КИБЕРНЕТИКА

И. М. ЯГЛОМ

БУЛЕВА СТРУКТУРА И ЕЕ МОДЕЛИ

Москва «Советское радио» 1980

ББК 32.81
Я 27
УДК 51+007(023)

Яглом И. М.

Я27 Булева структура и ее модели. — М.: Сов. радио, 1980. — 192 с., ил.

70 коп.

На конкретном примере структуры (алгебры) Буля в книге излагается общая схема создания математических теорий и приложений этих теорий к явлениям реальной жизни. Главное место в книге занимает алгебра высказываний, являющаяся фундаментом математической логики, алгебра релейно-контактных схем, лежащая в основе проектирования сложных электрических и электронных систем, и теория вероятностей. Изложение сопровождается большим числом примеров и упражнений для самостоятельного решения.

Книга не предполагает никаких специальных знаний, выходящих за пределы школьного курса математики. Предназначается для широкого круга читателей, интересующихся кибернетикой, общенаучными проблемами, математической логикой или теорией вероятностей.

$Я\frac{30501\text{-}077}{046(01)\text{-}80}$ 71-81 1502000000

ББК 32.81
6Ф0.1

Рецензенты: чл.-кор. АПН СССР *В. Г. Болтянский* и д-р физ.-мат. наук *Б. А. Розенфельд*

Редакция кибернетической литературы

Исаак Моисеевич Яглом

БУЛЕВА СТРУКТУРА И ЕЁ МОДЕЛИ

Редактор Н. Г. Давыдова
Художественный редактор Н. А. Игнатьев
Технический редактор Т. Н. Зыкина
Корректор Н. Н. Васина

ИБ № 541

Сдано в набор 29.12.79 г. Подписано в печать 22.10.80 г. Т-15077. Формат 60×84[1]/16. Бумага книжно-журн. Гарнитура литературная. Печать высокая. Объем 11,39 усл. п. л. 12,46 уч.-изд. л. Тираж 25 000 экз. Зак. 1518. Цена 70 к.
Издательство «Советское радио», Москва, Главпочтамт, а/я 693

Московская типография № 4 Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 129041, Москва, Б. Переяславская ул., д. 46.

ПРЕДИСЛОВИЕ

При написании настоящей книги автор руководствовался двумя целями, в соответствии с чем книга рассчитана на две разные категории читателей.

Прежде всего мне хотелось заполнить явственно ощущающийся пробел в доступной русскому читателю литературе. Научно-техническая революция наших дней, связанная с созданием ЭВМ, возникновением кибернетики и широчайшей математизацией знания, не только колоссально расширила круг потребителей математики, но и вызвала известную перестройку самих математических наук, заметно сместив здесь акценты и выдвинув на авансцену те направления математической мысли, которые совсем еще недавно считались чисто специальными и интересными лишь узкому кругу специалистов в соответствующей области. При этом особенно бросается в глаза рост значения теории вероятностей и математической (или символической) логики. Возросший авторитет теории вероятностей и логики связан не только (и даже не столько) с их большим местом во всех современных приложениях математики, но и с мировоззренческим значением соответствующих наук: ведь теоретико-вероятностные и статистические представления лежат в основе современной научной картины мира, а без математической логики теряют всякую почву столь модные сегодня дискуссии о том, может ли машина мыслить, и становится бессодержательной актуальная проблема создания искусственного интеллекта. Но обе эти теории (а точнее, науки или даже комплексы наук, имеющие первостепенное прикладное и общетеоретическое значение — теория вероятностей и математическая логика) базируются на одной и той же аксиоматической системе (или математической структуре, если использовать модную и удобную терминологию знаменитого Николá Бурбаки): на алгебре (или структуре) Буля.

Иной реализацией булевой структуры является играющая столь важную роль в современной технике (в частности, в учении о конструировании и функционировании ЭВМ) «алгебра релейных (электрических) цепей», профессионально необходимая каждому инженеру, связанному с электрическими сетями или электронными устройствами.

Все эти обстоятельства привели к тому, что во многих странах учение об алгебрах (структурах) Буля ныне прочно вошло в школьный курс математики. У нас дело обстоит пока иначе, однако элементы этой теории обстоятельно изучаются во многих высших учебных заведениях — не только на математических факультетах и отделениях университетов и пединститутов, но и на специализированных «математических» отделениях филологических, психологических или юридических факультетов и во многих втузах. С этим же связано наличие довольно обширной литературы об алгебрах (структурах) Буля.

Однако вся имеющаяся на русском языке литература об алгебрах Буля достаточно отчетливо распадается на три группы: это либо совсем уж элементарные введения в учение об алгебрах Буля, рассчитанные на малоопытных читателей, в первую очередь на школьников (таковы, например, книги [1.1—1.3]), либо обстоятельные пособия для студентов высших учебных заведений (скажем, [2.1, 2.2 или 2.8]), либо, наконец, монографии для специалистов-математиков (как [3.1 или 3.2]). Но при этом упускается из виду еще одна обширная категория читателей: ее составляют лица, ранее не изучавшие соответствующей теории (которая ведь еще совсем недавно не входила в обязательный курс ни одного из наших высших учебных заведений), а ныне желающие с ней самостоятельно познакомиться. В зарубежной литературе на эту категорию читателей — не получивших должного образования, но достаточно серьезных и по-настоящему заинтересованных в аппарате современной прикладной математики — рассчитано множество разнообразных по уровню требований и методическим установкам книг и статей (в качестве примеров здесь можно назвать сочинения [1.15—1.19 или 2.23—2.26], составляющие лишь весьма малую часть все не иссякающего потока книг такой направленности). У нас же подобных книг практически нет; лишь со значительной натяжкой к этой категории литературы по кибернетике и математике можно отнести переводные сочинения [1.4—1.7 и 1.13, 1.14], все, кстати сказать, очень сильно отличающиеся от настоящего. Таким образом, эту книгу, весьма естественную, как мне кажется, для серии «Кибернетика», можно рассматривать как пособие для самообразования или как книгу для чтения, обращенную к широкому кругу лиц (в том числе к студентам и выпускникам технических, педагогических, естественнонаучных и гуманитарных вузов), желающих самостоятельно познакомиться как с первоначальными представлениями математической логики, теории вероятностей и теории электрических цепей, так и с внутренними связями этих трех важных теорий.

Наряду со сказанным эта книга преследует еще одну, возможно несколько менее утилитарную цель. Ее вполне можно рассматривать как продолжение книги «Математические структуры и математическое моделирование» [II], призванной пояснить место математики в общем процессе познания, ее уникальность и одновременно тесную связь со всеми другими направлениями научной мысли. В книге [II] обсуждались вопросы об общем устройстве математических теорий, об их развертывании как формально-логических систем и о путях приложения математики к изучению реально существующих явлений материального, социального или духовного порядка (так сказать, к физике, или к социологии, или к литературоведению). Общие идеи иллюстрировались в [11] небольшим числом весьма эскизно набросанных примеров математических структур и математических моделей — на более подробный рассказ о каких-либо конкретных образцах математических теорий там просто не было места. Однако для того, чтобы по-настоящему понять природу и роль математики, совершенно необходим более тщательный анализ какой-нибудь конкретной темы — и в качестве подобного «эталонного» образца математической теории мне показалось привлекательным остановиться на булевой структуре, характеризующейся широкими связями со многими магистральными направлениями математической науки (например, с учением об алгебраических кольцах или о решетках) и весьма широким спектром приложений. Разумеется, от книги [11] настоящее сочинение нисколько не зависит.

Ориентация на разные категории читателей определила некоторую разноплановость книги, в целом достаточно элементарной (от ее читателя практически нигде не требуются знания, выходящие за рамки курса средней школы), но вовсе не тривиальной и в некоторых своих частях предполагающей известную настойчивость читателя. В частности, несколько более подробные, чем в других сочинениях на ту же тему, исторические сведения, как и другие вставки, расширяющие строгие рамки учения о булевой структуре (скажем, рассказ об аксиоматических системах, более широких, чем алгебра Буля, или отступление о теории размытых множеств Л. Заде), рассчитаны скорее на читателей, интересующихся общими вопросами, чем на лиц, непосредственно заинтересованных в теории вероятностей, математической логике и их приложениях. Напротив, большинство упражнений обращены, в первую очередь, к первой из двух указанных выше категорий возможных читателей книги. Напечатанные мелким шрифтом разделы текста могут быть опущены без ущерба для понимания остальной части книги; некоторым читателям будет, видимо, уместно опустить также и доказательства тех или иных фактов (т. е. принять эти доказательства на веру; начало и конец доказательства в книге всегда обозначаются заметными знаками ◀ и ▶).

Немногочисленные примеры и упражнения иногда выходят за рамки основного текста, намечая возможные выходы в смежные области; однако в большинстве случаев они рассчитаны лишь на закрепление полученных знаний и самопроверку степени усвоения содержания книги. Упражнения сопровождаются весьма краткими и неполными указаниями к их решению, собранными в конце книги. Дальнейшие задачи и упражнения по теме книги читатель сможет найти в вузовских задачниках [2.21 и 2.22], в некоторых из перечисленных в конце книги пособий, например, в [1.13, 1.14, 2.1 или 2.3], а также в содержательных книгах [2.2 и 2.23]. Читателю, специально заинтересованному в изучении математической логики, можно порекомендовать книги [1.4 и 2.4—2.12] (из которых хочется специально отметить элементарное введение в предмет [1.4], классическое сочинение [2.7], превосходный университетский учебник [2.10] и книгу [2.5], входящую в ту же серию, что и настоящая книга); читателю, пожелавшему углубить свои знания по теории вероятностей, хочется, в первую очередь, указать на весьма богатую по содержанию, однако вовсе не простую книгу [2.17]; читателя-инженера, нуждающегося в более полном изложении теории релейных электрических цепей, естественно адресовать к книге [2.13].

В книге принята двойная нумерация формул и упражнений, где первое число указывает номер параграфа, а второе — номер формулы (упражнения); при ссылке на формулу (упражнение) того же параграфа называется лишь второе число. Сравнительно сложную структуру имеет и список литературы, начинающийся с основополагающего сочинения Буля (к сожалению, пока не переведенного на русский язык) и с предшествующей книги автора. Затем идет (разумеется, весьма неполный) перечень общих сочинений по теории булевых структур, математической логике и теории вероятностей, довольно условно разбитый на три группы, в связи с чем в этой части списка литературы пришлось прибегнуть к двойной нумерации входящих в нее книг. Наконец, последнюю часть списка литературы составляют работы, на которые в тексте книги имеются прямые ссылки.

В заключение мне хочется поблагодарить за помощь моих друзей Л. И. Головину и Д. Б. Персица, прочитавших рукопись и помогавших в составлении окончательного варианта книги.

И. М. Яглом

Глава 1

АЛГЕБРА ЧИСЕЛ И АЛГЕБРА МНОЖЕСТВ

1. «СЛОЖЕНИЕ» И «УМНОЖЕНИЕ» В АЛГЕБРЕ МНОЖЕСТВ

Числа, с которыми мы встречаемся в арифметике и в алгебре, могут иметь разную природу — это могут быть целые или рациональные числа (дроби), вещественные или комплексные числа. Современная алгебра имеет дело иногда и с более сложными типами чисел, например с так называемыми *дуальными* числами $x + y\varepsilon$, где x и y вещественны, а $\varepsilon^2 = 0$ (см. [II, с. 87] или [1]), или с *кватернионами* $x + yi + zj + tk$, где x, y, z, t вещественны, $i^2 = j^2 = k^2 = -1$ и $ij = -ji = k$, $ki = -ik = j$, $jk = -kj = i$ (см. [II, с. 84] или [2]). Но независимо от природы рассматриваемых чисел мы всегда ставим в соответствие каждым двум числам a и b два новых числа, обозначаемых через $a + b$ и ab и называемых «суммой» и «произведением» чисел a и b.

