С.С. Марченков

ОСНОВЫ ТЕОРИИ БУЛЕВЫХ ФУНКЦИЙ

$$(xy \vee xz \vee yz) \oplus x \oplus y$$

С.С. Марченков

ОСНОВЫ ТЕОРИИ БУЛЕВЫХ ФУНКЦИЙ

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

МОСКВА
ФИЗМАТЛИТ®
2014

УДК 519.7
ББК 22.176
М 30

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

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

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

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

ISBN 978-5-9221-1562-9

ОГЛАВЛЕНИЕ

Предисловие

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

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

Главы I, II содержат традиционный материал, вводящий в теорию булевых функций, включая критерий полноты для класса всех булевых функций. Обычно в этом объеме булевы функции излагаются в курсах дискретной математики. Единственное нетрадиционное дополнение, которое включено в главу II, это перечисление всех замкнутых классов, содержащих константы. Иногда изучение замкнутых классов булевых функций помимо предполных классов ограничивают только классами, содержащими обе константы.

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

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

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

В главе VI рассматриваются вопросы полноты и конечной порождаемости для частичных булевых функций. Эта тематика практически не затрагивается в учебной и монографической литературе. Вместе с тем многие вопросы для частичных булевых функций решаются совершенно иначе, нежели для обычных булевых функций. Одна из целей главы VI — обратить внимание исследователей на проблемы, возникающие для частичных булевых функций, и, возможно, способствовать продвижению данной тематики в лекционные курсы.

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

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

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

Указатель обозначений

C — класс всех функций, равных константам 0 или 1

C_0 — класс всех функций, равных константе 0

C_1 — класс всех функций, равных константе 1

D — класс всех дизъюнкций

D_0 — класс всех дизъюнкций, сохраняющих константу 0

D_1 — класс всех дизъюнкций, сохраняющих константу 1

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

E_2 — множество $\{0,1\}$

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

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

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

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

K — класс всех конъюнкций

K_0 — класс всех конъюнкций, сохраняющих константу 0

K_1 — класс всех конъюнкций, сохраняющих константу 1

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

L — класс всех линейных функций

L_0 — класс всех линейных функций, сохраняющих константу 0

L_1 — класс всех линейных функций, сохраняющих константу 1

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

M — класс всех монотонных функций

M_0 — класс всех монотонных функций, сохраняющих константу 0

M_1 — класс всех монотонных функций, сохраняющих константу 1

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

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

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

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

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

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

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

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

P_2 — класс всех булевых функций

P_2^* — класс всех частичных булевых функций

Par — язык параметрического замыкания

$\mathrm{Par}[Q]$ — параметрическое замыкание множества функций Q

$\mathrm{Pol}(\rho)$ — класс всех функций, сохраняющих предикат ρ

$\mathrm{Pol}(R)$ — класс всех функций, сохраняющих предикаты множества R

Pos — язык позитивного замыкания

$\mathrm{Pos}[Q]$ — позитивное замыкание множества функций Q

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

S — класс всех самодвойственных функций

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

SL — класс всех самодвойственных линейных функций

SM — класс всех самодвойственных монотонных функций

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

T_0 — класс всех функций, сохраняющих константу 0

T_1 — класс всех функций, сохраняющих константу 1

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

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

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

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

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

Глава I

ЭЛЕМЕНТАРНЫЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ

§ 1. Табличное задание булевых функций

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

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

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

Таблица 1

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

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

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

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

§ 2. Некоторые элементарные булевы функции

Составим таблицу для всех четырех булевых функций от одной переменной.

Таблица 2

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

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

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