Если бы система Q целиком содержалась в одном из классов (30) (обозначим этот класс через R), то по свойству 3 замыкания выполнялось бы равенство $[R] = P_2$. Однако каждый из замкнутых классов (30) отличен от класса P_2. Поэтому система Q целиком не содержится ни в одном из классов (30).

Достаточность. Пусть система Q целиком не содержится ни в одном из классов (30). Обозначим через f_1, f_2, f_3, f_4, f_5 функции системы Q, которые не входят соответственно в классы T_0, T_1, S, M, L (некоторые из функций $f_1, \ldots, f_5$ могут совпадать). Покажем, что суперпозициями функций $f_1, \ldots, f_5$ можно получить функции $\overline{x}$, xy, которые, как нам известно, образуют полную в P_2 систему. Тогда по теореме 1 полной будет система $\{f_1, \ldots, f_5\}$ и, следовательно, система Q.

Получим сначала из функций f_1, f_2, f_3 константы 0 и 1. Из того, что f_1 не входит в класс T_0, следует, что $f_1(0, \ldots, 0) = 1$. Значит, если положить

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

то функция $g_1(x)$ будет совпадать с одной из функций 1, $\overline{x}$. Если $g_1(x)$ — константа 1, то, пользуясь соотношением $f_2(1, \ldots, 1) = 0$,

получаем константу 0:

$$f_2(g_1(x), \ldots, g_1(x)) = 0.$$

Пусть $g_1(x) = \overline{x}$. Тогда, применяя лемму о несамодвойственной функции к функции f_3, подстановками 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, с помощью леммы о немонотонной функции, примененной к функции f_4, строим функцию $\overline{x}$, а с помощью леммы о нелинейной функции, примененной к функции f_5, строим нелинейную функцию $g_2(x, y)$. Рассмотрим далее 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

$$g_2(x, y) = xy \oplus x = x(y \oplus 1) = x\overline{y}.$$

Следовательно, в этом случае $g_2(x, \overline{y}) = xy$. Аналогично рассматривается случай, когда $a_1 = 0$ и $a_2 = 1$. Наконец, если $a_1 = a_2 = 1$, то

$$g_2(x, y) = xy \oplus x \oplus y = x \vee y.$$

В этом случае

$$\overline{g}_2(\overline{x}, \overline{y}) = xy.$$

Теорема доказана.

Из теоремы 4 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. А нельзя ли в общем случае уменьшить это число до четырех? Оказывается, можно. Действительно, пусть функции $f_1, \ldots, f_5$ выбраны так, как указано в доказательстве теоремы. Рассмотрим функцию f_1. Согласно выбору этой функции имеем $f_1(0, \ldots, 0) = 1$. Если $f_1(1, \ldots, 1) = 1$, то функция f_1 несамодвойственна (на противоположных наборах $(0, \ldots, 0)$ и $(1, \ldots, 1)$ она принимает одно и то же значение 1). Поэтому функцию f_3 можно заменить функцией f_1. Если же $f_1(1, \ldots, 1) = 0$, то функция f_1 немонотонна. Значит, в этом случае функцией f_1 можно заменить функцию f_4.

Итак, мы приходим к следующему утверждению.

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

Можно ли продвинуться в этом направлении дальше, понизив оценку до трех? Следующий пример показывает, что, вообще говоря, этого сделать нельзя.

Пусть

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

Пользуясь, например, теоремой 4, 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 лежит в 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 нельзя исключить из системы, не нарушив при этом условий полноты.

УПРАЖНЕНИЯ

25. Постройте пример базиса в классе P_2, состоящего из трех функций.

26. Докажите, что булева функция f, не принадлежащая ни одному из классов T_0, T_1, S, является базисом класса P_2. Будет ли справедливо аналогичное утверждение, если вместо класса S взять класс L?

§ 5. Замкнутые классы, содержащие константы

Как велико число замкнутых классов? Можно ли каким-либо эффективным способом перечислить все замкнутые классы?

Американский математик Э. Пост установил, что число замкнутых классов в P_2 бесконечно. Тем не менее, существует эффективная процедура перечисления всех замкнутых классов с помощью конечных порождающих систем функций. Изложение этих результатов в полном объеме хотя и не требует специальных знаний, но выходит за рамки данной брошюры [2]). Мы решим более скромную задачу: найдем все замкнутые классы, содержащие обе константы 0 и 1.

[2]) Заинтересованному читателю можно посоветовать обратиться к книгам: *Яблонский С.В.*, *Гаврилов Г.П.*, *Кудрявцев В.Б.* Функции алгебры логики и классы Поста.— М.: Наука, 1966; *Марченков С.С.* Замкнутые классы булевых функций.— М.: Наука, 2000. В них приведены подробные доказательства упомянутых результатов.

Из всех замкнутых классов P_2, T_0, T_1, S, M, L, которые мы изучали в предыдущих параграфах, обе константы содержат лишь классы P_2, M и L. Дадим определение еще пяти замкнутых классов, которые также содержат обе константы (с некоторыми из этих классов мы уже начали знакомиться в § 6 гл. I).

Через C обозначим класс всех булевых функций-констант (от любого числа переменных).

Через MU обозначим класс всех функций, которые являются либо константами, либо селекторными функциями.

Через U обозначим класс всех булевых функций, которые существенно зависят не более чем от одной переменной.

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

$$a_0 \vee a_1 x_1 \vee \ldots \vee a_n x_n, \tag{31}$$

где $a_0, a_1, \ldots, a_n$ — произвольные элементы из B.

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

$$a_0 \cdot (a_1 \vee x_1) \cdot \ldots \cdot (a_n \vee x_n). \tag{32}$$

Замкнутость классов C, MU, U легко вытекает из их определения (напомним еще раз, что наряду с любой булевой функцией f мы считаем одновременно заданными все функции, которые получаются из f добавлением или изъятием несущественных переменных).

Чтобы доказать замкнутость класса D, полезно иметь в виду, что при $a_0 = 1$ дизъюнкция (31) 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 (31) 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 (31) и (32) видно, что класс D порождается системой функций $\{0, 1, x \vee y\}$, а класс K — системой функций $\{0, 1, xy\}$.

Теорема 5. *Существует всего* 8 *замкнутых классов, содержащих обе константы*:

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

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 4 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 из функций, существенно зависящих не более чем от одной переменной, то непосредственная проверка показывает, что R совпадает с одним из классов C, MU, U. Пусть, далее, 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

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

где $n \geqslant 2$ и a — элемент множества B. При $n > 2$ подстановкой константы 0 вместо всех переменных $x_3, \ldots, x_n$ получаем функцию $x_1 \oplus x_2 \oplus a$, 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 $x_1 \oplus x_2 \oplus 1$:

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

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, MU, U, L.

Пусть теперь класс R состоит только из монотонных функций. Если R содержит только функции, существенно зависящие не более чем от одной переменной, то он совпадает с одним из классов C, MU (класс U содержит немонотонную функцию $\overline{x}$).

Пусть в класс R входит функция, существенно зависящая не менее чем от двух переменных. Тогда согласно лемме о нелинейной функции в класс R будет входить нелинейная функция от двух переменных. Заметим, что она монотонна, поскольку получается из монотонной функции подстановкой констант 0 и 1. Легко проверить, что нелинейными монотонными функциями от двух переменных являются лишь функции

$$xy \quad \text{и} \quad x \vee y = xy \oplus x \oplus y.$$

Поскольку системы функций

$$\{0, 1, x \vee y\} \quad \text{и} \quad \{0, 1, xy\}$$

порождают соответственно классы D и K, мы 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 след-

ствию 1 из теоремы 3 функцию $f(x_1, \ldots, x_n)$ можно представить в виде ДНФ Ф, которая не содержит отрицаний переменных. Поскольку функция $f(x_1, \ldots, x_n)$ отлична от дизъюнкции, ДНФ Ф 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 Ф 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 Ф можно было бы опустить). Таким образом, любая конъюнкция из ДНФ Ф, 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.

Довольно просто найти все замкнутые классы, которые целиком лежат в одном из классов L, D, K. Мы приведем полный перечень этих классов. Попытайтесь самостоятельно установить, что не существует других замкнутых классов, целиком лежащих в классах L, D, K.

Итак, класс L линейных функций целиком содержит замкнутые классы

$$L_0,\ L_1,\ SL,\ L_{01},\ U,\ MU,\ SU,\ U_0,\ U_1,\ U_{01},\ C,\ C_0,\ C_1,$$

где

L_0 — класс всех линейных функций, сохраняющих константу 0;

L_1 — класс всех линейных функций, сохраняющих константу 1;

SL — класс всех самодвойственных линейных функций;

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

SU — класс всех самодвойственных функций, существенно зависящих от одной переменной;

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

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

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

C_0 — класс всех функций-констант, равных 0 (от любого числа переменных);

C_1 — класс всех функций-констант, равных 1.

Класс D всех дизъюнкций целиком содержит следующие замкнутые классы:

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;

а также классы

$$MU,\ U_0,\ U_1,\ U_{01},\ C,\ C_0,\ C_1.$$

Класс K всех конъюнкций целиком содержит следующие замкнутые классы, двойственные к соответствующим классам из D:

$$K_0,\ K_1,\ K_{01},\ MU,\ U_0,\ U_1,\ U_{01},\ C,\ C_0,\ C_1.$$

Глава III

СЛОЖНОСТЬ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ

§ 1. Минимизация ДНФ

Пусть Q — полная система функций. Тогда любую булеву функцию можно реализовать формулой над Q. Как мы уже не раз видели, для некоторых полных систем Q существуют функции, которые реализуются различными формулами. (Нетрудно показать, что для любой полной системы Q и любой булевой функции f существует бесконечное число формул над Q, реализующих функцию f.) Поэтому возникает желание для любой булевой функции f найти оптимальную (в каком-либо смысле) формулу над Q, которая реализует функцию f. Вопрос этот представляется в прикладном отношении очень важным. Однако пока не сформулирован критерий оптимальности, нельзя даже утверждать, что для данной булевой функции имеется хотя бы одна оптимальная формула, реализующая эту функцию.