Определение суммы и произведения двух чисел в разных случаях будет совершенно разным. Так, для случая ц е л ы х п о л о ж и т е л ь н ы х чисел *сумма* $a + b$ означает число предметов, получаемое при объединении двух наборов предметов, первый из которых содержит a, а второй b предметов (рис. 1, *а*); *произведение* ab означает число предметов в a наборах, каждый из которых содержит b предметов (рис. 1, *б*). Ясно, что эти определения не имеют смысла, если числа a и b — не целые или не положительные; в этих случаях их надо заменить совсем другими соглашениями. Так, например, сумма и произведение р а ц и о н а л ь н ы х чисел (дробей) определяются по правилам:

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1 b_2 + a_2 b_1}{a_2 b_2}, \quad \frac{a_1}{a_2} \cdot \frac{b_1}{b_2} = \frac{a_1 b_1}{a_2 b_2}$$

(здесь a_1, b_1, a_2, b_2 — целые числа); для в е щ е с т в е н н ы х чисел существует, скажем, правило

$$(-a) \cdot (-b) = ab;$$

сумма и произведение к о м п л е к с н ы х чисел определяются так:

$$(a_1 + a_2 i) + (b_1 + b_2 i) = (a_1 + b_1) + (a_2 + b_2) i,$$

$$(a_1 + a_2 i)\cdot(b_1 + b_2 i) = (a_1 b_1 - a_2 b_2) + (a_1 b_2 + a_2 b_1) i$$

(здесь a_1, a_2, b_1, b_2 — вещественные числа) и т. д.

Единые названия «сумма» и «произведение» для операций, определенных для объектов («чисел») разной природы и вводимых совсем по-разному, оправдываются тем, что во всех случаях общие законы действий над числами остаются одними и теми же. Вот эти законы:

а) $a+b=b+a$, б) $ab=ba$; (1.1)
(коммутативный закон для сложения) (коммутативный закон для умножения)

а) $(a+b)+c=a+(b+c)$, б) $(ab)c=a(bc)$; (1.2)
(ассоциативный закон для сложения) (ассоциативный закон для умножения)

$(a+b)c=ac+bc$. (1.3а)
(дистрибутивный закон)

Далее, во всех случаях существуют два замечательных числа, обозначаемых символами 0 и 1, таких, что прибавление первого из них к любому числу и умножение любого числа на второе не меняют самого числа:

а) $a+0=a$ и б) $a\cdot 1=a$. (1.4)

Сохранение общих свойств сложения и умножения для чисел разной природы чрезвычайно удобно: оно позволяет на каждом этапе расширения понятия числа (при переходе от целых положительных чисел к относительным числам или к дробям, при переходе от вещественных чисел к комплексным и т. д.) не переучиваться, полностью использовать навыки, полученные ранее при изучении чисел другой, более простой природы. Собственно, именно это сходство и делает допустимым использование названий «сложение» или «умножение» для обозначения, казалось бы, совершенно разных операций и употребление одного термина «число» для разных объектов.

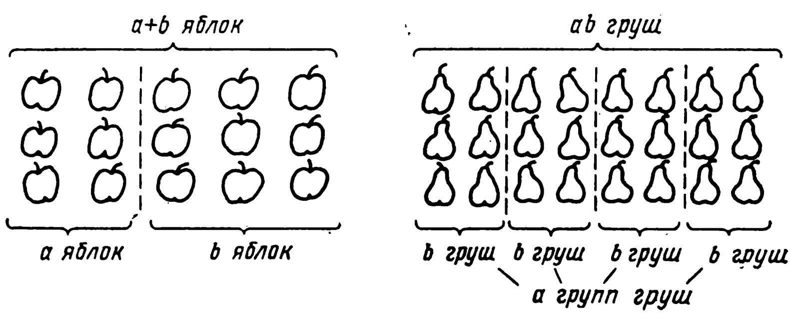


Рис. 1

Иногда свойства (1)—(4) берут за основу при о п р е д е л е н и и операций сложения и умножения, т. е. рассматривают произвольные множества элементов, для которых определены две (не описываемые явным образом) операции, сопоставляющие двум элементам a и b третий элемент $c = a + b$ и $d = ab$ соответственно, причем от этих операций требуется только, чтобы они удовлетворяли условиям (1)—(4) (и некоторым другим дополнительным условиям). Полученную таким путем алгебраическую систему или алгебраическую структуру называют *полем* или *кольцом* в зависимости от того, какие дополнительные требования предъявляются к операциям сложения и умножения (см. [11, с. 82—87] или [3]). Мы, однако, займемся здесь алгебраическими системами, отличными от колец и полей.

Заметим еще, что одна из перечисленных в начале параграфа числовых систем — система кватернионов — не удовлетворяет всем выписанным законам: умножение кватернионов не коммутативно, т. е. для двух кватернионов a и b, вообще говоря, $ab \neq ba$. Однако все остальные правила действий (1а), (2), (3а), (4) остаются в силе и для кватернионов: кватернионы образуют «почти поле», хотя и не совсем точно поле. Для того чтобы включить кватернионы в множество объектов, изучаемых в теории полей, иногда исключают правило (1б) из тех, которые определяют поле (из аксиом поля), говоря, что кватернионы образуют *некоммутативное поле* (подобно тому, как кольца бывают коммутативными и некоммутативными, унитальными и неунитальными, причем условия коммутативности и существования единицы или унитальности могут включаться или не включаться в аксиомы кольца — ср. [11], с. 82). Чаще, однако, алгебраические системы, отличающиеся от поля лишь тем, что правило (1б) может и не иметь места, рассматривают отдельно, присваивая таким системам специальное название («тело»).

При рассмотрении законов (1)—(4) сразу бросается в глаза, что законы сложения очень похожи на законы умножения:

а) $a + b = b + a$ и б) $ab = ba$; (1.1)

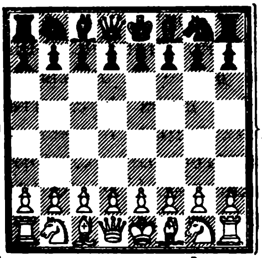
а) $(a + b) + c = a + (b + c)$ и б) $(ab)c = a(bc)$; (1.2)

а) $a + 0 = a$ и б) $a \cdot 1 = a$. (1.4)

Заметим, впрочем, что сходство между действиями сложения и умножения не простирается слишком далеко. Так, например, число 0 играет особую роль не только по отношению к сложению, но и по отношению к умножению: эта особая роль числа 0 определяется замечательным равенством

$a \cdot 0 = 0$. (1.5б)

[Из этого равенства, в частности, вытекает, что число $a \neq 0$ нельзя делить на нуль.] В противоположность этому число 1 по отношению к сложению не играет никакой особой роли; равенство, которое полу-

a)  I

б) 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ... } I

Рис. 2

чается из равенства $a \cdot 0 = 0$ заменой числа 0 числом 1 и умножения сложением:

$$a + 1 = 1, \qquad (1.5а)$$

почти никогда не будет верным. [Это равенство справедливо лишь при $a = 0$.]

Так же и дистрибутивный закон $(a + b)c = ac + bc$ подчеркивает различие между действиями сложения и умножения. Если заменить в записи этого закона сложение умножением и наоборот, то мы получим курьезное «равенство»

$$(ab) + c = (a + c)(b + c), \qquad (1.3б)$$

как правило, не выполняющееся. [Это равенство справедливо лишь при $c = 0$ и при $a + b + c = 1$.]

В математике, однако, встречаются и отличные от чисел объекты, для которых можно определить две операции, аналогичные сложению и умножению. При этом иногда удается прийти к «алгебре», в которой сходство между ~~операциями «сложения» и «умножения» оказывается~~ бо́льшим, чем в обычной алгебре чисел. В качестве примера мы остановимся здесь на своеобразной **алгебре множеств**.

Рассмотрим систему всевозможных множеств (совокупностей) тех или иных объектов; для конкретности мы вначале все время будем говорить о множестве шахматных фигур (конечное множество; рис. 2, *а*) и о множестве натуральных (целых положительных) чисел (бесконечное множество; рис. 2, *б*), хотя на самом деле элементами рассматриваемых множеств могут служить объекты какой угодно (и даже неопределенной) природы. Нам только нужно будет в дальнейшем, чтобы общее множество всех рассматриваемых элементов (множество всех фигур или множество всех чисел) было четко очерчено; это множество мы будем называть *универсальным* множеством и обозначать буквой I (множества мы будем обозначать большими буквами латинского алфавита).

Сумму $A + B$ двух множеств A и B мы определим как такое множество C, которое получается при о б ъ е д и н е н и и множеств A и B. Так, например, если A есть множество всех белых фигур, а B — множество ферзей, то $A + B = C$ состоит из всех белых фигур и черного ферзя (рис. 3, *а*); если A есть множество всех натуральных чисел, делящихся на 2, а B — множество всех чисел, делящихся на 3, то $A + B = C$ состоит из всех чисел, делящихся на 2 или на 3 (рис. 3, *б*).

То обстоятельство, что мы назвали «сложением» совершенно новую операцию, не должно нас смущать: ведь мы и раньше каждый раз, когда переходили от чисел одной природы к числам другой, определяли сложение по-новому. Ясно, например, что сложение положи-

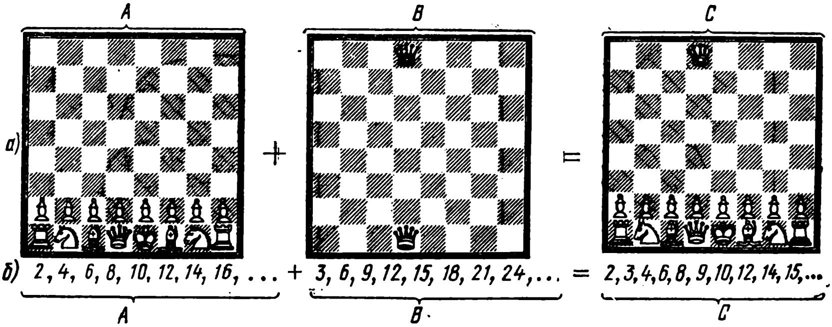


Рис. 3

тельных и отрицательных чисел — это не то же самое, что сложение одних положительных чисел; так, *сумма* чисел (— 5) и (8) — это то же самое, что разность чисел 8 и 5. Точно так же сложение дробей — это не то же самое, что сложение целых чисел: ясно, что указанное на с. 7 определение сложения целых положительных чисел (см. рис. 1, *а*) совершенно непригодно для определения сложения дробей. Употребление во всех случаях одного и того же термина «сложение» мы оправдывали тем, что общие законы, которым подчиняется операция сложения целых чисел, остаются в силе и при переходе, скажем, к дробям: так, в обоих случаях сложение коммутативно (см. (1а)) и ассоциативно (см. (2а)).

Посмотрим теперь, сохраняют ли силу эти законы и для множеств. При этом нам удобно будет использовать специальные диаграммы, иллюстрирующие действия над множествами. Условимся обозначать множество всех рассматриваемых элементов (скажем, множество всех шахматных фигур или множество всех натуральных чисел) в виде квадрата; в этом квадрате можно отметить точки, обозначающие конкретные элементы нашего множества[1]. При этом отдельные множества элементов, взятых из тех, которые составляют «полное» (универсальное) множество (множества шахматных фигур или множества натуральных чисел), будут изображаться частями квадрата. Такие диаграммы часто называют *диаграммами Венна* — по имени

---

[1] Разумеется, такое сопоставление отдельных точек квадрата элементам рассматриваемого множества возможно лишь тогда, когда мощность всех элементов этого множества не превышает мощности континуума — мощности всех точек квадрата. Так, например, можно противопоставить какие-то 32 точки квадрата 32 шахматным фигурам; можно также выбрать каким-либо способом счетное множество точек квадрата и сопоставить их с целыми числами. Однако общие законы алгебры множеств нисколько не зависят от мощности рассматриваемого множества.

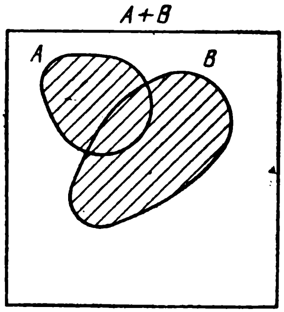


Рис. 4

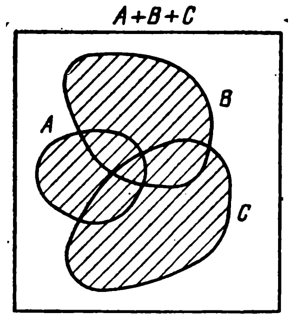


Рис. 5

английского священника Джона Венна (1834—1923)[1], применявшего их в своих исследованиях по логике (см. [2.3]). Правильнее, однако, было бы назвать их *диаграммами Эйлера*, поскольку задолго до Венна их употреблял знаменитый Леонард Эйлер (1707—1783) — швейцарский математик, много лет живший и работавший в Петербурге[2].