На практике, как правило, рассматриваются такие критерии оптимальности, для которых вопрос о существовании оптимальных формул решается тривиальным образом. Обычно для формул определяется числовая характеристика (параметр), имеющая смысл некоторой сложности, и *оптимальной формулой* называется формула с наименьшим возможным значением этого параметра. Сам процесс поиска формул наименьшей сложности носит название *минимизации формул*.

Из всех полных систем функций наиболее употребительной в вопросах минимизации является система $Q_0 = \{\overline{x},\ xy,\ x \vee y\}$. В качестве меры сложности чаще всего рассматривают две взаимосвязанные меры: число символов функций, входящих в формулу, либо число символов переменных. При этом как символы функций, так и символы переменных подсчитываются с теми кратностями, с которыми они встречаются в формуле. Так, например, в формуле

$$x_1\overline{(x_2 \vee x_3)} \vee \overline{x}_2\overline{x}_3\overline{(x_1x_2 \vee \overline{x}_4)}$$

имеется 12 символов функций и 8 символов переменных.

В этом параграфе в качестве меры сложности формул мы выбираем число символов переменных, входящих в формулу. Нетрудно понять, что для всякой булевой функции существует реализующая ее формула наименьшей сложности над системой Q_0 (таких формул может быть несколько). В самом деле, для заданной булевой функции $f(x_1, \ldots, x_n)$ можно, например, последовательно перебирать в

некотором порядке все формулы над Q_0 сложности $1, 2, \ldots$, содержащие только символы переменных $x_1, \ldots, x_n$, и сравнивать реализуемые ими функции с функцией f. Этот процесс не может продолжаться неограниченно долго, поскольку, во-первых, функцию $f(x_1, \ldots, x_n)$ всегда можно реализовать в виде совершенной ДНФ со сложностью, не превосходящей $n \cdot 2^n$. А во-вторых, количество формул над Q_0 заданной сложности конечно (количество формул сложности l заведомо меньше числа всех строк длины l, составленных из символов $(,)$, $\bar{}$, $\&$, $\vee$, $x_1, \ldots, x_n$; это число равно $(n+5)^l$).

Описанный выше тривиальный алгоритм поиска формулы наименьшей сложности относится к классу так называемых переборных алгоритмов. Отличительной особенностью этих алгоритмов является то, что для отыскания искомого объекта (в нашем случае — формулы) сложности l приходится перебирать все объекты сложности, меньшей или равной l. Обычно это приводит к тому, что переборный алгоритм при работе над входными данными размера l затрачивает около c^l шагов, где c — константа, превосходящая 1.

Если обратиться к формулам над системой Q_0, то можно показать, что число различных формул, содержащих ровно r символов переменных из множества $\{x_1, \ldots, x_n\}$, не меньше, чем $(4n)^r$. Поэтому если функция $f(x_1, \ldots, x_n)$ задана формулой сложности l, то непосредственный просмотр всех формул со сложностью k $(k \leqslant l)$ потребует не менее c_1^l шагов, где $c_1 > 1$.

В настоящее время неизвестны алгоритмы непереборного типа, осуществляющие минимизацию формул над системой Q_0 (как, впрочем, и над любой другой полной системой). Трудности, стоящие на этом пути, носят, по-видимому, принципиальный характер. Некоторое представление об этих трудностях дает пример минимизации ДНФ — формул над системой Q_0, имеющих довольно простое строение. Хотя проблема минимизации ДНФ пока также не получила окончательного удовлетворительного решения, на пути ее решения создана разветвленная система понятий и получен ряд интересных и важных результатов.

Дадим необходимые определения, используемые в теории минимизации ДНФ.

Элементарной конъюнкцией называется формула вида $x_{i_1}^{\sigma_1} \cdot \ldots \cdot x_{i_r}^{\sigma_r}$, где $\sigma_1, \ldots, \sigma_r \in \{0, 1\}$ и все переменные $x_{i_1}, \ldots, x_{i_r}$ различны. Число r называется *рангом конъюнкции*.

Дизъюнктивная нормальная форма (ДНФ) есть формула вида $K_1 \vee \ldots \vee K_t$, где $K_1, \ldots, K_t$ — различные элементарные конъюнкции (порядок сомножителей в конъюнкции роли не играет).

Минимальной ДНФ функции f называется ДНФ, которая реализует функцию f и имеет наименьшее число символов переменных среди всех ДНФ, реализующих функцию f.

Булева функция может иметь несколько минимальных ДНФ. Так, для функции $f(x, y, z)$, заданной двоичным набором (11100101), минимальными ДНФ являются

$$\overline{x}\overline{y} \vee xz \vee \overline{x}\overline{z} \quad \text{и} \quad xz \vee \overline{x}\overline{z} \vee \overline{y}z. \tag{33}$$

Как мы уже говорили, проблему минимизации ДНФ можно решить тривиальным переборным алгоритмом. Мы хотим уменьшить перебор за счет удаления некоторых элементарных конъюнкций, которые заведомо не входят ни в одну из минимальных ДНФ. С этой целью введем следующие понятия.

Пусть $f(x_1, \ldots, x_n)$ — булева функция и K — элементарная конъюнкция, все переменные которой принадлежат множеству $\{x_1, \ldots, x_n\}$. Назовем конъюнкцию K *импликантом* функции f, если функция

$$K \to f(x_1, \ldots, x_n) \tag{34}$$

тождественно равна 1, и *простым импликантом* функции f, если K — импликант функции f, но перестает быть таковым после вычеркивания из K любого сомножителя (если ранг конъюнкции K равен 1, то импликант K по определению считается простым импликантом функции f, если f не равна тождественно 1).

Из представления (34) видно, что импликант K функции f принимает значение 1 только на тех наборах, на которых равна 1 функция f (импликант K "имплицирует" единичные значения функции f). Далее, если элементарная конъюнкция K' получается из элементарной конъюнкции K вычеркиванием некоторых сомножителей, то, очевидно, функция $K \to K'$ будет тождественно равна 1, т.е. всякий двоичный набор, обращающий в 1 конъюнкцию K, будет обращать в 1 и конъюнкцию K'. Поэтому простой импликант K функции f обладает свойством максимальности: он, как говорят, покрывает наибольшее число единиц функции f (т.е. наборов, на которых функция f равна 1) среди всех импликантов функции f, которые получаются из K умножением на некоторые сомножители. Все эти соображения наводят на мысль, что простые импликанты и дизъюнкция всех простых импликантов должны играть важную роль в вопросах минимизации ДНФ.

Назовем ДНФ функции f *сокращенной*, если она представляет собой дизъюнкцию всех простых импликантов функции f.

Нетрудно заметить, что сокращенная ДНФ не обязана быть минимальной. Так, для рассмотренной выше функции (11100101) с минимальными ДНФ (33) сокращенной ДНФ будет формула

$$\overline{x}\overline{y} \vee \overline{x}\overline{z} \vee xz \vee \overline{y}z.$$

Тем не менее справедливо следующее утверждение.

Теорема 6. *Любая минимальная ДНФ булевой функции может быть получена из ее сокращенной ДНФ путем удаления некоторых конъюнкций.*

Доказательство. Достаточно установить, что любая минимальная ДНФ булевой функции f является дизъюнкцией только простых импликантов функции f. Последнее почти очевидно, поскольку, во-первых, в силу определения каждая входящая в ДНФ конъюнкция представляет собой импликант функции f. А во-вторых, если бы импликант минимальной ДНФ не был простым, то из него удалением некоторых сомножителей можно было бы получить простой импликант функции f. Как следствие, получили бы другую ДНФ с меньшим числом символов переменных. Это противоречит определению минимальной ДНФ. Теорема доказана.

Следствие. *Если некоторая конъюнкция не входит в сокращенную ДНФ функции f, то она не входит ни в одну минимальную ДНФ функции f.*

Теорема 6 показывает, что при построении минимальных ДНФ нет необходимости рассматривать произвольные импликанты — достаточно ограничиться теми, которые входят в сокращенную ДНФ.

Как мы уже убедились, сокращенная ДНФ может не быть минимальной. Однако существуют достаточно широкие классы функций, для которых эти понятия совпадают. Один из них — класс монотонных функций.

Теорема 7. *Сокращенная ДНФ монотонной функции, отличной от константы, не содержит отрицаний переменных и является ее единственной минимальной ДНФ.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — монотонная функция, отличная от константы, а конъюнкция

$$K = x_{i_1} \cdot \ldots \cdot x_{i_r} \cdot \overline{x}_{i_{r+1}} \cdot \ldots \cdot \overline{x}_{i_s}$$

является импликантом функции f, причем $s > r$. Тогда конъюнкция K, а вместе с ней и функция f, принимает значение 1 при

$$x_{i_1} = \ldots = x_{i_r} = 1, \quad x_{i_{r+1}} = \ldots = x_{i_s} = 0$$

(значения остальных переменных могут быть произвольными). Ввиду монотонности функция f будет принимать значение 1, как только $x_{i_1} = \ldots = x_{i_r} = 1$. Следовательно, если положить $K' = x_{i_1} \cdot \ldots \cdot x_{i_r}$, то K' будет также импликантом функции f, который получается из импликанта K вычеркиванием сомножителей $\overline{x}_{i_{r+1}}, \ldots, \overline{x}_{i_s}$. Поскольку $s > r$, получаем, что K не есть простой импликант функции f. Значит, сокращенная ДНФ функции f не содержит отрицаний переменных.

Итак, любая конъюнкция K из сокращенной ДНФ функции $f(x_1, \ldots, x_n)$ имеет вид $x_{i_1} \cdot \ldots \cdot x_{i_r}$. Покажем, что конъюнкция K яв-

ляется единственной конъюнкцией в сокращенной ДНФ функции f, которая принимает значение 1 при

$$x_{i_1} = \ldots = x_{i_r} = 1, \quad x_{i_{r+1}} = \ldots = x_{i_n} = 0. \tag{35}$$

В самом деле, пусть имеется еще одна конъюнкция K' из сокращенной ДНФ функции f, которая принимает значение 1 при выполнении условий (35). Тогда согласно первой части доказательства теоремы конъюнкция K' не может содержать сомножителей $\overline{x}_{i_{r+1}}, \ldots, \overline{x}_{i_n}$, а ввиду условия $x_{i_{r+1}} = \ldots = x_{i_n} = 0$ из (35) — также и сомножителей $x_{i_{r+1}}, \ldots, x_{i_n}$. Значит, в конъюнкцию K' могут входить лишь сомножители из числа $x_{i_1}, \ldots, x_{i_r}$. Но тогда K' получается из K вычеркиванием некоторых сомножителей, что противоречит простоте импликанта K.

Таким образом, конъюнкцию K из сокращенной ДНФ функции f удалить нельзя. Для завершения доказательства теоремы 7 теперь остается обратиться к теореме 6.

Как же строить сокращенную ДНФ булевой функции? Существует целый ряд методов синтеза сокращенной ДНФ. Мы рассмотрим только один из них — *метод Блейка*. Этот метод применим к произвольной ДНФ булевой функции, отличной от константы, и состоит в многократном выполнении двух эквивалентных преобразований над конъюнкциями, входящими в ДНФ:

1) *обобщенное склеивание*

$$xK' \vee \overline{x}K'' = xK' \vee \overline{x}K'' \vee K'K'';$$

2) *поглощение*

$$K' \vee K'K'' = K'$$

(подразумевается, что преобразования выполняются только слева направо).

Итак, пусть D — произвольная ДНФ булевой функции f, отличной от константы. По методу Блейка сначала выполняем все возможные преобразования 1) и получаем ДНФ D'. Покажем, что при этом каждый простой импликант K функции f будет включен в ДНФ D'. Очевидно, достаточно рассмотреть случай, когда K не входит в D.

Прежде всего заметим, что в K входят только те переменные, которые содержаться в D. В самом деле, если бы это было не так, то, удалив из K переменную, не входящую в D, мы получили бы конъюнкцию K', которая, очевидно, также является импликантом функции f. Это противоречит простоте импликанта K.

Рассмотрим теперь множество конъюнкций $\{K_j\}$, которое удовлетворяет следующим трем условиям.

1°. K_j содержит только те переменные, которые входят в D.

2°. K_j получается из K домножением на некоторые множители (случай $K_j = K$ не исключается).

3°. Для любой конъюнкции H из ДНФ D конъюнкции K_j удовлетворяет хотя бы один набор, не удовлетворяющий конъюнкции H.

Множество $\{K_j\}$ непусто, так как содержит, например, конъюнкцию K (условие 3° для конъюнкции K выполняется, поскольку в противном случае конъюнкция K либо входит в D, либо не является простым импликантом функции f).

Выберем в множестве $\{K_j\}$ конъюнкции наибольшего ранга $K_1, \ldots, K_m$. Рассмотрим конъюнкцию K_1. Она не может содержать все переменные, входящие в D, так как в этом случае конъюнкции K_1 удовлетворяет только один набор (переменные функции f, не входящие в D, здесь можно не принимать во внимание), который в силу условия 3° не удовлетворяет ни одной конъюнкции из D. То есть получаем, что K_1 не является импликантом функции f, что противоречит условию 2°.

Возьмем переменную x, которая входит в D и не входит в K_1. Рассмотрим конъюнкции xK_1 и $\overline{x}K_1$. Они удовлетворяют условиям 1° и 2° и имеют ранг, на 1 больший, чем ранг K_1. Следовательно, по выбору конъюнкции K_1 конъюнкции xK_1, $\overline{x}K_1$ не удовлетворяют условию 3°. Тогда в ДНФ D имеются такие конъюнкции H_1 и H_2, что все сомножители конъюнкций H_1, H_2 входят соответственно в конъюнкции xK_1 и $\overline{x}K_1$. Понятно, что в конъюнкцию H_1 должен входить сомножитель x, а в конъюнкцию H_2 — сомножитель $\overline{x}$. Поэтому

$$H_1 = xH_1', \quad H_2 = \overline{x}H_2',$$

где все сомножители конъюнкций H_1', H_2' принадлежат конъюнкции K_1. Следовательно, после выполнения преобразования 1) над конъюнкциями H_1 и H_2 в ДНФ D' будет включена конъюнкция $H_1'H_2'$, все сомножители которой входят в конъюнкцию K_1.

Аналогичные построения и утверждения справедливы и для конъюнкций $K_2, \ldots, K_m$. Обозначим через D_1 ДНФ, которая получается из ДНФ D добавлением конъюнкций вида $H_1'H_2'$, образованных при рассмотрении всех конъюнкций $K_1, \ldots, K_m$. Если теперь для этой ДНФ D_1 определить множество конъюнкций $\{L_j\}$, удовлетворяющих условиям 1°–3°, то конъюнкция наибольшего ранга из $\{L_j\}$ будет иметь ранг, меньший, чем ранг конъюнкции K_1. Понятно, что на некотором шаге этого индуктивного процесса в ДНФ D' будет включена конъюнкция K.

После того как в ДНФ D' будут включены все конъюнкции — простые импликанты функции f, — преобразование 2) удаляет из D' конъюнкции, не являющиеся простыми импликантами. В результате образуется сокращенная ДНФ функции f.

Еще раз рассмотрим функцию $f(x, y, z)$, заданную двоичной строкой (11100101). Ее совершенная ДНФ есть

$$D = \overline{x}\overline{y}\overline{z} \vee \overline{x}\overline{y}z \vee \overline{x}y\overline{z} \vee x\overline{y}z \vee xyz.$$

Отправляясь от ДНФ D, методом Блейка построим сокращенную ДНФ функции f. Применим четыре раза преобразование 1):

$$\bar{z}\bar{y}\bar{z} \vee \bar{x}\bar{y}z = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}\bar{y},$$
$$x\bar{y}z \vee xyz = x\bar{y}z \vee xyz \vee xz,$$
$$\bar{x}\bar{y}z \vee x\bar{y}z = \bar{x}\bar{y}z \vee x\bar{y}z \vee \bar{y}z,$$
$$\bar{x}\bar{y}\bar{z} \vee \bar{x}y\bar{z} = \bar{x}\bar{y}\bar{z} \vee \bar{x}y\bar{z} \vee \bar{x}\bar{z}.$$

Таким образом, с помощью преобразования 1) к ДНФ D дизъюнктивно добавляем слагаемое

$$D_{\mathrm{c}}(f) = \bar{x}\bar{y} \vee xz \vee \bar{y}z \vee \bar{x}\bar{z}$$

и образуем ДНФ $D' = D \vee D_{\mathrm{c}}(f)$. Затем, пользуясь преобразованием 2), из ДНФ D' удаляем все конъюнкции, входящие в совершенную ДНФ D. В результате получим сокращенную ДНФ $D_{\mathrm{c}}(f)$ функции f.

Как мы уже знаем, сокращенная ДНФ может не быть минимальной. Вместе с тем любая минимальная ДНФ получается из сокращенной отбрасыванием некоторого числа конъюнкций. Оказывается, в зависимости от того, какие конъюнкции и в каком порядке будут отброшены, может образоваться как минимальная ДНФ, так и неминимальная ДНФ, из которой невозможно удалить ни одну конъюнкцию, не нарушая при этом реализуемую ею функцию. В связи с этим дадим следующее определение.

ДНФ D функции f называется *тупиковой*, если она состоит только из простых импликантов функции f и после удаления любой конъюнкции из D полученная ДНФ уже не реализует функцию f.

Очевидно, что всякая минимальная ДНФ является тупиковой. Как показывает следующий пример, булева функция может иметь несколько тупиковых ДНФ, которые не являются минимальными. Пусть

$$f(x, y, z) = \bar{x}\bar{y}\bar{z} \vee \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee x\bar{y}z \vee xy\bar{z} \vee xyz.$$

Сокращенная ДНФ функции f имеет вид

$$\bar{x}\bar{y} \vee \bar{x}\bar{z} \vee xy \vee xz \vee \bar{y}z \vee y\bar{z}.$$

Тупиковыми ДНФ функции f будут

$$D_1 = \bar{x}\bar{y} \vee xz \vee y\bar{z}, \quad D_2 = \bar{x}\bar{z} \vee xy \vee \bar{y}z, \quad D_3 = \bar{x}\bar{y} \vee xy \vee \bar{y}z \vee y\bar{z},$$
$$D_4 = \bar{x}\bar{y} \vee xy \vee \bar{x}\bar{z} \vee xz, \quad D_5 = \bar{x}\bar{z} \vee xz \vee \bar{y}z \vee y\bar{z}.$$

Из них только D_1 и D_2 являются минимальными.

Таким образом, если сокращенная ДНФ строится по функции однозначно, то процесс перехода от сокращенной ДНФ к тупиковой ДНФ уже неоднозначен. При этом удаление одних элементарных конъюнкций из сокращенной ДНФ приводит к минимальной ДНФ, а удаление других приводит к тупиковой, не являющейся минимальной. Поэтому для построения минимальной ДНФ приходится, вообще

говоря, строить все тупиковые ДНФ и затем проводить среди них отбор.