Ясно, что множество $A + B$ будет изображаться объединением фигур, отвечающих множествам A и B (рис. 4). Из определения суммы двух множеств A и B непосредственно следует, что

$$A + B = B + A \tag{Ia}$$

(*коммутативный* закон для сложения множеств; рис. 4), а также

$$(A + B) + C = A + (B + C) \tag{IIa}$$

(*ассоциативный* закон для сложения множеств; рис. 5). Сумму $(A + B) + C = A + (B + C)$ естественно обозначать просто через $A + B + C$ (без скобок); она означает объединение трех множеств A, B, C (т. е. в сумму $A + B + C$ входят все элементы, принадлежащие хотя бы одному из множеств A, B и C).

Определим теперь *произведение* AB двух множеств A и B как множество D, получаемое в пересечении множеств A и B; дру-

[1] Впрочем, став доктором наук и будучи избран в Академию — английское Королевское общество, Венн полностью отказался от церковной деятельности в пользу занятий математической логикой — и даже оформил письменный документ, удостоверяющий его неспособность к исполнению обязанностей священника.

[2] В замечательных «Письмах немецкой принцессе» (1768) Л. Эйлер, объясняя своей корреспондентке простоту аристотелевой силлогистики, систематически изображал отдельные множества объектов кругами на плоскости; соответствующие диаграммы (мало существенно, разумеется, отличающиеся от диаграмм Венна) часто называют *кругами Эйлера*. [Впрочем, подобные графические иллюстрации теоретико-множественных и логических зависимостей встречались и до Эйлера, например, в весьма примечательных, но, к сожалению, оставшихся неопубликованными заметках по логике Готфрида Вильгельма Лейбница (1646—1716); см. [2, 3].]

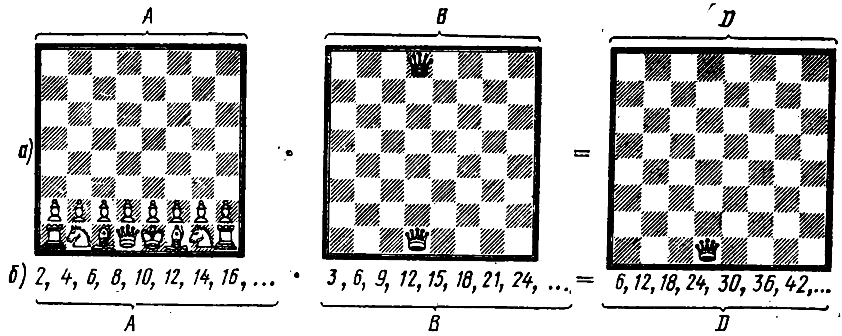


Рис. 6

гими словами, в множество $AB = D$ входят те и только те элементы, которые входят как в множество A, так и в множество B. Так, например, если A и B—это указанные выше множества шахматных фигур или натуральных чисел, то множество $AB = D$ состоит соответственно из одного только белого ферзя (рис. 6, *а*) или из всех чисел, которые делятся на 6 (рис. 6, *б*). На рис. 7 множество AB изображено на диаграмме Венна как пересечение фигур A и B.

Использование знакомого термина «произведение» в совершенно новом смысле оправдывается тем обстоятельством, что из самого определения произведения множеств следует выполнимость для него основных свойств умножения чисел:

$$AB = BA \tag{Iб}$$

(*коммутативный* закон для умножения множеств; рис. 7);

$$(AB)\,C = A\,(BC) \tag{IIб}$$

(*ассоциативный* закон для умножения множеств; рис. 8).

Множество $(AB)\,C = A\,(BC)$ естественно обозначать просто через ABC (без скобок); оно состоит из тех и только тех элементов, кото-

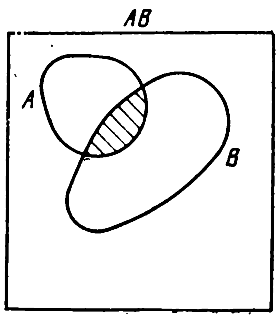


Рис. 7

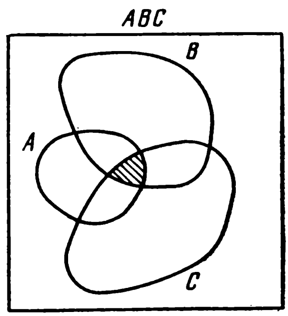


Рис. 8

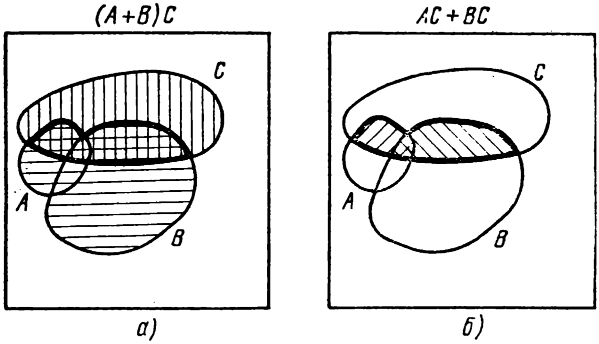


Рис. 9

рые принадлежат к а ж д о м у из множеств A, B и C (представляет собой пересечение т р е х множеств).

Проверим теперь, выполняется ли для множеств дистрибутивный закон (3а).

◀На рис. 9, *а* заштрихованы множества $A + B$ и C; при этом двойной штриховкой оказывается покрыто множество $(A + B)\,C$. На рис. 9, *б* различно заштрихованы множества AC и BC; при этом заштриховано на рисунке множество $AC + BC$. Но легко видеть, что множество, покрытое двойной штриховкой на рис. 9, *а*,— это в точности то множество, которое заштриховано на рис. 9, *б*.▶

Итак, мы видим, что в алгебре множеств выполняется и дистрибутивный закон:

$$(A + B)\,C = AC + BC. \tag{IIIa}$$

Покажем, что и равенства (4) и (5а) также переносятся в алгебру множеств. Нетрудно понять, что роль единицы этой алгебры будет играть «полное» или универсальное множество I: для любого множества A

$$A \cdot I = A. \tag{IVб}$$

Так, произведение (пересечение) множества A всех белых фигур и множества всех вообще шахматных фигур состоит из белых фигур, а произведение множества ферзей и множества всех фигур состоит из ферзей. Роль нуля алгебры множеств играет так называемое *пустое* множество O, вовсе не содержащее никаких элементов: ясно, что при любом множестве A

$$A + O = A. \tag{IVa}$$

Наконец,

$$AO = O, \tag{Vб}$$

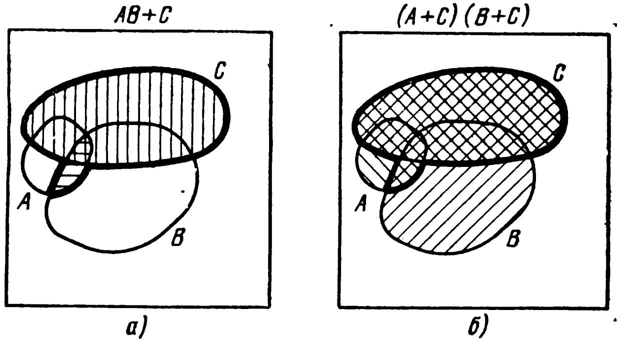


Рис. 10

ибо все элементы множества AO должны принадлежать как множеству A, так и пустому множеству O, в то время как множеству O не принадлежит ни один элемент универсального множества.

Все рассматриваемые до сих пор законы действий над множествами совпадали с законами действий над числами; может даже создаться впечатление, что алгебра множеств представляет собой частный случай той же общей алгебраической схемы, что и, скажем, алгебра вещественных чисел. Однако на самом деле это представление совершенно ошибочно. Алгебра множеств вовсе не копирует точно числовую алгебру; она обладает многими своеобразными свойствами, не выполняющимися ни для одной из изучаемых в средней и высшей школе числовых систем.

Демонстрацию своеобразия алгебры множеств мы начнем с несправедливого в области чисел равенства (5а). Если заменить в нем числа множествами, то получим

$$A + I = I. \tag{Va}$$

Но ясно, что это равенство имеет место при любом множестве A: ведь в сумму $A + I$, по определению, входят все элементы, принадлежащие слагаемому I, т. е. все без исключения элементы универсального множества.

Рассмотрим далее *второй дистрибутивный закон* (3б), получаемый из первого дистрибутивного закона (3а) заменой сложения умножением и наоборот. Как уже указывалось, в алгебре чисел этот закон, вообще говоря, места не имеет. По-другому обстоит дело в алгебре множеств.

◀ На рис. 10, *а*, по-разному заштрихованы множества AB и C. На рис. 10, *б* заштрихованы множества $A + C$ и $B + C$; двойной штриховкой здесь покрыто множество $(A + C)(B + C)$. Но легко видеть, что множество, покрытое на рис. 10, *б* двойной штриховкой,— это в точности то множество, которое заштриховано на рис. 10, *a*, т. е. множество $AB + C$. ▶

Таким образом, в алгебре множеств наряду с (IIIa) выполняется и второй дистрибутивный закон: для любых трех множеств A, B и C

$$AB + C = (A + C)(B + C). \qquad \text{(IIIб)}$$

Отметим еще необычные равенства:

а) $A + A = A$ и б) $AA = A$ (VI)

(выражающие так называемые *идемпотентные* законы), также выполняющиеся для каждого множества A. В самом деле, сумма $A + A$ представляет собой объединение множества A с самим собой; но это, разумеется, то же множество A. Аналогично этому произведение AA — пересечение множества A с самим собой, — не отличается от множества A. Наконец, иногда оказываются полезными следующие тождества алгебры множеств, также не выполняющиеся в числовых алгебрах:

а) $A + AB = A$ и б) $A(A + B) = A$; (VII)

эти тождества выражают так называемые *законы поглощения* (или *абсорбции*). Равенство (VIIa) следует из того, что множество AB составляет ч а с т ь множества A (см. рис. 7) и поэтому «поглощается» множеством A в том смысле, что сумма $A + AB$ совпадает с A. Аналогично устанавливается и справедливость равенства (VIIб), вытекающая из того, что A есть часть множества $A + B$.

Исходя из правил действий над множествами (I)—(VII), в чем-то копирующих хорошо знакомые нам арифметические и алгебраические законы, а в чем-то весьма своеобразно их искажающих (второй дистрибутивный закон (IIIб) или идемпотентные законы (VI)!), можно развить содержательную алгебру множеств, включающую учение о тождественных равенствах и (см. ниже § 3) неравенствах, теорию решения уравнений и неравенств и т. д.; эта алгебра, по своей содержательности не уступающая школьной алгебре, в ряде отношений оказывается проще нее. Мы не ставим перед собой задачу глубокого изучения алгебры множеств (в частности, в этой книге будет полностью обойден вопрос о решении уравнений в алгебре множеств), а ограничимся лишь некоторыми первоначальными сведениями из нее; в частности, в § 2 мы вскроем основную причину, делающую алгебру множеств более простой, чем алгебра чисел.

Пример. Докажем, что в алгебре множеств всегда (при любых множествах A, B и C)

$$(A + B)(B + C)(C + A) = AB + BC + CA$$

(см. также ниже упр. 4).