УПРАЖНЕНИЯ

27. Постройте сокращенную, тупиковые и минимальные ДНФ для функции $f(x, y, z)$, заданной двоичной строкой (10111101).

§ 2. Схемы из функциональных элементов

В современной технике и, прежде всего, в вычислительной технике имеется целый арсенал средств и методов для реализации булевых функций, систем булевых функций и других более сложных дискретных функций. Обычно "массовым тиражом" в виде некоторых "элементов" реализуется сравнительно небольшой набор "элементарных" функций. Эти "элементы" действительно могут представлять собой простейшие вычислительные устройства (например, транзисторы или переключатели), а могут являться достаточно крупными системными блоками. Далее из этих элементов по определенным правилам собираются крупные вычислительные устройства (схемы), способные выполнять сколь угодно сложные преобразования информации.

В математической кибернетике и дискретной математике изучаются математические модели устройств, осуществляющих преобразование информации. Одной из самых простых и вместе с тем распространенных моделей являются схемы из функциональных элементов. Они предназначены в первую очередь для вычисления булевых функций либо систем булевых функций, хотя могут быть использованы и для вычисления функций более сложной природы. Содержательно схема из функциональных элементов (сокращенно СФЭ) представляет собой геометрический объект, составленный из полюсов (входы схемы), треугольников либо квадратов, изображающих функциональные элементы, и дуг либо отрезков прямых, которые соединяют полюса, входы и выходы функциональных элементов ("проводники" схемы).

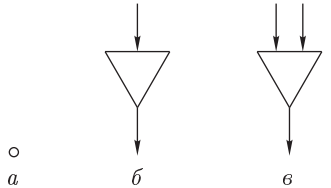

Рис. 2

Прежде чем дать точное определение схемы из функциональных элементов, приведем определение вспомогательного объекта — *сети*. Сеть позволяет описать строение СФЭ безотносительно к ее функционированию. Итак, сеть состоит из полюсов и элементов, которые могут соединяться в сети дугами или отрезками прямых. Полюса будем изображать маленькими кружками (рис. 2, *а*). Для упрощения изложения элементы будем рассматривать только с

одним или двумя входами. Элементы изображаем в виде треугольников (рис. 2, *б*, *в*) с двумя или тремя стрелками. Стрелка, ведущая в элемент, соответствует входу элемента, ведущая из элемента — его выходу.

Еще раз подчеркнем, что на этапе определения сети нас совершенно не интересует ни возможное техническое происхождение полюсов и элементов, ни отношение сети к булевым функциям и способам их вычисления. На этом этапе мы рассматриваем лишь способ соединения полюсов и элементов в схеме, или, как говорят, топологию схемы.

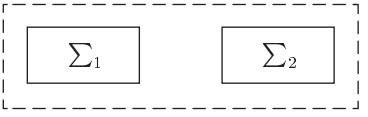

Рис. 3

По индукции определим сеть и множество вершин сети.

1. Полюс есть сеть. Он является единственной вершиной этой сети.

2. Пусть Σ_1, Σ_2 — две сети без общих вершин. Тогда формальное объединение сетей Σ_1, Σ_2 дает новую сеть (рис. 3). Вершинами этой сети являются все вершины сетей Σ_1 и Σ_2.

3. Пусть Σ — сеть, а E — элемент, входы и выход которого не являются вершинами сети Σ. Тогда результат присоединения (или отождествления) всех входов элемента E к некоторым вершинам сети Σ есть сеть (рис. 4, где показан элемент E с двумя входами). При этом в случае элемента E с двумя входами оба входа элемента E могут быть присоединены к одной и той же вершине сети Σ, однако каждый вход должен присоединяться только к одной вершине. Вершинами новой сети являются все вершины сети Σ и выход элемента E.

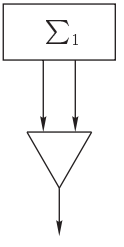

Рис. 4

Непосредственно из определения вытекают следующие два свойства сети.

1°. Никакой элемент сети не присоединен своим выходом ни к полюсу, ни к выходу другого элемента сети.

2°. Вершины сети можно занумеровать натуральными числами так, что выход любого элемента будет иметь номер, больший, чем номер каждого из его входов. Поэтому в сети невозможно найти последовательность вершин $a_1, a_2, \ldots, a_m$ такую, что $a_m = a_1$ и при $1 \leqslant j < m$ вершина a_j является входом некоторого элемента, а a_{j+1} — его выходом. Иными словами, сеть не содержит ориентированных циклов, составленных из элементов.

Перейдем теперь к определению схемы из функциональных элементов. *Схемой из функциональных элеметов* называется сеть в которой:

1) каждому полюсу приписана одна из переменных $x_1, \ldots, x_n, \ldots$, причем различным полюсам приписаны различные переменные; полюса сети называются *входами схемы*;

2) каждому элементу E с одним или двумя входами приписана некоторая функция f_E, зависящая соответственно от одной или двух

переменных; функция f_E называется *функцией элемента* E; элемент E с приписанной ему функцией f_E называется *функциональным элементом*;

3) некоторым вершинам сети приписаны натуральные числа $1, 2, \ldots, m$, причем одной и той же вершине может быть приписано несколько чисел; вершины, которым приписаны числа $1, \ldots, m$, называются *выходами схемы*; *l-м выходом схемы* называется (единственный) выход, которому приписано число l (возможно, что этой вершине приписаны и другие числа).

Так же, как для формул, по индукции дадим определение *функции, реализуемой СФЭ*. При этом будем сопоставлять вершинам схемы булевы функции.

1) Каждому входу сопоставляется функция, равная той переменной, которая приписана этому входу.

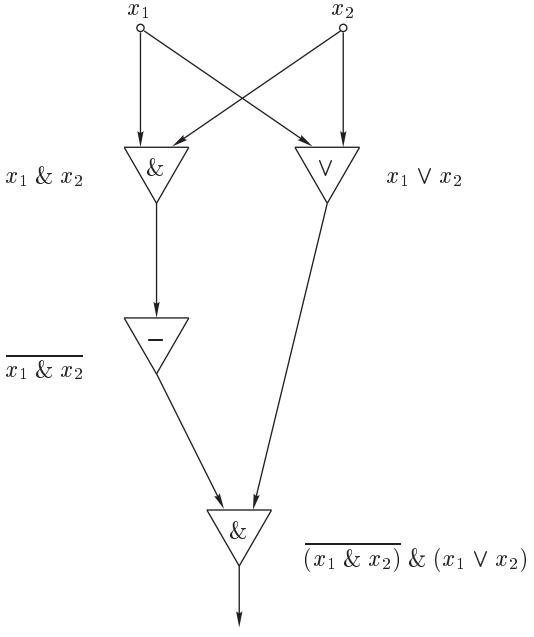

Рис. 5

2) Пусть всем вершинам, к которым присоединены входы элемента E, уже сопоставлены функции (реализуемые в этих вершинах). Тогда выходу элемента E сопоставляется функция $f_E(f^{(1)})$ или $f_E(f^{(1)}, f^{(2)})$, где f_E — функция элемента E, а $f^{(i)}$ — функция, сопоставленная той вершине, с которой соединен i-й вход элемента E (рис. 5).

В результате этого процесса каждой вершине будет сопоставлена некоторая булева функция. По определению схема реализует упорядоченную систему функций (вектор-функцию)

$$F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

где $f_i(x_1, \ldots, x_n)$ — функция, сопоставленная i-му выходу схемы.

Свойства 1°, 2° сети могут быть положены в основу более абстрактного определения схемы из функциональных элементов, которое не использует геометрических понятий. Будем рассматривать два типа переменных: входные $x_1, x_2, \ldots$ и рабочие $y_1, y_2, \ldots$ Схемой из функциональных элементов назовем теперь такую последовательность $z_1, \ldots, z_{m+n}$ входных и рабочих переменных, которая имеет вид $x_1 \ldots x_n y_1 \ldots y_m$, причем если z_i не является входной переменной, то числу i сопоставлены либо число j $(1 \leqslant j < i)$ и булева функция $g_i(z_j)$ от одной переменной, либо два числа j, k $(1 \leqslant j, k < i)$ и булева функция $g_i(z_j, z_k)$ от двух переменных. Так же, как и для СФЭ в исходном определении, каждой переменной z_i по индукции сопоставляется единственная булева функция $f_i(x_1, \ldots, x_n)$, значения которой будут равны значениям переменной z_i в этой схеме.

Если функции всех элементов схемы Σ принадлежат множеству функций Q, то говорят, что схема Σ есть *схема в базисе* Q. Заметим, что в отличие от определения базиса, приведенного в гл. I, в этом параграфе мы не предполагаем функции базиса независимыми. В частности, в дальнейшем рассматриваем СФЭ исключительно в базисе $Q_0 = \{\overline{x},\ xy,\ x \vee y\}$.

Так же, как и для ДНФ, при изучении СФЭ основной задачей является построение для заданной булевой функции (или множества булевых функций) схемы (схем) наименьшей сложности. При этом под сложностью схемы Σ понимается число всех функциональных элементов, входящих в схему Σ. Сложность схемы Σ будем обозначать через $L(\Sigma)$. Пусть далее $L(F)$ обозначает минимум из величин $L(\Sigma)$, где минимум берется по всем схемам Σ, реализующим систему функций F. Положим

$$L(n) = \max L(f),$$

где максимум берется по всем функциям $f(x_1, \ldots, x_n)$, зависящим от n переменных. Функция $L(n)$ носит название *функции Шеннона*. Она играет важнейшую роль в теории синтеза управляющих систем. Величина $L(n)$, как это следует из определения, равна наименьшей сложности, с которой заведомо можно реализовать любую булеву функцию от n переменных. Как и для ДНФ, точное значение $L(n)$ можно найти, последовательно перебирая все функции f от n переменных и находя для каждой из них величину $L(f)$. Следует отметить, что к настоящему времени не известно никаких неперебор-

алгоритмов для точного вычисления функции $L(n)$. Более того, существует гипотеза, что перебор в этой задаче в принципе неустраним.

Наша дальнейшая цель состоит в оценках сверху величин $L(n)$ и $L(F)$ для некоторых функций F.

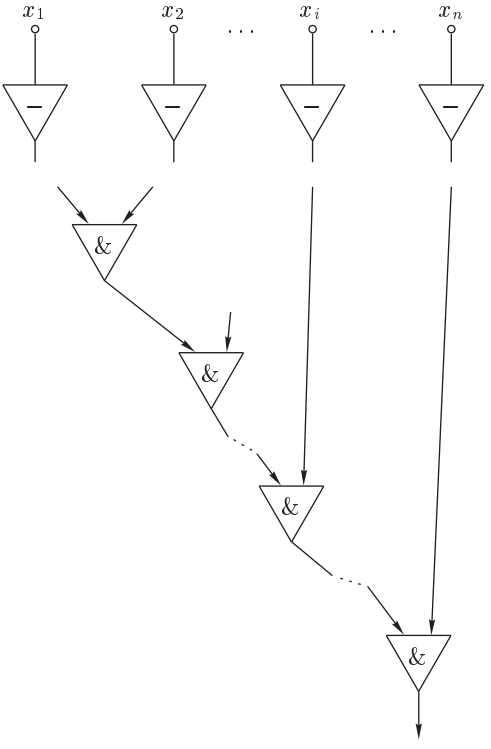

Рис. 6

Используя моделирование совершенной ДНФ, оценим, прежде всего, величину $L(n)$. Будем называть *конъюнктором*, *дизъюнктором* и *инвертором* элементы, которым сопоставлены соответственно функции $\&$, $\vee$, $\bar{}$.

Пусть $K = x_1^{\sigma_1} \,\&\, \ldots \,\&\, x_n^{\sigma_n}$ — элементарная конъюнкция. Нетрудно видеть, что ее можно реализовать СФЭ, состоящей не более чем из n инверторов и $n-1$ конъюнкторов (рис. 6). Если $\sigma_i = 0$, то i-й вход схемы присоединен к инвертору, в противном случае инвертора, соответствующего i-у входу схемы, нет и i-й вход присоединяется к конъюнктору. Очевидно, что

$$L(K) \leqslant 2n - 1. \tag{36}$$

Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, отличная от константы 0, и $K_1 \vee \ldots \vee K_m$ — ее совершенная ДНФ. СФЭ для функ-

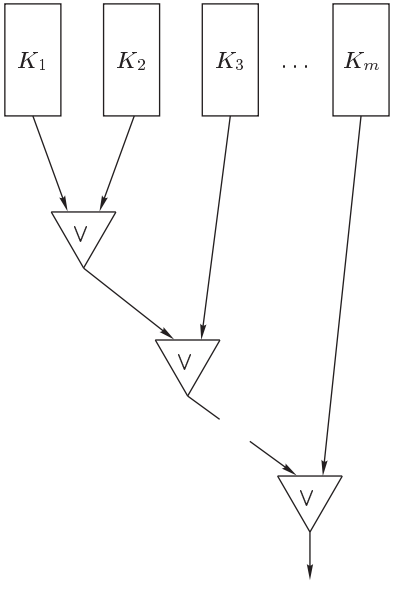

Рис. 7

ции f строится из m схем для конъюнкций K_j и цепочки из $m-1$ дизъюнкторов, которая "объединяет" выходы схем для конъюнкций (рис. 7). Таким образом, учитывая неравенство (36), приходим к следующему утверждению.

Если совершенная ДНФ функции $f(x_1, \ldots, x_n)$ содержит m $(m \geqslant 1)$ конъюнкций, то

$$L(f) \leqslant 2mn.$$

Так как всегда $m \leqslant 2^n$, то для произвольной функции $f(x_1, \ldots, x_n)$, не равной тождественно 0, имеем

$$L(f) \leqslant n\,2^{n+1}.$$

Функция, тождественно равная 0, может быть реализована схемой, изображенной на рис. 8. Поэтому

$$L(n) \leqslant n\,2^{n+1}.$$

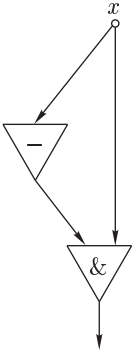

Рис. 8

Существенно лучшую оценку для $L(n)$ можно получить, если воспользоваться индуктивным процессом разложения функции по переменной. В самом деле, легко видеть (рис. 9), что $L(1) = 2$. Если же

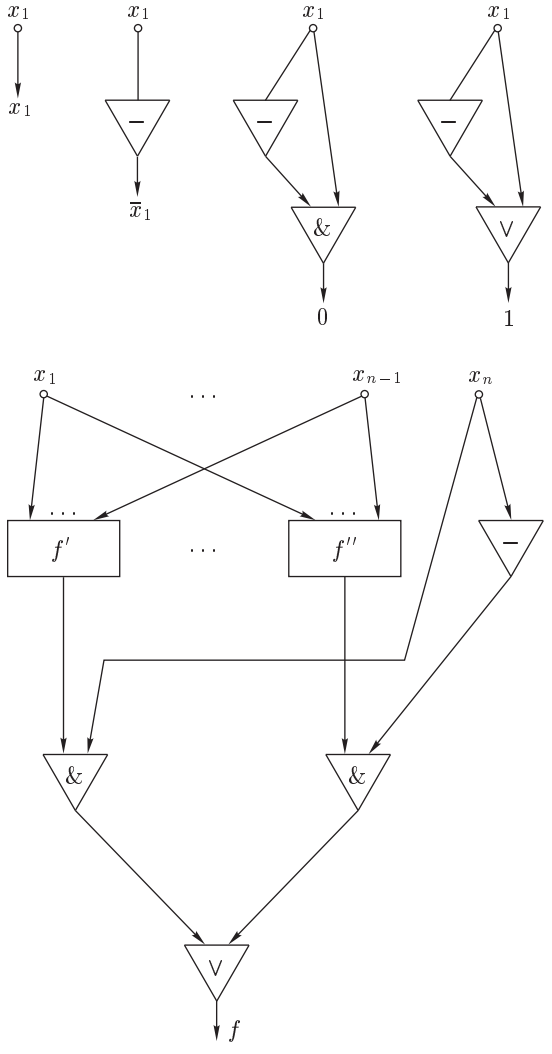

Рис. 9

$n \geqslant 2$, то разложим произвольную функцию $f(x_1, \ldots, x_n)$ по переменной x_n:

$$f(x_1, \ldots, x_{n-1}, x_n) = x_n \,\&\, f(x_1, \ldots, x_{n-1}, 1) \vee \overline{x}_n \,\&\, f(x_1, \ldots, x_{n-1}, 0),$$

и обозначим для краткости функции $f(x_1, \ldots, x_{n-1}, 1)$ и $f(x_1, \ldots, x_{n-1}, 0)$ через f' и f''.

На рис. 9 показано, как из схем, реализующих функции f' и f'', получить схему, реализующую функцию f. Из нее видно, что

$$L(n) \leqslant 2 \cdot L(n-1) + 4.$$

Это рекуррентное соотношение вместе с условием $L(1) = 2$ дает

$$L(n) \leqslant 3 \cdot 2^n - 4.$$

Отметим, что более тонкие методы синтеза схем позволяют установить, что при больших значениях n величина $L(n)$ будет близка к величине $2^n/n$. Как говорят в подобных случаях, $L(n)$ асимптотически равна $2^n/n$.

Общая теория синтеза СФЭ показывает, что для "почти всех" булевых функций от n переменных минимальная сложность реализующих их схем близка к величине $L(n)$. На этом фоне представляют интерес функции, сложность реализации которых схемами существенно мень-

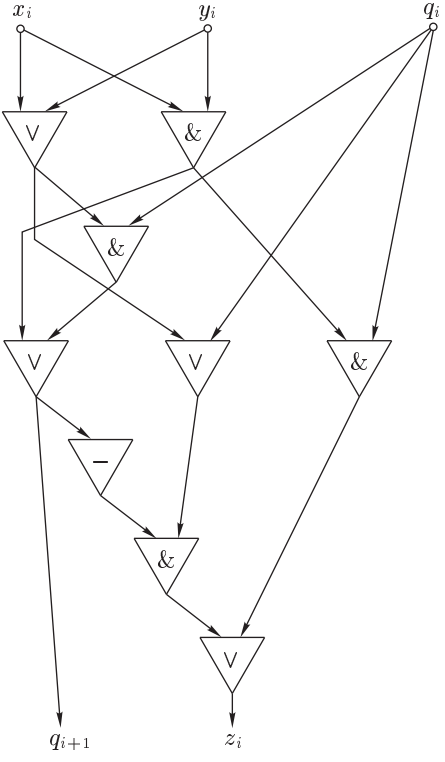

Рис. 10

ше, чем $L(n)$, например, имеющие линейную (по n) сложность. К последним функциям относится двоичный сумматор — вектор-функция,

вычисляющая двоичные разряды $z_1, \ldots, z_n, z_{n+1}$ суммы n-разрядных чисел x, y, заданных в двоичной системе счисления представлениями $x_n \ldots x_1$ и $y_n \ldots y_1$ (старшие разряды этих представлений могут быть нулевыми). Сложение чисел x, y можно осуществить "столбиком", обозначая через $q_1, \ldots, q_{n+1}$ результаты переносов из предыдущих разрядов ($q_1 = 0$):

$$\begin{array}{rcccc} (q_{n+1} & q_n & \ldots & q_1) \\ & x_n & \ldots & x_1 \\ + & y_n & \ldots & y_1 \\ \hline z_{n+1} & z_n & \ldots & z_1 \end{array}$$

Очевидно, что

$$z_i = x_i \oplus y_i \oplus q_i, \quad q_{i+1} = x_i y_i \vee x_i q_i \vee y_i q_i. \tag{37}$$

Опираясь на тождество

$$x_i \oplus y_i \oplus q_i = \overline{x_i y_i \vee x_i q_i \vee y_i q_i} \,\&\, (x_i \vee y_i \vee q_i) \vee x_i y_i q_i,$$

нетрудно построить СФЭ, реализующую преобразования (37) (рис. 10). Обозначим соответствующую схему через B_i $(1 < i \leqslant n)$.