◀ Согласно правилам (I)—(VII) имеем

$$(A+B)(B+C)(C+A) \underset{(\text{IIб})}{=} (A+B)[(B+C)(C+A)] \underset{(\text{Ia})}{=}$$

$$= (A+B)[(C+B)(C+A)] \underset{(\text{IIIб})}{=} (A+B)(C+AB) \underset{(\text{IIIa})}{=} (A+B)C +$$

$$+ (A+B)(AB) \underset{(\text{Iб})}{=} C(A+B) + (AB)(A+B) \underset{(\text{IIIa})}{=} (CA +$$

$$+ CB) + (ABA + ABB) \underset{(\text{Iб, IIa})}{=} CA + BC + AAB + ABB \underset{(\text{VIб})}{=} CA +$$

$$+ BC + AB + AB \underset{(\text{VIa})}{=} CA + BC + AB \underset{(\text{Ia})}{=} AB + BC + CA. \ ▶$$

Мы видим, что правила алгебры множеств во многом отличны от правил, имеющих место в области чисел: ряд законов обычной числовой алгебры теряет силу при переходе к алгебре множеств и наоборот. В этой связи определенные выше операции над множествами часто называют не суммой и произведением множеств, а *объединением* и *пересечением* и обозначают специальными знаками $\bigcup$ и $\bigcap$, не подсказывающими аналогий с операциями над числами. Мы, однако, предпочтем во всех случаях использовать привычные знаки сложения и умножения.

Упражнения. 1.1. Докажите следующие тождества алгебры множеств:

а) $A(A+C)(B+C) = AB + AC$;

б) $(A+B)(A+C)(B+D)(C+D) = AD + BC$;

в) $(A+B)(B+C)(C+D) = AC + BC + BD$;

г) $(A+B+C)(B+C+D)(C+D+A) = AB + AD + BD + C$;

д) $(A+B+C)(A+B+D)(A+C+D)(B+C+D) = AB + AC + AD + BC + BD + CD$;

е) $(A+B)(A+C)(A+D)(B+C)(B+D)(C+D) = ABC + ABD + ACD + BCD$

1.2. Упростите следующие выражения алгебры множеств:

а) $(A+B)(A+I) + (A+B)(B+O)$;

б) $(A+B)(B+I)(A+O)$;

в) $A + AB + ABC + ABCD + BCD + CD + D$,

где, как всегда, O и I — пустое и универсальное множества.

1.3. Докажите следующее обобщение дистрибутивных законов (III):

а) $(A_1 + A_2 + \ldots + A_n)B = A_1B + A_2B + \ldots + A_nB$;

б) $(A+B_1)(A+B_2)\ldots(A+B_n) = A + B_1B_2\ldots B_n$

1.4. Пусть $A_1, A_2, \ldots, A_n \in I$ — какие-то n множеств; докажите, что для любого натурального k (где $1 \leqslant k \leqslant n$) сумма всевозможных k-кратных произведений наших множеств равна произведению всевозможных $(n-k+1)$-кратных сумм тех же множеств [Примечание: разобранный в тексте (с 16) пример отвечает случаю $n = 3$ $k = 2$, а результаты упр 1 д), е) — случаям $n = 4$, $k = 2$ и $n = 4$, $k = 3$.]

Выше мы ввели две операции, сопоставляющие с каждыми двумя множествами A и B новые множества $C = A + B$ и $D = AB$; эти операции мы назвали сложением и умножением множеств. В математике операции такого рода, сопоставляющие с каждыми двумя элементами a и b какой-то определенной природы третий элемент c, полностью определяемый элементами a и b, называют *бинарными операциями*; в анализе им отвечают *функции двух переменных* $c = f(a, b)$. Таким образом, сложение и умножение множеств — это бинарные операции, определенные в области рассматриваемых нами множеств, подобно тому как сложение и умножение чисел — это бинарные операции в множестве чисел.

Анализируя операции сложения и умножения множеств, мы установили ряд правил или законов, которым подчиняются эти две операции. При этом сразу бросается в глаза глубокая аналогия между правилами, относящимися к сложению множеств, и правилами умножения. Перепишем снова установленные нами правила:

а) $A + B = B + A$ и б) $AB = BA$; (I)

а) $(A + B) + C = A + (B + C)$ и б) $(AB)C = A(BC)$; (II)

а) $(A + B)C = AC + BC$ и б) $AB + C = (A + C)(B + C)$; (III)

а) $A + O = A$ и б) $AI = A$; (IV)

а) $A + I = I$ и б) $AO = O$; (V)

а) $A + A = A$ и б) $AA = A$; (VI)

а) $A + AB = A$ и б) $A(A + B) = A$. (VII)

Эта таблица создает впечатление, что *всякое равенство, тождественно выполняющееся в алгебре множеств, при замене знака сложения знаком умножения и наоборот и пустого множества O* (если только оно входит в первоначальное равенство) *универсальным множеством I и наоборот переходит в новое равенство, также тождественно имеющее место*. Последнее утверждение представляет большую ценность: оно позволяет из всякого равенства алгебры множеств получить еще одно равенство, которое уже не нужно доказывать, поскольку справедливость его автоматически вытекает из справедливости первоначального равенства[1]. Оно составляет содержание **принципа** (или закона) **двойственности** алгебры множеств, а равенства, получаемые одно из друго-

[1] Разумеется, в принципе возможен случай, когда тождество, двойственное данному равенству, не отличается от исходного — так, например, применяя принцип двойственности к доказанному на с. 16—17 тождеству, мы получим $AB+BC+CA = (A+B)(B+C)(C+A)$, т. е. то же самое тождество. Однако случаи такого рода, когда указанное преобразование тождества ничего нам не дает, являются, разумеется, исключением, а не правилом.

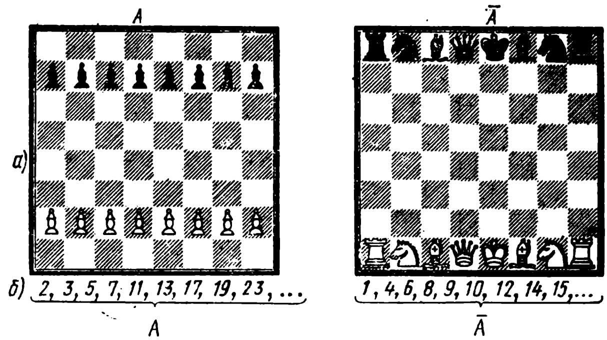


Рис. 11

го с помощью этого принципа, называются *двойственными* друг другу. Сейчас мы докажем принцип двойственности в общем виде.

Для доказательства нам понадобится еще одна своеобразная операция алгебры множеств, сопоставляющая новое множество не с двумя заданными множествами A и B, а с одним множеством A. В математике операции, сопоставляющие новый элемент b одному элементу a, называются *унарными операциями*; этим операциям отвечают *функции одного переменного* $b = f(a)$. В области чисел унарными операциями являются, например, операция образования числа $1/a$, обратного a, операция взятия логарифма $\log a$ числа a или (в области комплексных чисел) операция образования числа $\bar{z}$, сопряженного исходному числу z. Операция в области множеств, о которой идет речь, называется образованием *дополнения* множества; она обозначается чертой, поставленной над рассматриваемым множеством. А именно, через $\bar{A}$ (читается «дополнение A») мы будем обозначать множество всех элементов универсального множества I, не принадлежащих множеству A. Так, если A есть множество всех пешек, то $\bar{A}$ состоит из всех отличных от пешек шахматных фигур (рис. 11, *а*); если A есть множество всех простых чисел, то $\bar{A}$ состоит из всех не простых чисел (т. е. из единицы и всех составных чисел; рис. 11, *б*) и т. д. На диаграмме Венна множество $\bar{A}$ изображается частью квадрата I, не покрытой фигурой A (рис. 12).

Ясно, что

$$\text{а) } A + \bar{A} = I \text{ и б) } A\bar{A} = O; \tag{VIII}$$

эти равенства можно даже принять за определение множества $\bar{A}$. Отметим еще, что

$$\bar{\bar{A}} = A \tag{IX}$$

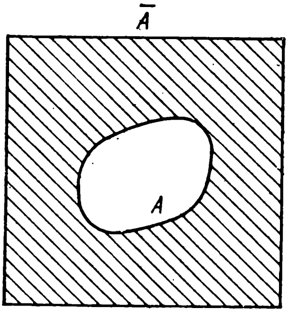


Рис. 12

— дополнение множества $\bar{A}$ совпадает с исходным множеством A. Наконец, очевидно, что

а) $\bar{I} = O$ и б) $\bar{O} = I$. (X)

Свойство (IX) означает взаимный характер операции взятия дополнения множества (или операции «черта», как мы будем также иногда ее называть, имея в виду принятое обозначение $\bar{A}$ дополнения множества A): ведь в силу (IX),

если $B = \bar{A}$, то и $A = \bar{B}$. (IX′)

Из известных нам операций алгебры чисел аналогичным свойством обладают, скажем, операции образования обратного и противоположного числа, ибо,

если $b = 1/a$, то $a = 1/b$ (и, значит, $1/(1/a) = a$);

если $b = -a$, то $a = -b$ (и, значит, $-(-a) = a$)

(или операция сопряжения, сопоставляющая комплексному числу z «сопряженное» число $\bar{z}$), но, конечно, не операции log или $\sqrt{\ }$ (поскольку, как правило, $\log\log x \neq x$ и $\sqrt{\sqrt{x}} \neq x$). В математике принято называть обладающие свойством взаимности унарные операции *инволютивными операциями* или *инволюциями*; таким образом, образование дополнения является инволютивной операцией алгебры множеств (подобно тому, как в арифметике инволюциями являются операции образования обратного, противоположного или сопряженного комплексного числа).

Очень важную роль играют в алгебре множеств следующие два соотношения:

а) $\overline{A+B} = \bar{A}\,\bar{B}$ и б) $\overline{AB} = \bar{A} + \bar{B}$ (XI)

или словами: *дополнение суммы двух множеств совпадает с произведением дополнений этих множеств; дополнение произведения двух множеств совпадает с суммой дополнений этих множеств* (правила де Моргана)[1].

◀ На рис. 13,*а* заштрихованы множества A и B, а на рис. 13,*б* — их дополнения $\bar{A}$ и $\bar{B}$. Но ясно, что фигура, заштрихованная на рис. 13,*а*, и фигура, покрытая двойной штриховкой на рис. 13,*б*, дополняют друг друга до полного квадрата I; это и доказывает, что $\overline{A + B} = \bar{A}\bar{B}$. Аналогично дополняют друг друга до полного квад-

[1] Аугустус де Морган (A. de Morgan, 1806—1871) — известный английский математик (ср. с. 111—112).

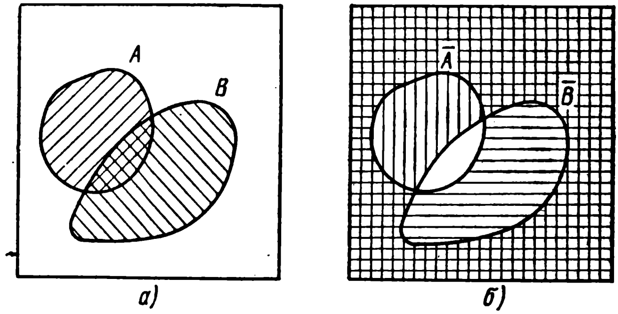


Рис. 13

рата I фигура, покрытая двойной штриховкой на рис. 13,*а*, и фигура, заштрихованная на рис. 13,*б*; это доказывает равенство $\overline{AB} = \bar{A} + \bar{B}$. ▶

Теперь мы можем уже доказать принцип двойственности алгебры множеств.

◀ Пусть

$$\Phi = \Psi, \tag{2.1}$$

где слева и справа стоят какие-то «многочлены» Φ и Ψ, образованные из множеств A, B, C, ... с помощью сложения и умножения. Из равенства (1), очевидно, следует

$$\bar{\Phi} = \bar{\Psi}, \tag{2.1'}$$

где $\bar{\Phi}$ и $\bar{\Psi}$ — дополнения множеств Φ и Ψ. Предположим теперь, что последнее действие, которое нам надо произвести для того, чтобы образовать множество Φ, — это сложение; другими словами, пусть

$$\Phi = \Phi_1 + \Phi_2,$$

где Φ_1 и Φ_2 — два других «сложных» множества, образованные с помощью действий сложения и умножения из первоначальных «простых» множеств A, B, C, ... Тогда в силу первого из правил де Моргана

$$\bar{\Phi} = \bar{\Phi}_1 \cdot \bar{\Phi}_2.$$

Напротив, если последнее действие, осуществление которого приводит к образованию множества Φ, является умножением, т. е. мы имеем

$$\Phi = \Phi_1 \cdot \Phi_2,$$

то из второго правила де Моргана следует

$$\bar{\Phi} = \bar{\Phi}_1 + \bar{\Phi}_2.$$

Упрощая далее таким же образом, с помощью правил де Моргана (XI), множества Φ_1 и Φ_2, мы убеждаемся, что множество $\overline{\Phi}$ получается из множества Φ заменой исходных множеств A, B, C,... их дополнениями $\overline{A}$, $\overline{B}$, $\overline{C}$, ... и заменой в алгебраическом выражении для Φ каждого действия сложения действием умножения и наоборот, а также заменой пустого множества O (если оно входит в выражение Φ) универсальным множеством I и наоборот (ср. (X)). Так, например, если

$$\Phi = (A + B + CD)(AB + CD + ABCD),$$

то

$$\overline{\Phi} = [\overline{A}\,\overline{B}(\overline{C} + \overline{D})] + [(\overline{A} + \overline{B})(\overline{C} + \overline{D})(\overline{A} + \overline{B} + \overline{C} + \overline{D})]$$

(проверьте!). Аналогично этому получается и множество $\overline{\Psi}$ из множества Ψ.