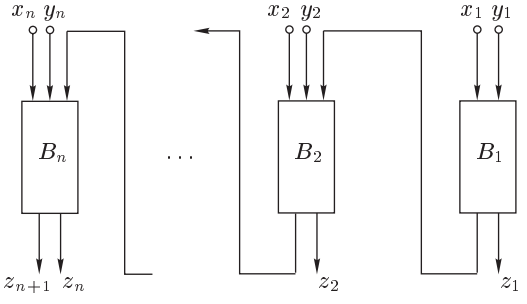

Рис. 11

Тогда схема Σ_n для двоичного сумматора n-разрядных чисел получается путем последовательного соединения блоков B_i (рис. 11). Здесь $z_{n+1} = q_{n+1}$, а схема B_1 осуществляет преобразование

$$z_1 = \overline{(x_1 \,\&\, y_1)} \,\&\, (x_1 \vee y_1), \quad q_2 = x_1 \,\&\, y_1.$$

Очевидно, что $L(B_1) = 4$ и $L(B_i) = 9$ при $1 < i \leqslant n$. Таким образом,

$$L(\Sigma_n) \leqslant 9(n-1) + 4 = 9n - 5.$$

УПРАЖНЕНИЯ

28. Постройте СФЭ, реализующую функцию $x_1 \oplus \ldots \oplus x_n$ $(n \geqslant 2)$ со сложностью $4\,(n-1)$.

29. Докажите, что существует такая константа C, что для любой

симметрической функции f, зависящей от n переменных, справедлива оценка $L(f) \leqslant Cn$ (определение симметрической функции см. в упр. 5).

§ 3. Выполнимость КНФ

В начале 70-х годов в ряде разделов математики (теория алгоритмов, теория булевых функций, теория графов, теория чисел, линейное программирование и др.) было обнаружено большое число задач (сейчас их насчитывается свыше 800), которые обладают следующими отличительными особенностями.

Каждая из задач представляет собой по форме массовую задачу переборного типа. Если для любой из этих задач каким-либо образом "угадано" решение, то проверка того факта, что найденное решение действительно удовлетворяет условиям задачи, требует полиномиального (от длины записи входных данных) числа шагов. Наконец, все эти задачи, как говорят, полиномиально эквивалентны. Это следует понимать так. Пусть, например, задачи A и B представляют собой поиск для заданного двоичного набора a некоторого набора b, который по отношению к a обладает заданным свойством. Тогда должны существовать полиномы $p_1(n)$ и $p_2(n)$ с натуральными коэффициентами и такие алгоритмически вычислимые функции $f_1(x)$, $f_2(x)$, отображающие множество всех двоичных наборов в себя, что, во-первых, функции $f_1(x)$, $f_2(x)$ можно вычислить подходящими алгоритмами, которые для любого двоичного набора длины n заканчивают работу соответственно не более чем через $p_1(n)$ или $p_2(n)$ шагов. А во-вторых, для произвольного двоичного набора x задача A (соответственно задача B) имеет решение тогда и только тогда, когда для двоичного набора $f_1(x)$ (для $f_2(x)$) имеет решение задача B (задача A). О функциях $f_1(x)$, $f_2(x)$ говорят, что они полиномиально сводят задачу A к задаче B и задачу B к задаче A.

Все эти многочисленные задачи из различных разделов математики в научной литературе получили название NP-полных проблем (от английских слов Nondeterministic Polynomial). В теории булевых функций одной из "канонических" NP-полных проблем является проблема выполнимости конъюнктивных нормальных форм (сокращенно ВЫПОЛНИМОСТЬ). Содержательно эта проблема состоит в том, чтобы по произвольной конъюнктивной нормальной форме (определение КНФ см. в § 8 гл. I) выяснить, существует ли двоичный набор, обращающий эту КНФ в 1 (выполняющий КНФ). Ясно, что проблему ВЫПОЛНИМОСТЬ можно решить тривиальным алгоритмом, перебирая для заданной КНФ K, зависящей от n переменных, все 2^n двоичных наборов длины n и вычисляя для каждого из них значение формулы K. Понятно также, что проверка выполнимости КНФ K

на заданном двоичном наборе требует сравнительно небольшого (по отношению к размеру формулы K) числа шагов: следует вместо каждой из переменных формулы K подставить соответствующее значение 0 или 1 из рассматриваемого набора и затем вычислить значение каждой дизъюнкции, входящей в K, пользуясь хорошо известными соотношениями

$$\overline{0} = 1, \quad \overline{1} = 0, \quad 0 \vee 0 = 0, \quad 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1.$$

Все эти действия можно выполнить, например, за квадратичное (относительно длины записи формулы K) число шагов.

Строгое доказательство NP-полноты проблемы ВЫПОЛНИМОСТЬ требует привлечения понятий недетерминированной машины Тьюринга и полиномиального вычисления на такой машине, что выходит за рамки данной брошюры. Мы ограничимся лишь рассмотрением двух важных частных случаев проблемы ВЫПОЛНИМОСТЬ: 2-ВЫПОЛНИМОСТЬ и 3-ВЫПОЛНИМОСТЬ (сокращенно 2-ВЫП и 3-ВЫП). Проблема 2-ВЫП получается из проблемы ВЫПОЛНИМОСТЬ, если в последней рассмотреть лишь такие КНФ, у которых каждый конъюнктивный сомножитель содержит не более двух переменных. Аналогичным образом определяется проблема 3-ВЫП. Далее мы докажем, что проблема 2-ВЫП полиномиально разрешима (это означает, в частности, что проблема 2-ВЫП не является проблемой переборного типа), а проблема 3-ВЫП NP-полна.

Начнем с проблемы 2-ВЫП. Итак, будем рассматривать лишь такие КНФ K, у которых каждый конъюнктивный сомножитель имеет вид x_i^σ или $x_i^\sigma \vee x_j^\tau$, где $\sigma, \tau \in \{0, 1\}$. Алгоритм проверки выполнимости формулы K будет состоять из нескольких этапов, число которых не превосходит числа переменных, входящих в формулу K. Каждый этап характеризуется некоторой переменной из K. На каждом этапе происходит либо удаление из K некоторых конъюнктивных сомножителей, либо удаление переменной, однако в последнем случае могут появиться дополнительные конъюнктивные сомножители. Число таких дополнительных сомножителей не превосходит квадрата от числа переменных, входящих в исходную формулу K. После проведения каждого этапа образуется КНФ K', которая выполнима или невыполнима одновременно с КНФ K. На заключительном этапе будет получена формула от одной переменной, выполнимость которой определяется тривиальным образом.

Сначала рассмотрим этапы, когда в формулу K входит однобуквенный сомножитель вида x или $\overline{x}$. Пусть для определенности это будет сомножитель x. Найдя такой сомножитель в формуле K, просмотрим формулу K и выделим в ней все остальные сомножители, содержащие переменную x. Если среди них есть сомножитель $\overline{x}$, то, очевидно, формула K невыполнима. Тогда завершаем работу алгоритма, давая отрицательный ответ на вопрос о выполнимости формулы K.

Пусть сомножителя $\overline{x}$ в формуле K нет. Пользуясь эквивалентностями (слева направо)

$$x \,\&\, (x \vee y^\sigma) = x, \quad x \,\&\, (\overline{x} \vee y^\sigma) = x \,\&\, y^\sigma,$$

производим сокращения в КНФ K: либо вычеркиваем сомножитель $x \vee y^\sigma$, либо заменяем сомножитель $\overline{x} \vee y^\sigma$ сомножителем y^σ. В образовавшейся после этих преобразований формуле приводим одинаковые сомножители и получаем КНФ K'. Поскольку формула K' получается из формулы K применением некоторых эквивалентных преобразований, формула K' будет эквивалентна формуле K. Однако она содержит меньше символов, чем формула K. Кроме того, весь процесс построения формулы K' из формулы K требует заведомо не более $C_1 n^2$ "элементарных" действий, где C_1 — натуральная константа, а n — длина записи формулы K. При этом под элементарным действием мы понимаем сравнение символов в формуле, перемещение внутри формулы на один символ влево или вправо, вычеркивание одного символа и т.п.

Пусть теперь в формуле K однобуквенные сомножители отсутствуют. Возьмем произвольную переменную x, входящую в формулу K. Пусть K_0 представляет собой конъюнкцию всех сомножителей из K вида $\overline{x} \vee y$ (здесь y может быть как символом переменной, так и ее отрицанием):

$$K_0 = (\overline{x} \vee y_1) \,\&\, \ldots \,\&\, (\overline{x} \vee y_k);$$

K_1 представляет аналогичную конъюнкцию сомножителей вида $x \vee z$:

$$K_1 = (x \vee z_1) \,\&\, \ldots \,\&\, (x \vee z_l);$$

K_2 представляет конъюнкцию всех остальных сомножителей из K. Тогда

$$K = K_0 \,\&\, K_1 \,\&\, K_2.$$

Если, например, конъюнкция K_0 пуста (соответствующих сомножителей вида $\overline{x} \vee y$ в формуле K нет), то конъюнкция K_1 выполнима при $x = 1$. Следовательно, формула K будет выполнимой тогда и только тогда, когда выполнима КНФ K_2. Поэтому в качестве КНФ K' можно взять КНФ K_2, которая получается из КНФ K вычеркиванием всех сомножителей, входящих в K_1. Аналогично рассуждаем, если пуста конъюнкция K_1.