Предположим теперь, что равенство (1) является *тождеством*, т. е. справедливо при любых множествах A, B, C, ... В таком случае и равенство (1′) — тоже тождество, т. е. оно выполняется при любых множествах $\overline{A}$, $\overline{B}$, $\overline{C}$, ... А так как и A, B, C, ..., и $\overline{A}$, $\overline{B}$, $\overline{C}$, ... — произвольные множества, то мы можем в равенстве (1′) несколько изменить обозначения, условившись писать не $\overline{A}$, а по-прежнему A; не $\overline{B}$, а по-прежнему B и т. д. При этом мы придем к равенству

$$\Phi_1 = \Psi_1, \tag{2.1″}$$

где выражения Φ_1 и Ψ_1 получаются из выражений Φ и Ψ по правилам, указанным в принципе двойственности. Принцип двойственности утверждает, что из тождественного выполнения равенства (1) вытекает и тождественное выполнение равенства (1″),— но это мы только что доказали! ▶

Заметим еще, что наше доказательство принципа двойственности позволяет несколько расширить его формулировку. До сих пор мы говорили только о таких равенствах, в составлении которых участвуют лишь действия сложения и умножения. Однако правило (IX) позволяет распространить принцип двойственности и на равенства, составленные при участии операции взятия дополнения множества. Очевидно, что если в выражении Φ фигурирует, скажем, множество $\overline{A}$, то соответствующий член выражения $\overline{\Phi}$ будет содержать множество $(\overline{\overline{A}}) = A$; при переходе же к выражению Φ_1, которое получается из $\overline{\Phi}$ заменой $\overline{A}$ на A, $\overline{B}$ на B и т. д., у нас снова возникнет множество $\overline{A}$. Отсюда видно, что в двойственных друг другу формулах алгебры множеств взятию дополнения множества отвечает та же операция. Так, например, двойственными друг другу являются формулы де Моргана:

$$\overline{A + B} = \overline{A}\,\overline{B} \quad \text{и} \quad \overline{AB} = \overline{A} + \overline{B}.$$

Упражнения. 2.1. Выпишите равенства алгебры множеств, двойственные равенствам, фигурирующим в упр 1.1 а) —е) и 1.2 а)—в).

2.2. Упростите:

а) $(A+B)(A+\overline{B})$;

б) $AB+(A+B)(\overline{A}+\overline{B})$;

в) $\overline{\overline{A}\overline{B}C}\,\overline{\overline{A}B}\,\overline{A}C$;

г) $A+B+C\,\overline{\overline{A}\overline{B}\overline{C}}$;

д) $A+\overline{A}B$.

2.3 Выпишите формулы, двойственные фигурирующим в упр. 2 а)—д).

2.4 Докажите следующие обобщения правил де Моргана (XI):

а) $\overline{A_1+A_2+\ldots+A_n}=\overline{A}_1\,\overline{A}_2\ldots\overline{A}_n$;

б) $\overline{A_1\,A_2\ldots A_n}=\overline{A}_1+\overline{A}_2+\ldots+\overline{A}_n$.

3. МНОЖЕСТВА, ПОДМНОЖЕСТВА, РЕШЕТКИ

Идемпотентные законы

$$а)\ A+A=A \quad и \quad б)\ AA=A \tag{VI}$$

и законы поглощения

$$а)\ A+AB=A \quad и \quad б)\ A(A+B)=A \tag{VII}$$

являются частными случаями более общих соотношений алгебры множеств, связанных со своеобразным упорядочением элементов этой алгебры. Естественно считать, что множество A «не меньше» множества B, если все элементы множества B принадлежат и множеству A. Это отношение между множествами записывается так: $A\supset B$ или $B\subset A$; оно читается: «множество A содержит множество B» или «B содержится в A»[1]. Так, если A есть множество всех белых фигур, B — множество белых пешек, то $A\supset B$; точно так же, если A есть множество четных чисел, а B — множество чисел, десятичная запись которых оканчивается двумя нулями, то $A\supset B$. На диаграмме Венна соотношение $\supset$ иллюстрируется двумя фигурами A и B, причем фигура B целиком содержится в фигуре A (рис. 14) или совпадает с A. При этом очевидно, что для всех A

$$A\supset A \tag{XII}$$

(*рефлексивность* отношения $\supset$);

$$\textit{если } A\supset B \textit{ и } B\supset C, \textit{ то } A\supset C \tag{XIII}$$

---

[1] Отношение $A\supset B$ переносит в область алгебры множеств отношение $a\geqslant b$ (но не $a>b$!) алгебры чисел.

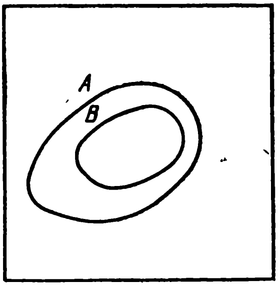


Рис. 14

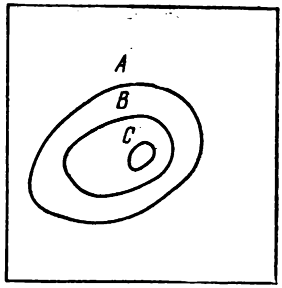


Рис. 15

(*транзитивность* отношения $\supset$; рис. 15) и

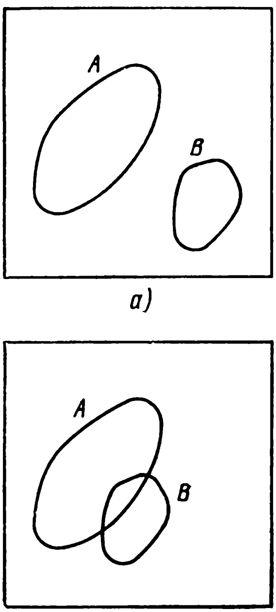
$$\text{если } A \supset B \text{ и } B \supset A, \text{ то } A = B \tag{XIV}$$

(*антисимметричность* отношения $\supset$).

Разумеется, если A и B — произвольные множества (являющиеся подмножествами рассматриваемого универсального множества I), то, вообще говоря (см. рис. 16, *а* или *б*), не имеет места ни одно из отношений $A \supset B$ и $B \supset A$ — отношение между множествами есть отношение *частичного порядка* (ср. [II, с. 94]), но не полного (линейного) порядка. Так, на рис. 17 изображен граф отношения $\supset$ между подмножествами множества $I = A_{1234} = \{a_1, a_2, a_3, a_4\}$, где, скажем, множество

$$A_{ij} = \{a_i, a_j\}, \text{ а } A_{ijk} = \{a_i, a_j, a_k\}$$
$$(i, j, k = 1, \ldots, 4);$$

на этом рисунке соединяющая две точки линия означает, что отвечающее верхней точке множество содержит нижнее (или



а)

б)

Рис. 16

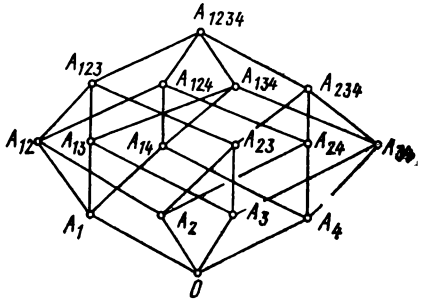


Рис. 17

«меньшее») множество. Из рис. 17 видно, что в то время, как из 16 элементов алгебры подмножеств множества $I = A_{1234}$ можно образовать $(16 \cdot 17)/2 = 136$ пар множеств, отношением связаны из них лишь 81 пара, ибо, скажем, множества A_{123} и A_{134} или A_{124} и A_3 несравнимы, т. е. ни одно из них не «больше» второго[1].

Очевидно, что каково бы ни было множество A, всегда

а) $I \supset A$ и б) $O \subset A$. (XV)

Далее, из определения сложения и умножения множеств (рис. 4 и 7) вытекает, что для любых множеств A и B

а) $A + B \supset A$ и б) $AB \subset A$. (XVI)

Нетрудно видеть также, что

если $A \supset B$, то а) $A + B = A$; б) $AB = B$ (XVII)

(см. рис. 14). Так как $A \supset A$ (см. (XII)) и $A \supset AB$, $A + B \supset A$ (см. (XVI)), то тождества (VI) и (VII) являются следствиями более общих законов (XVII). Это обстоятельство мы и имели в виду, говоря в начале параграфа о возможности обобщить идемпотентные законы и законы поглощения.

Соотношения (XVI) можно еще усилить. Из «симметричности» (коммутативности) операции сложения множеств и (XVI а) следует, что

$$A + B \supset A \text{ и } A + B \supset B.$$

С другой стороны, пусть M — произвольное множество, такое, что

$M \supset A$ и $M \supset B$, (3.1)

другими словами, такое, что M содержит A и M содержит B. Но это утверждение означает, разумеется, что M содержит **объединение** A и B (рис. 18, *а*). Напротив, если

$A \supset N$ и $B \supset N$, (3.1′)

т. е. если N содержится как в множестве A, так и в множестве B, то, очевидно (рис. 18, *б*), N содержится в **пересечении** A и B:

если $M \supset A$ *и* $M \supset B$, *то* $M \supset A + B$; (3.2)

если $N \subset A$ *и* $N \subset B$, *то* $N \subset AB$. (3.2′)

Условимся обозначать символом Max $[A, B]$ любое множество M, большее как A, так и B, т. е. удовлетворяющее (1); «наименьшее» из всех таких множеств M, т. е. такое множество m, что $m \supset A$,

[1] На рис. 17 мы имеем вовсе не 81 дугу, соединяющую отдельные точки, а всего только 32 отрезка. Это связано с тем, что при «чтении» рисунка надо еще учитывать рефлексивность (XII) отношения $\supset$, в силу которой каждая пара A, A связана этим отношением, и транзитивность (XIII), позволяющую заключить, что, скажем, $A_{123} \supset A_3$, ибо соответствующие точки соединены ломаной $A_{123}A_{13}A_3$.