Предположим, что обе конъюнкции K_0, K_1 непусты. Имеем

$$(\overline{x} \vee y_1) \,\&\, \ldots \,\&\, (\overline{x} \vee y_k) = \overline{x} \vee y_1 \,\&\, \ldots \,\&\, y_k,$$

$$(x \vee z_1) \,\&\, \ldots \,\&\, (x \vee z_l) = x \vee z_1 \,\&\, \ldots \,\&\, z_l.$$

Далее, формула вида $(\overline{x} \vee Y) \,\&\, (x \vee Z)$ выполнима в том и только том случае, когда выполнима формула $Y \vee Z$. Следовательно, формула K будет выполнима тогда и только тогда, когда будет выполнимой формула

$$(y_1 \,\&\, \ldots \,\&\, y_k \vee z_1 \,\&\, \ldots \,\&\, z_l) \,\&\, K_2.$$

Однако

$$y_1 \,\&\, \ldots \,\&\, y_k \vee z_1 \,\&\, \ldots \,\&\, z_l = \mathop{\&}_{1\leqslant i\leqslant k} \; \mathop{\&}_{1\leqslant j\leqslant l} (y_i \vee z_j).$$

Таким образом, вопрос о выполнимости формулы K сводится к аналогичному вопросу для формулы

$$K' = \Big(\mathop{\&}_{1\leqslant i\leqslant k} \; \mathop{\&}_{1\leqslant j\leqslant l} (y_i \vee z_j) \Big) \,\&\, K_2.$$

В формулу K' не входит переменная x и, как видно из сравнения формул K и K', в формулу K' добавляется не более $2kl$ новых вхождений символов y_i, z_j. Поскольку $k, l \leqslant n$ (напомним, что n — длина записи формулы K), длина записи формулы K' увеличивается по сравнению с длиной записи формулы K не более, чем на $2n^2$. Из описания процесса построения формулы K' следует также, что формулу K можно преобразовать в формулу K' не более, чем за $C_2 n^2$ "элементарных" действий, где C_2 — натуральная константа.

Таким образом, последовательно применяя к исходной КНФ K описанные выше этапы преобразований, мы не далее, чем на $(n-1)$-м этапе либо убедимся в невыполнимости формулы K, либо придем к формуле вида x, $\overline{x}$, $x \vee \overline{x}$, $x \,\&\, \overline{x}$ от одной переменной. В первых трех случаях имеем, очевидно, выполнимость формулы K, в четвертом случае — невыполнимость. В целом весь процесс проверки выполнимости формулы K займет не более, чем $C \cdot n^2 \cdot n = Cn^3$ "элементарных" действий, где $C = \max(C_1, C_2)$. Тем самым мы установили, что проблему 2-ВЫП можно решить, произведя примерно Cn^3 элементарных действий, где n имеет смысл длины записи исходной КНФ. Иными словами, проблема 2-ВЫП является полиномиально разрешимой.

Рассмотрим теперь проблему 3-ВЫП и докажем, что она является NP-полной. Наше доказательство будет относительным, поскольку мы предполагаем NP-полной проблему ВЫПОЛНИМОСТЬ. Очевидно, что проблема 3-ВЫП полиномиально сводится к проблеме ВЫПОЛНИМОСТЬ: соответствующая сводящая функция $f(x)$ по каждой КНФ, имеющей не более трех дизъюнктивных слагаемых в каждом конъюнктивном сомножителе, выдает в качестве результата эту же самую КНФ. Докажем, что проблема ВЫПОЛНИМОСТЬ также полиномиально сводится к проблеме 3-ВЫП. С этой целью продемонстрируем, как за полиномиальное число шагов преобразовать произвольную КНФ K в такую КНФ K' с не более чем тремя слагаемыми в каждом сомножителе, что K и K' выполнимы или невыполнимы одновременно.

Очевидно, что можно ограничиться рассмотрением только таких КНФ, у которых имеются сомножители, содержащие более трех дизъюнктивных слагаемых. Пусть $C = y_1 \vee \ldots \vee y_m$ — один из таких сомножителей в формуле K ($y_1, \ldots, y_m$ могут быть здесь как переменными, так и отрицаниями переменных). Обозначим через K_1

КНФ, которая получается из КНФ K вычеркиванием сомножителя C. Пусть u — переменная, не входящая в K. Положим

$$D = (y_1 \vee y_2 \vee u) \,\&\, (y_3 \vee \ldots \vee y_m \vee \overline{u}).$$

Покажем, что КНФ K выполнима тогда и только тогда, когда выполнима КНФ $D \,\&\, K_1$.

Пусть набор $a = (a_1, \ldots, a_n)$ обращает КНФ K в 1. Тогда, в частности, набор a обращает в 1 дизъюнкцию C. Если набор a обращает в 1 формулу $y_1 \vee y_2$, то набор $(a_1, \ldots, a_n, 0)$ будет обращать в 1 формулу D и, следовательно, формулу $D \,\&\, K_1$ (последний разряд набора $(a_1, \ldots, a_n, 0)$ отвечает переменной u). Если же набор a обращает в 1 формулу $y_3 \vee \ldots \vee y_n$, то аналогичное утверждение будет справедливо для набора $(a_1, \ldots, a_n, 1)$.

Обратно, пусть $(a_1, \ldots, a_n, b)$ — набор, обращающий в 1 КНФ $D \,\&\, K_1$. Если $b = 0$, то набор a обращает в 1 формулу $y_1 \vee y_2$ и, следовательно, формулу C. При $b = 1$ то же самое будет справедливо для формул $y_3 \vee \ldots \vee y_m$ и C.

Описанное преобразование уменьшает на 1 число слагаемых в сомножителе $y_3 \vee \ldots \vee y_m \vee \overline{u}$, полученном из C, и увеличивает на 2 общее число букв в КНФ $D \,\&\, K_1$ по сравнению с КНФ K. Если в КНФ K имеется k сомножителей соответственно с числом слагаемых $m_1, \ldots, m_k$, где $m_1, \ldots, m_k > 3$, то достаточно аналогичным способом добавить не более $2\,(m_1 + \ldots + m_k - 3k)$ букв с тем, чтобы получить требуемую КНФ K', выполнимую или невыполнимую одновременно с КНФ K. То, что преобразование формулы K в формулу K' можно выполнить за полиномиальное число действий, очевидно.

ОТВЕТЫ, РЕШЕНИЯ, УКАЗАНИЯ

1. 2^{2^n-k}.

2. Набор (1011) определяет импликацию $x_2 \to x_1$, набор (1001) — эквивалентность $x_1 \sim x_2$, набор (1000) — функцию $x_1 \downarrow x_2$, называемую *стрелкой Пирса* (или *антидизъюнкцией*).

3. Функция $g_1(x_1, x_2, x_3)$ существенно зависит от переменных x_1, x_3, функция $g_2(x_1, x_2, x_3)$ — от переменных x_1, x_2, x_3.

4. Существенные (фиктивные) переменные функций f и g совпадают. Чтобы в этом убедиться, достаточно заметить, что если $a_i = f(b_1, \ldots, b_n)$ $(1 \leqslant i \leqslant 2^n)$, то $a_i = g(\overline{b}_1, \ldots, \overline{b}_n)$. Поэтому из равенств

$$a_k = f(b_1, \ldots, b_{j-1}, 0, b_{j+1}, \ldots, b_n), \quad a_l = f(b_1, \ldots, b_{j-1}, 1, b_{j+1}, \ldots, b_n)$$

следуют равенства

$$a_k = g(\overline{b}_1, \ldots, \overline{b}_{j-1}, 1, \overline{b}_{j+1}, \ldots, \overline{b}_n), \quad a_l = g(\overline{b}_1, \ldots, \overline{b}_{j-1}, 0, \overline{b}_{j+1}, \ldots, \overline{b}_n).$$

Значит, из существенной зависимости функции $f(x_1, \ldots, x_n)$ от переменной x_j вытекает существенная зависимость функции $g(x_1, \ldots, x_n)$ от переменной x_j, и наоборот.

5. Пусть $f(x_1, \ldots, x_n)$ — симметрическая функция, отличная от константы. Тогда для некоторого m $(0 \leqslant m < n)$ и некоторого a из множества B функция f принимает значение a на всех двоичных наборах, содержащих m единичных компонент, и значение $\overline{a}$ на всех двоичных наборах, содержащих $m+1$ единичных компонент. Теперь для доказательства утверждения достаточно для любого i $(1 \leqslant i \leqslant n)$ рассмотреть двоичные наборы, содержащие m и $m+1$ единичных компонент и различающиеся только в i-ой компоненте.

6. $h_1(x_1, x_2) = 1$, $h_2(x_1, x_2, x_3) = x_1 \oplus x_3 \oplus 1$.

8. Ни при одном n $(n \geqslant 3)$.

10. а) и в) являются, б) не является.

11. Неверно. Например, объединение замкнутых классов T_0 и C_1 не содержит функцию $\overline{x}$, которая получается суперпозицией функций $x \oplus y$ из класса T_0 и 1 из класса C_1.

12. $xyz \oplus xz \oplus y \oplus z \oplus 1 = xz \vee x\overline{z} \cdot \overline{y} \vee \overline{x}z \cdot y \vee \overline{x}\overline{z} \cdot \overline{y}$.