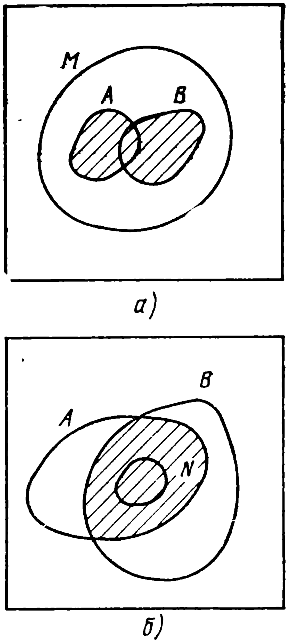


Рис. 18

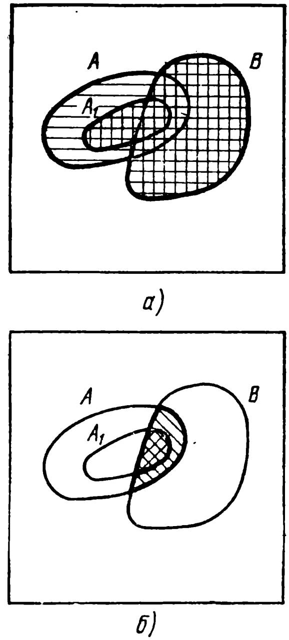


Рис. 19

$m \supset B$ и из (1) следует $M \supset m$, мы назовем (*строгим*) *максимумом* A и B (или *верхней гранью* A и B) и обозначим через max $[A, B]$. Аналогично запись $N = \mathrm{Min}\,[A, B]$ будет означать выполнимость отношений (1′); если же $n \subset A$, $n \subset B$ и из (1′) вытекает $n \supset N$ (т. е. если n — «наибольшее» из множеств N, меньших как A, так и B), то n называется (*строгим*) *минимумом* (или *нижней гранью*) A и B и обозначается символом $\min\,[A, B]$. Теперь соотношения (2) и (2′) позволяют утверждать, что

$$\text{а) } A + B = \max\,[A,B], \quad \text{б) } AB = \min\,[A,B] \qquad \text{(XVIII)}$$

Множество каких-то элементов, для которых введено отношение порядка $\supset$, удовлетворяющее условиям (XII)—(XIV), называется *решеткой*[1], если для каждых двух элементов этого множества существует как их (строгий) максимум (верхняя грань) $\max\,[A, B]$, так и их (строгий) минимум (нижняя грань) $\min\,[A, B]$ (см. [II, с. 95]). Из (XVIII) следует, что *по отношению естественного упорядочения* $\supset$ *множество подмножеств любого универсального множества* I *образует решетку*. При этом соответствующая решетка обладает также *абсо-*

[1] Английское lattice, немецкое Verband; в нашей литературе решетки именуют иногда также *структурами*. По поводу решеток, см., например [2.18, 2.19, 4], первую из книг [3] или Приложение II к книге [8].

лютным максимумом I (элементом, большим всех рассматриваемых элементов — см. (XVa)) и *абсолютным минимумом* O (наименьшим из всех элементов — см. (XV б)).

Перепишем (по существу — равносильные (XVIII)) соотношения (2), (2′) в том виде, в каком мы будем их использовать ниже:

а) *если* $A \supset B$ *и* $A \supset C$, *то* $A \supset B + C$;

б) *если* $B \supset A$ *и* $C \supset A$, *то* $BC \supset A$. (XIX)

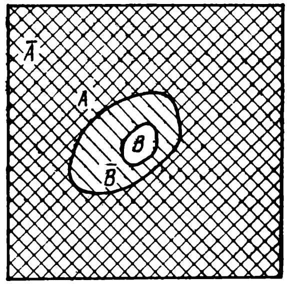


Рис. 20

Заметим, наконец, что введенное в алгебре множеств отношение порядка $\supset$ согласовано с операциями сложения и умножения множеств в том смысле, что

если $A \supset A_1$, *то* а) $A + B \supset A_1 + B$; б) $AB \supset A_1B$ (XX)

при любом множестве B (рис. 19, *а*, *б*). Напротив, с (унарной) операцией $\bar{}$ отношение порядка $\supset$ «противосогласовано» в том смысле, что

если $A \supset B$, *то* $\bar{A} \subset \bar{B}$ (XXI)

(если множество $\bar{A}$ содержит множество B, то множество $\bar{A}$ содержится в множестве $\bar{B}$; рис. 20). Так, например, очевидно, что если множество B умеющих играть в шахматы учеников определенного класса состоит из одних лишь мальчиков (т. е. составляет часть множества A мальчиков), то множество $\bar{B}$ не умеющих играть в шахматы учеников охватывает множество $\bar{A}$ девочек.

Важное условие (XXI) позволяет расширить установленный в § 2 принцип двойственности алгебры множеств, чтобы получать с его помощью новые результаты не только из равенств, но и из «неравенств» алгебры множеств, утверждающих, что из двух составленных из множеств выражений одно всегда «больше» другого. В самом деле, *пусть тождественно имеет место отношение*

$$\Phi \supset \Psi, \tag{3.3}$$

где Φ и Ψ — два выражения алгебры множеств, составленные из некоторых множеств A, B, C, ... с помощью операций сложения, умножения и взятия дополнения; *тогда тождественно имеет место также и соотношение*

$$\Phi_1 \subset \Psi_1, \tag{3.3′}$$

где выражения Φ_1 и Ψ_1 получаются из выражений Φ и Ψ с помощью замены сложения умножением и наоборот и множества O множеством I и наоборот (операция взятия дополнения множества при переходе от (3) к (3′) сохраняется).

◀ Доказательство сформулированного предложения подобно изложенному в § 2 доказательству «узкого» принципа двойственности. В самом деле, из (3) с учетом (XXI) следует

$$\overline{\Phi} \subset \overline{\Psi}, \tag{3.3''}$$

а если неравенство (3) (значит, и (3″)!) тождественно выполняется, то (3″) равносильно (3′). ▶ Так, например, двойственны друг другу соотношения (XVа) и (XVб) или (XVIа) и (XVIб) (см. также ниже упр. 2).

Можно даже считать, что последняя формулировка принципа двойственности является общей, а «узкий» принцип двойственности § 2 представляет собой следствие этого общего принципа. В самом деле, в силу рефлексивности (XII) и антисимметричности (XIV) отношения $\supset$ равенство (2.1) равносильно двум соотношениям:

$$\Phi \supset \Psi \text{ и } \Phi \subset \Psi.$$

Но в силу «общего» принципа двойственности из этих двух соотношений вытекает, что

$$\Phi_1 \subset \Psi_1 \text{ и } \Phi_1 \supset \Psi_1,$$

а это и устанавливает справедливость равенства (2.1″).

Упражнения. 3.1. Докажите следующие тождественно выполняющиеся неравенства:

а) $A + B + C \supset (A + B)(A + C)$;
б) $(A + B)(A + C)(A + I) \supset ABC$ (где I — универсальное множество);
в) $(A + B)(B + C)(C + A) \supset ABC$;
г) $A + B \supset \overline{A}B + A\overline{B}$.

3.2. Выпишите неравенства, двойственные неравенствам упр. 1 а)—г).

3.3. Докажите, что если $A_1 \supset A_2 \supset \ldots \supset A_n \supset A_1$, то $A_1 = A_2 = A_3 = \ldots = A_n$

4. ВЫЧИТАНИЕ МНОЖЕСТВ — РАЗНОСТЬ И СИММЕТРИЧЕСКАЯ РАЗНОСТЬ

В алгебре чисел, как известно, разность двух чисел a и b определяется так:

$$x = a - b, \text{ если } a = b + x. \tag{4.1}$$

При этом разность $a - b$ существует не всегда: так, например, в множестве целых неотрицательных чисел разность $a - b$ определена только при $a \geqslant b$. Но если бинарная операция «вычитание» на том или ином множестве чисел определена, то она обладает весьма специфическими свойствами, во многом отличными от свойств сложения и умножения. Так, эта операция не коммутативна: вообще говоря,

$$a - b \neq b - a,$$

а не ассоциативна: как правило,

$$(a - b) - c \neq a - (b - c)$$

(для чисел первое неравенство обращается в равенство лишь при $a = b$, а второе — лишь при $c = 0$). С другой стороны, всегда (при всех a)

$$a - a = 0; \qquad (4.1')$$

более того, $a - b = 0$ лишь если $b = a$. Аналогично всегда

$$a - 0 = a, \qquad (4.1'')$$

причем здесь тоже $a - b = a$ только при $b = 0$.

В алгебре множеств не удается определить «разность» A«—»B двух множеств A и B родственным (1) образом:

$$X = A\text{«—»}B, \text{ если } A = X + B. \qquad (4.2)$$

В самом деле, из $A = X + B$ следует, что $A \supset B$ (см. (XVIa)); с другой стороны, поскольку для любого $Z \subset B$ имеем

$$(X + Z) + B = X + (Z + B) = X + B$$

(см. (XVIIa)), то если какое-то X таково, что $A = X + B$, то и каждое $X_1 = X + Z$, где $Z \subset B$, удовлетворяет равенству $A = X_1 + B$ Таким образом, при $A \supset B$ определенное соотношением (2) множество X не единственно, а если отношение $A \supset B$ не имеет места, то X не существует. Поэтому при желании дополнить список операций алгебры множеств операцией вычитания мы должны определить эту операцию как-то по-другому.

Наиболее распространенным является следующее

Определение А. Множество $X = A \setminus B$ называется (*теоретико-множественной*) *разностью* множеств A и B, если элемент $x \in X$ в том и только в том случае, когда $x \in A$ и $x \notin B$:

$$X = A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}. \qquad (4.3)$$

Другими словами,

$$X = A \setminus B = A\overline{B}, \qquad (4.3')$$

где, как всегда, дополнение $\overline{B}$ множества B состоит из всех элементов универсального множества I, не принадлежащих B (рис. 21). Операция образования множества $A \setminus B$ называется (*теоретико-множественным*) *вычитанием* B из A. Если $A \supset B$ (рис. 21, *б*), то наряду с записью $A \setminus B$ применяется и более обычная запись $A - B$.

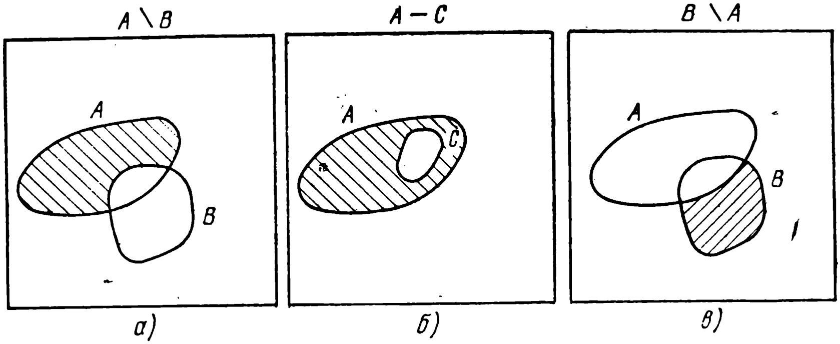


Рис. 21

Очевидны следующие свойства разности:

$P_1 : A \setminus A = O,$

$P_2 : A \setminus O = A,$

$P_3 : O \setminus A = O,$

$P_4 : (A \setminus B) \setminus C = (A \setminus C) \setminus B,$

$P_5 : (A \setminus B)\, C = AC \setminus BC$

(*дистрибутивность* вычитания множеств относительно умножения); здесь всюду A, B, C — произвольные множества. Но, как правило,

$$A \setminus B \neq B \setminus A \tag{4.4}$$

(вычитание множеств не коммутативно — рис. 21, *а*, *в*) и

$$(A \setminus B) \setminus C \neq A \setminus (B \setminus C) \tag{4.4'}$$

(вычитание множеств не ассоциативно[1] — рис. 22).

Равенства P_1 и P_2 близки к свойствам (1′) и (1″) вычитания чисел: однако в то время, как в алгебре чисел равенства $a - b = 0$ и $a - b = a$ выполняются лишь в том случае, когда вычитаемое b равно соответственно a и 0, в алгебре множеств дело обстоит не так: здесь

$P_1' : A \setminus B = O$ равносильно $B \supset A$;

$P_2' : A \setminus B = A$ равносильно $\bar{B} \supset A$ (или $B \subset \bar{A}$).

[Но

$P_1'' : A - B = O$ равносильно $B = A$,

как и в алгебрах чисел; напомним, что из отношений $A \supset B$ и $B \supset A$ следует $A = B$ и что запись $A - B$ применима лишь при $B \subset A$].

[1] Но зато в алгебре множеств имеет место «смешанное» равенство P_4, в известном смысле промежуточное между коммутативностью и ассоциативностью.

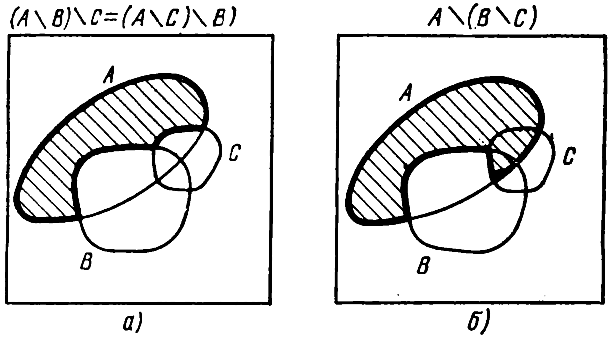


Рис. 22

◀ Ясно, что равенства P_{1-3} и утверждения P_1', P_2' следуют из определения (теоретико-множественного) вычитания множеств. P_4 вытекает из того, что

$$(A\setminus B)\setminus C = A\setminus(B+C) = A\setminus(C+B) = (A\setminus C)\setminus B$$

(рис. 22,*а*; отсюда снова следует неравенство (4′), поскольку в левой его части стоит $A\setminus(B+C)$, а в правой $A\setminus(B\setminus C)$). Справедливость P_5 следует из того, что в левой части этого равенства стоит множество

$$\{x \mid x\in A \text{ и } x\notin B \text{ и } x\in C\},$$

а справа

$$\{x\in A \text{ и } C, \text{ но } x\notin B \text{ и } C\},$$

что, очевидно, то же самое (рис. 23). [Равенства P_4 и P_5 легко также вывести из определения (3′) разности множеств:

$$(A\setminus B)\setminus C = (A\overline{B})\,\overline{C} = (A\overline{C})\,\overline{B} = (A\setminus C)\setminus B$$

(см. (Iб), (IIб)) и

$$(A\setminus B)\,C = (A\overline{B})\,C = (AC)\,\overline{B} = (AC)\,\overline{B} + (AC)\,\overline{C} = AC\,(\overline{B}+\overline{C}) =$$
$$= AC\cdot\overline{BC} = AC\setminus BC$$

(см. (Iб) и (IIб); (VIIIб), (Vб) и (IVa); (XIб)).] ▶

Заметим еще, что, очевидно,

$$\overline{A} = I\setminus A \tag{4.5}$$

и

$$\text{если } AB=O, \text{ то } A\setminus B = A. \tag{4.6}$$

Так как

из $A\setminus B = O$ не следует $A=B$,

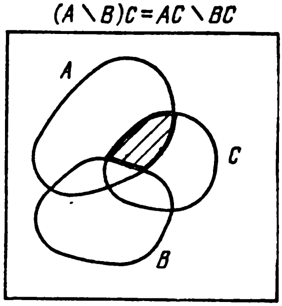


Рис. 23

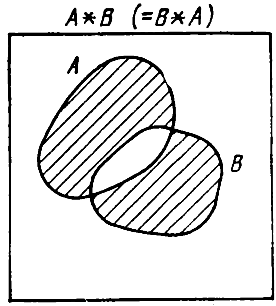


Рис. 24

то наше определение разности двух множеств не особенно удобно — в области чисел соответствующее свойство вычитания мы привыкли считать одним из самых основных. Это обстоятельство оправдывает введение в алгебре множеств еще одной операции «вычитания»:

О п р е д е л е н и е Б. Множество $Y = A * B$ называется *симметрической разностью*[1] множеств A и B, если $y \in Y$ в том и только в том случае, когда y принадлежит р о в н о о д н о м у из множеств A и B:

$$Y = A * B = \{y \mid (y \in A \text{ и } y \notin B) \text{ или } (y \notin A \text{ и } y \in B)\}. \tag{4.7}$$

Другими словами,

$$Y = A * B = A\overline{B} + \overline{A}B \quad (= (A \setminus B) + (B \setminus A)) \tag{4.7'}$$

(рис. 24; операцию образования множества $A * B$ можно назвать *симметрическим вычитанием* B из A). Нетрудно видеть, что

$CP_1 : A * A = O$ и из $A * B = O$ следует, что $B = A$;

$CP_2 : A * O = A$, и если $A * B = A$, то $B = O$;

$CP_3 : A * B = B * A$

(*коммутативность* симметрического вычитания, именно в силу которой множество $A * B$ и называется с и м м е т р и ч е с к о й разностью A и B);

$CP_4 : (A * B) * C = A * (B * C)$

(*ассоциативность* симметрического вычитания; она позволяет вместо левой и правой частей равенства CP_4 писать просто $A * B * C$ без скобок);

$CP_5 : (A * B)\, C = (AC) * (BC)$

---

[1] В литературе для симметрической разности множеств A и B чаще используется обозначение $A \Delta B$ или $A \dot{-} B$.

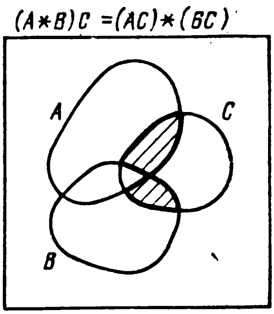


Рис. 25

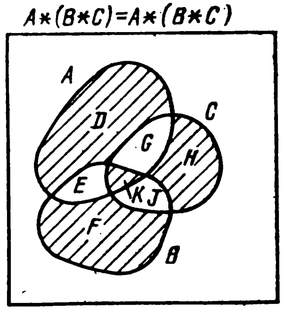


Рис. 26

(*дистрибутивность* симметрического вычитания относительно умножения).

◀ Условия CP_{1-3} вытекают из самого определения симметрической разности. Так, например,

если $A * B = (A \setminus B) + (B \setminus A) = O$, то $A \setminus B = B \setminus A = O$, т. е. $B \supset A$ и $A \supset B$, а значит, $A = B$.

Несколько сложнее доказываются равенства CP_4 и CP_5. Второе из них вытекает из того, что $U = (A * B) C$ — это множество всех $x \in I$, принадлежащих ровно одному из множеств A и B и множеству C, а $V = (AC) * (BC)$ — множество x, принадлежащих AC или BC, но не AC и BC одновременно; но, очевидно, $U = V$ (рис. 25; см. также ниже упр. 6). Равенство CP_4 следует из того, что на рис. 26

$X = A * B = D + G + F + J$, а $C = G + H + J + K$,
в силу чего

$(A * B) * C = X * C = D + F + H + K$.

Аналогично

$Y = B * C = E + F + G + H$, $A = D + E + G + K$,

и поэтому в силу коммутативности и ассоциативности сложения множеств

$A * (B * C) = A * Y = D + K + F + H = X * C = (A * B) * C$

(см. упр. 6). ▶

Заметим еще, что аналогично (5) имеем

$$\bar{A} = I * A \tag{4.5'}$$

(ибо, очевидно, $I * A = I\bar{A} + \bar{I}A = I\bar{A} + OA = \bar{A}$); однако справедливо и родственное (5′) равенство

$$A * \bar{A} = I \tag{4.8}$$

(ибо $A * \bar{A} = A\bar{\bar{A}} + \bar{A}\bar{A} = AA + \bar{A}\bar{A} = A + \bar{A} = I$; см. (IX), (VIб) и (VIIIa)).

Наконец, впоследствии нам будет полезно важное равенство

$$A + B = A * B * (AB). \tag{4.9}$$

◀ Равенство (9) вытекает, например, из следующих преобразований:

$$A * B * (AB) = A * [B * (AB)] = A * [B\overline{AB} + \bar{B}AB] =$$

$$= A * [B(\bar{A} + \bar{B}) + O] = A * \bar{A}B = A\overline{\bar{A}B} + \bar{A}(\bar{A}B) = A \times$$

$$\times (A + \bar{B}) + \bar{A}B = (A + A\bar{B}) + \bar{A}B = A + \bar{A}B = (A + AB) +$$

$$+ \bar{A}B = A + (AB + \bar{A}B) = A + (A + \bar{A})B = A + B$$

(здесь используются кроме коммутативных, ассоциативных, идемпотентных законов, правил (VIIIб) и (IVa) и правил де Моргана также законы поглощения (VIIa)). ▶

Укажем еще, что аналогично свойствам вычитания чисел: если $a - c = b - c$, то $a = b$; если $a - b = c$, то $a - c = b$, имеем

$$\text{если } A * C = B * C, \text{ то } A = B; \tag{4.10}$$

$$\text{если } A * C = B, \text{ то } A * B = C. \tag{4.11}$$

С другой стороны, утверждения

$$\text{если } A \setminus C = B \setminus C, \text{ то } A = B; \tag{4.10$'$}$$

$$\text{если } A \setminus B = C, \text{ то } A \setminus C = B \tag{4.11$'$}$$

уже, вообще говоря, места не имеют (см. упр. 12 и 13).

Упражнения. 4.1. Пусть $A = \{1, 2, 3, 4, 6\}$, $B = \{1, 2, 3, 4\}$, $C = \{1, 2, 5, 6\}$; составьте разности $A \setminus B$, $A \setminus C$, $B \setminus C$, $B \setminus A$, $C \setminus A$, $C \setminus B$ и соответствующие симметрические разности $A * B$, $A * C$, $B * C$; проверьте на этом примере выполнение законов P_4 и P_5; CP_4 и CP_5.

4.2. Докажите следующие тождества алгебры множеств:

а) $(A \setminus B)(A \setminus C) = A \setminus (B + C)$;

б) $(A \setminus B) + (B \setminus C) + (C \setminus A) + ABC = A + (B \setminus A) + [C \setminus (A + B)]$;

в) $A \setminus [(A \setminus B) + (A \setminus C)] = ABC$;

г) $(A \setminus B)(C \setminus D) = AC \setminus (B + D)$.

4.3. Обобщите следующим образом результат упр. 2 б)—г): для любых множеств $A_1, A_2, \ldots, A_n$ и $B_1, B_2, \ldots, B_n$

а) $(A_1 \setminus A_2) + (A_2 \setminus A_3) + \ldots + (A_{n-1} \setminus A_n) + (A_n \setminus A_1) + A_1A_2 \ldots A_n =$
$= A_1 + A_2 + A_3 + \ldots + A_n = A_1 + (A_2 \setminus A_1) + [A_3 \setminus (A_1 + A_2)] + [A_4 \setminus (A_1 +$
$+ A_2 + A_3)] + \ldots + [A_n \setminus (A_1 + A_2 + \ldots + A_{n-1})]$;

б) $A_1 \setminus [(A_1 \setminus A_2) + (A_1 \setminus A_3) + \ldots + (A_1 \setminus A_n)] = A_1A_2 \ldots A_n$;

в) $(A_1 \setminus B_1)(A_2 \setminus B_2) \ldots (A_n \setminus B_n) = A_1A_2 \ldots A_n \setminus (B_1 + B_2 + \ldots + B_n)$.

4.4. Упростите

а) $\overline{A \setminus B}$; б) $\overline{A * B}$,

где операции $\setminus$ и $*$ имеют смысл, определенный выше [Примечание: здесь требуется преобразовать выписанные выражения так, чтобы операция «черта» применялась лишь к индивидуальным множествам, но не к их комбинациям.]

4.5. Обозначим $A/B = A + \overline{B}$ (т. е. $A/B = \{x \mid x$ принадлежит A или x не принадлежит $B\}$). Докажите, что операция $/$ двойственна операции $\setminus$ в смысле § 2; выведите свойства операции $/$, двойственные известным Вам свойствам операции $\setminus$ (в частности, дистрибутивность $(A/B) + C = (A + C)/(B + C)$ этой операции относительно сложения).

4.6. Выведите все свойства $СР_{1-5}$ симметрической разности из ее определения (7′).

4.7. Докажите, что

а) $A * B = (A + B)\,\overline{AB}$;

б) $A * (AB) = A\overline{B}$;

в) $A * (A + B) = \overline{A}B$;

г) $A + (A * B) = A + B$.

4.8. Используйте тождества упр. 7 а), в) для доказательства формулы (9).

4.9. Докажите, что при любом (натуральном) n

а) $(A_1 + A_2 + \ldots + A_n) * (B_1 + B_2 + \ldots + B_n) \subset (A_1 * B_1) + (A_2 * B_2) + \ldots + (A_n * B_n)$;

б) $(A_1 A_2 \ldots A_n) * (B_1 B_2 \ldots B_n) \subset (A_1 * B_1) + (A_2 * B_2) + \ldots + (A_n * B_n)$,

где $A_1, A_2, \ldots, A_n$; $B_1, B_2, \ldots, B_n \subset I$ — какие угодно множества.