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

15. Если

$$f(a_1,\dots,a_{i-1},0,a_{i+1},\dots,a_n)=b,\quad f(a_1,\dots,a_{i-1},1,a_{i+1},\dots,a_n)=\overline{b},$$

то

$$f^*(\overline{a}_1,\dots,\overline{a}_{i-1},1,\overline{a}_{i+1},\dots,\overline{a}_n)=\overline{b},$$
$$f^*(\overline{a}_1,\dots,\overline{a}_{i-1},0,\overline{a}_{i+1},\dots,\overline{a}_n)=b.$$

16. Верно.

17. $(x_1\vee\dots\vee x_n)\oplus 1$.

18. $xyzw\oplus xyw\oplus xzw\oplus yzw\oplus xz\oplus xw\oplus w\oplus 1$.

19. Имеется четыре самодвойственные функции $f(x_1,x_2)$, которые задаются двоичными наборами

$$(0011),\quad (0101),\quad (1010),\quad (1100).$$

Это суть соответственно функции x_1, x_2, $\overline{x}_2$, $\overline{x}_1$.

21. При любом n $(n\geqslant 3)$ функция $f(x_1,\dots,x_n)$, задаваемая полиномом Жегалкина

$$x_1x_2\oplus x_1x_3\oplus x_2x_3,$$

принимает значение 1 ровно на 2^{n-1} наборах. Если $n\leqslant 2$, то любая функция от n переменных, принимающая значение 1 ровно на 2^{n-1} наборах, является линейной.

22. Имеется 20 монотонных функций от трех переменных:

$$0,\ 1,\ x,\ y,\ z,\ x\vee y,\ x\vee z,\ y\vee z,\ xy,\ xz,\ yz,\ x\vee y\vee z,\ xyz,$$
$$x\vee yz,\ y\vee xz,\ z\vee xy,\ x(y\vee z),\ y(x\vee z),\ z(x\vee y),\ xy\vee xz\vee yz.$$

23. Пусть функция $f(x_1,\dots,x_n)$ монотонна и $(a_1,\dots,a_n)\leqslant(b_1,\dots,b_n)$. Тогда

$$(\overline{b}_1,\dots,\overline{b}_n)\leqslant(\overline{a}_1,\dots,\overline{a}_n),\quad f(\overline{b}_1,\dots,\overline{b}_n)\leqslant f(\overline{a}_1,\dots,\overline{a}_n)$$

и, следовательно,

$$\overline{f}(\overline{a}_1,\dots,\overline{a}_n)\leqslant\overline{f}(\overline{b}_1,\dots,\overline{b}_n).$$

24. $0,\ 1,\ e_i^n(x_1,\dots,x_n)$ $(1\leqslant i\leqslant n,\ n=1,2,\dots)$.

25. Например, $\{1,\ x\oplus y,\ x\vee y\}$.

26. Из непринадлежности функции $f(x_1,\dots,x_n)$ классам T_0, T_1 следует, что $f(0,\dots,0)=1$ и $f(1,\dots,1)=0$. Таким образом, f не является монотонной функцией. Если бы функция f была линейной, т.е.

$$f(x_1,\dots,x_n)=x_{i_1}\oplus\dots x_{i_s}\oplus a,$$

то из условия $f(0,\dots,0)=1$ вытекало бы, что $a=1$, а из условия $f(1,\dots,1)=0$, что s — нечетное число. Однако тогда f была бы самодвойственной функций. Если вместо класса S взять класс L, то

утверждение становится неверным. Это видно на примере самодвойственной функции $xy \oplus xz \oplus yz \oplus 1$.

27. Сокращенная ДНФ есть

$$\overline{x}y \vee x\overline{y} \vee \overline{x}\overline{z} \vee xz \vee \overline{y}\overline{z} \vee yz,$$

минимальные —

$$\overline{x}y \vee xz \vee \overline{y}\overline{z}, \quad x\overline{y} \vee \overline{x}\overline{z} \vee yz,$$

тупиковые неминимальные —

$$\overline{x}y \vee x\overline{y} \vee \overline{y}\overline{z} \vee yz, \quad \overline{x}\overline{z} \vee xz \vee \overline{y}\overline{z} \vee yz, \quad \overline{x}y \vee x\overline{y} \vee \overline{x}\overline{z} \vee xz.$$

28. Взять за основу схему, изображенную на рис. 5.

29. Любую симметрическую функцию $f(x_1, \ldots, x_n)$ можно задать набором чисел $(i_1, \ldots, i_m)$ таким, что $0 \leqslant i_1 < \ldots < i_m \leqslant n$ и $f(a_1, \ldots, a_n) = 1$ тогда и только тогда, когда количество единиц в наборе $(a_1, \ldots, a_n)$ есть число из набора $(i_1, \ldots, i_m)$. В связи с этим сначала следует построить схему линейной сложности, которая для любого двоичного набора $(a_1, \ldots, a_n)$ вычисляет двоичные разряды $b_1, \ldots, b_r$ числа $a_1 + \ldots + a_n$ (сложение арифметическое, а не по модулю 2).

Тогда $r = [\log_2 n] + 1$, где $[d]$ обозначает целую часть числа d, и по набору $(b_1, \ldots, b_r)$ можно однозначным образом определить значение $f(a_1, \ldots, a_n)$.

Вторая схема линейной сложности осуществляет преобразование $(b_1, \ldots, b_r) \to f(a_1, \ldots, a_n)$.

ОГЛАВЛЕНИЕ

Учебное издание

МАРЧЕНКОВ Сергей Серафимович

БУЛЕВЫ ФУНКЦИИ

Редактор *Е.Ю. Ходан*
Оригинал-макет *Д.В. Горбачева*
Оформление обложки *А.Ю. Алехиной*

ЛР № 071930 от 06.07.01. Подписано в печать 23.05.02.
Формат 60×90/16. Бумага офсетная № 1. Печать офсетная.
Усл. печ. л. 31. Уч.-изд. л. 34,1. Тираж 3000 экз. Заказ №

Издательская фирма
«Физико-математическая литература»
МАИК «Наука/Интерпериодика»
117864 Москва, ул. Профсоюзная, 90

Отпечатано в ФГУП
«Производственно-издательский комбинат ВИНИТИ»
140010, г. Люберцы, Московская обл., Октябрьский пр-т, 403

В серии «Популярные лекции по математике» в разные годы вышли следующие книги.

Маркушевич А.И. Возвратные последовательности.
Натансон И.П. Простейшие задачи на максимум и минимум.
Соминский И.С. Метод математической индукции.
Маркушевич А.И. Замечательные кривые.
Коровкин П.П. Неравенства.
Воробьев Н.Н. Числа Фибоначчи.
Курош А.Г. Алгебраические уравнения произвольных степеней.
Гельфонд А.О. Решение уравнений в целых числах.
Маркушевич А.И. Площади и логарифмы.
Смогоржевский А.С. Метод координат.
Дубнов Я.С. Ошибки в геометрических доказательствах.
Натансон И.П. Суммирование бесконечно малых величин.
Маркушевич А.И. Комплексные числа и конформные отображения.
Фетисов А.И. О доказательствах в геометрии.
Шафаревич И.Р. О решении уравнений высших степеней.
Шерватов В.Г. Гиперболические функции.
Болтянский В.Г. Что такое дифференцирование?
Миракьян Г.М. Прямой круговой цилиндр.
Люстерник Л.А. Кратчайшие линии.
Лопшиц А.М. Вычисление площадей ориентированных фигур.
Головина Л.И., *Яглом И.М.* Индукция в геометрии.
Болтянский В.Г. Равновеликие и равносоставленные фигуры.
Смогоржевский А.С. О геометрии Лобачевского.
Аргунов Б.И., *Скорняков Л.А.* Конфигурационные теоремы.
Смогоржевскнй А.С. Линейка в геометрических построениях.
Трахтенброт Б.А. Алгоритмы и машинное решение задач.
Успенский В.А. Некоторые приложения механики к математике.
Архангельский И.А., *Зайцев Б.И.* Автоматические цифровые машины.
Костовский А.Н. Геометрические построения одним циркулем.
Шилов Г.Е. Как строить графики.
Дорфман А.Г. Оптика конических сечений.

Вентцель Е.С. Элементы теории игр.
Барсов А.С. Что такое линейное программирование.
Маргулис В.Е. Системы линейных уравнений.
Виленкин Н.Я. Метод последовательных приближений.
Болтянский В.Г. Огибающая.
Шилов Г.Е. Простая гамма (устройство музыкальной шкалы).
Шрейдер Ю.А. Что такое расстояние?
Воробьев Н.Н. Признаки делимости.
Фомин С.В. Системы счисления.
Коган В.Ю. Приложение механики к геометрии.
Любич Ю.И., *Шор Л.А.* Кинематический метод в геометрических задачах.
Успенский В.А. Треугольник Паскаля.
Бакельман И.Я. Инверсия.
Яглом И.М. Необыкновенная алгебра.
Соболь И.М. Метод Монте-Карло.
Калужнин Л.А. Основная теорема арифметики.
Солодовников А.С. Системы линейных неравенств.
Шилов Г.Е. Математический анализ в области рациональных функций.
Болтянский Б.Г., *Гохберг Н.Ц.* Разбиение фигур на меньшие части.
Бескин П.М. Изображения пространственных фигур.
Бескин Н.М. Деление отрезка в данном отношении.
Розенфельд Б.А., *Сергеева Н.Д.* Стереографическая проекция.
Успенский В.А. Машина Поста.
Беран Л. Упорядоченные множества.
Абрамов С.А. Элементы программирования.
Успенский В.А. Теорема Гёделя о неполноте.
Шашкин Ю.А. Эйлерова характеристика.
Скорняков Л.А. Системы линейных уравнений.
Шашкин Ю.А. Неподвижные точки.
Петросян Л.А., *Рихсиев Б.Б.* Преследование на плоскости.