4.10. Докажите

а) дистрибутивность сложения множеств относительно вычитания, т. е. равенство $(A + B)\setminus C = (A\setminus C) + (B\setminus C)$;

б) дистрибутивность $(AB)\setminus C = (A\setminus C)(B\setminus C)$ умножения относительно вычитания;

в) антидистрибутивность вычитания относительно сложения, т. е. равенство $A\setminus(B + C) = (A\setminus B)(A\setminus C)$;

г) антидистрибутивность $A\setminus(BC) = (A\setminus B) + (A\setminus C)$ вычитания относительно умножения;

д) дистрибутивность умножения относительно симметрического вычитания, т. е. равенство $(AB) * C = (A * C)(B * C)$.

4.11. Выведите из «антидистрибутивных законов» (упр. 10 в), г)) правила де Моргана (XI).

4.12. Докажите

а) утверждение (10); б) утверждение (11).

4.13. Приведите пример, опровергающий

а) утверждение (10′); б) утверждение (11′).

4.14. Определите (бинарную) операцию $\circ$ алгебры множеств, двойственную (в смысле § 2) симметрическому вычитанию $*$; докажите ее свойства, двойственные известным Вам свойствам операции $*$ (в частности, ассоциативность $(A \circ B) \circ C = A \circ (B \circ C)$ этой операции и ее дистрибутивность $(A \circ B) + C = (A + C) \circ (B + C)$ относительно сложения).

4.15. а) Нарисуйте диаграмму Венна для «тройной симметрической разности» $A * B * C$ трех множеств; выразите $A * B * C$ с помощью операций $+$, $\cdot$ и $-$ алгебры множеств и их комбинаций, примененных к A, B и C.

б) Выразите с помощью операций $+$, $\cdot$ и $-$ «n-кратную симметрическую разность» $A_1 * A_2 * A_3 * \ldots * A_n$.

4.16. Бинарной операцией ω алгебры множеств назовем закон, сопоставляющий с каждыми двумя множествами A, B некоторое третье множество $C = A\omega B$, где принадлежность или непринадлежность элемента x множеству C полностью определяется информацией о том, верно или неверно каждое из следующих утверждений: $x \in A$; $x \in B$. Докажите, что в алгебре множеств существует 10 и только 10 бинарных операций, где результат C операции существенно зависит и от A и от B: $+$ (сложение множеств); $\cdot$ (умножение); $\setminus$(разность); «$\setminus$» («перевернутая разность»: $C = A$«$\setminus$»$B = B\setminus A$); $*$ (симметрическая разность или исключающая дизъюнкция; см. с. 127); $|$ (операция Шеффера; см. с. 61); $\downarrow$ (двойственная операция Шеффера; см. с. 62); $\Rightarrow$ (импликация; см. с. 123); $\Longleftrightarrow$ (эквивалентность; с. 125); $\Leftarrow$ («обращенная импликация»: $C = B \Rightarrow A$); кроме того, существуют еще 6 бинарных операций, где результат $C = A\omega B$ операции зависит лишь от одного из множеств A, B или даже ни от одного из них: $C = A$; $= B$; $= \overline{A}$; $= \overline{B}$; $= I$; $= O$. Какие из этих операций двойственны (в смысле § 2) разности (ср. упр. 5); симметрической разности (ср. упр. 14); импликации? Какие из этих 16 операций алгебры множеств коммутативны, ассоциативны; дистрибутивны относительно умножения (т. е. таковы, что $(A\omega B)\,C = (AC)\,\omega\,(BC)$); дистрибутивны относительно сложения (таковы, что $(A\omega B) + C = (A + C)\,\omega\,(B + C)$)?

Глава 2

БУЛЕВА СТРУКТУРА

5. ОПРЕДЕЛЕНИЕ БУЛЕВОЙ СТРУКТУРЫ

Выше мы видели, что алгебра множеств во многом отлична от известных нам ранее алгебраических систем. Важность этой новой системы заставляет дать ей специальное название и рассматривать общие свойства алгебраических образований со сходными свойствами. По имени математика, впервые рассмотревшего алгебраические системы, подобные алгебре множеств, все эти системы обычно называют **алгебрами Буля**; мы в этой книге чаще будем употреблять в том же смысле термин **булева структура**, имея в виду, что речь здесь идет об определенной математической структуре (ср., например, [5] или [11]), задаваемой свойственным ей набором аксиом.

Итак, *булевой структурой* (или *алгеброй Буля*) называется структура

$$\mathbf{B} = \langle \mathcal{B};\ +,\ \cdot,\ \bar{\ },\ \supset \rangle, \tag{5.1}$$

где

$$\mathcal{B} = \{\alpha,\ \beta,\ \gamma,\ \ldots;\ o,\ \iota\}; \tag{5.1'}$$

другими словами, множество элементов $\mathcal{B}$, в котором выделены два «особых» элемента o и ι и определены две бинарные операции: $+$ («сложение») и $\cdot$ («умножение»), одна унарная операция $\bar{\ }$ («черта») и бинарное отношение $\supset$ между элементами, связывающее некоторые (не обязательно любые) пары элементов, причем выполняются следующие правила (аксиомы):

А. *Свойства сложения* Б. *Свойства умножения*

а) $\alpha + \beta = \beta + \alpha$, б) $\alpha\beta = \beta\alpha$ (I)

(коммутативные законы для сложения и умножения);

а) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, б) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (II)

(ассоциативные законы);

а) $\alpha + \alpha = \alpha$, б) $\alpha\alpha = \alpha$ (VI)

(идемпотентные законы).

В. *Правила, связывающие сложение и умножение*

а) $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$, б) $\alpha\beta + \gamma = (\alpha + \gamma)(\beta + \gamma)$ (III)

(дистрибутивные законы);

а) $\alpha + \alpha\beta = \alpha$, б) $\alpha(\alpha + \beta) = \alpha$ (VII)

(законы поглощения).

Г. *Свойства элементов* о *и* ι

а) $\alpha + o = \alpha$, б) $\alpha\iota = \alpha$; (IV)

а) $\alpha + \iota = \iota$, б) $\alpha o = o$. (V)

Д. *Свойства операции* — (*«черта»*)

$\bar{\bar{\alpha}} = \alpha$ (IX)

(инволютивность операции —);

а) $\bar{\iota} = o$, б) $\bar{o} = \iota$. (X)

Е. *Правила, связывающие операции* —, + и $\cdot$

а) $\alpha + \bar{\alpha} = \iota$, б) $\alpha\bar{\alpha} = o$; (VIII)

а) $\overline{\alpha + \beta} = \bar{\alpha}\bar{\beta}$, б) $\overline{\alpha\beta} = \bar{\alpha} + \bar{\beta}$ (XI)

(правила де Моргана).

Ж. *Свойства отношения* $\supset$

$\alpha \supset \alpha$ (XII)

(рефлексивность);

если $\alpha \supset \beta$ и $\beta \supset \gamma$, то $\alpha \supset \gamma$ (XIII)

(транзитивность);

если $\alpha \supset \beta$ и $\beta \supset \alpha$, то $\alpha = \beta$ (XIV)

(антисимметричность);

а) $\iota \supset \alpha$, б) $\alpha \supset o$. (XV)

3. *Связь отношения $\supset$ со сложением и умножением*

а) $\alpha + \beta \supset \alpha$, б) $\alpha \supset \alpha\beta$; (XVI)

если $\alpha \supset \beta$, то а) $\alpha + \beta = \alpha$, б) $\alpha\beta = \beta$; (XVII)

а) если $\alpha \supset \beta$ и $\alpha \supset \gamma$, то $\alpha \supset \beta + \gamma$,
б) если $\beta \supset \alpha$ и $\gamma \supset \alpha$, то $\beta\gamma \supset \alpha$; (XIX)

если $\alpha \supset \beta$, то а) $\alpha + \gamma \supset \beta + \gamma$, б) $\alpha\gamma \supset \beta\gamma$; (XX)

а) $\alpha + \beta = \max[\alpha, \beta]$, б) $\alpha\beta = \min[\alpha, \beta]$. (XVIII)

И. *Правило, связывающее отношение $\supset$ с операцией —*,

если $\alpha \supset \beta$, то $\bar{\beta} \supset \bar{\alpha}$. (XXI)

[Во всех аксиомах α, β, γ — произвольные элементы множества $\mathscr{B}$.]

Иногда в число определяющих булеву структуру аксиом вводят еще неравенство $o \neq \iota$. Ясно, что если $o = \iota$, то в силу (IVб) и (Vб) для каждого элемента α множества $\mathscr{B}$ имеем $\alpha = o$, т. е. наша структура сводится к единственному элементу ω (являющемуся для нее одновременно и нулевым, и единичным элементом), причем, конечно, $\omega + \omega = \omega\omega = \bar{\omega} = \omega$ (а как еще можно определить тут элементы $\omega + \omega$, $\omega\omega$ и $\bar{\omega}$?). Разумеется, при этом у нас будут выполняться все аксиомы (I)—(XXI), поскольку и левая, и правая части любого равенства или неравенства неизбежно сведутся к единственному элементу ω нашей структуры, а в силу свойств отношений $=$ и $\supset$ мы имеем $\omega = \omega$ и $\omega \supset \omega$ (см. (XII)). Ясно, что эта «тривиальная» структура Буля (ее можно отождествить с множеством подмножеств пустого множества)[1] не представляет ни малейшего интереса, и поэтому ее стремятся исключить из числа рассматриваемых систем. Мы, однако, предпочтем просто запомнить, что равенство $o = \iota$ совместимо с аксиомами булевой структуры, но лишает эту структуру какого бы то ни было содержательного смысла, т. е. что внимания заслуживают исключительно структуры (1), для которых $o \neq \iota$ (и множество $\mathscr{B}$ содержит более одного элемента)

Ясно, что характеризующие булеву структуру (1) основные операции $+$, $\cdot$ и $^-$ и основное отношение $\supset$ никакого содержательного (конструктивного) определения (или описания) не имеют: косвенным (дескриптивным) их определением являются свойства (I)—(XXI), выполняющиеся для рассматриваемых операций и отношения. Такое определение структуры (1) является, конечно, довольно громоздким: 4 типа основных отношений между элементами множества $\mathscr{B}$; 37 аксиом (ср., скажем, с определением *группы*, задаваемым тремя

[1] Впрочем, иногда (и это хорошо иллюстрирует несколько схоластический характер современной математики!) в алгебре подмножеств пустого множества различают универсальное множество $\{\phi\}$ (множество, состоящее из единственного элемента ϕ) и пустое подмножество ϕ нашего множества, не содержащее уже ни одного элемента. В этом случае алгебра подмножеств пустого множества будет состоять из двух элементов $\{\phi\} = I$ и $\phi = O$, т. е. она сведется к многократно встречающейся в этой книге простейшей «истинной» структуре Буля из двух элементов ι и o.

аксиомами, касающимися о д н о й бинарной операции; см. [II, с. 75] или [3]). Впрочем, впоследствии мы увидим, что громоздкость определения булевой структуры частично является фиктивной — она связана с тем, что мы, не мудря, включили в число аксиом в с е известные нам свойства алгебры множеств, просто не задумываясь над тем, какие из них являются следствиями других.

Из определения группы как структуры

$$\mathbf{G} = < \mathcal{G}; \ \cdot >, \tag{5.1''}$$

задаваемой тремя свойствами группового умножения[1] — ассоциативностью, существованием единичного элемента e и существованием обратного g^{-1} для каждого $g \in \mathcal{G}$ — вытекают, как известно, ряд других присущих всем группам свойств, например, единственность единичного элемента e или возможность деления одного элемента a на другой элемент b (т. е. существование такого элемента x, что $xb = a$; этот элемент равен ab^{-1}). Аналогично этому из определения структуры Буля вытекают многие другие ее свойства. Мы здесь остановимся только на двух примерах подобного рода, первый из которых при всей своей простоте достаточно принципиален, а второй понадобится нам впоследствии.

Покажем прежде всего, что определенные равенствами (IV) элементы o и ι е д и н с т в е н н ы, т. е. что если наряду с o существует еще один элемент o_1, такой, что

$$\alpha + \mathrm{o}_1 = \alpha \ \text{для всех} \ \alpha \in \mathcal{B}, \tag{*}$$

то $\mathrm{o}_1 = \mathrm{o}$; аналогично, если

$$\alpha\iota_1 = \alpha \ \text{для всех} \ \alpha \in \mathcal{B}, \tag{**}$$

то обязательно $\iota_1 = \iota$. ◀ В самом деле, так как по (IVа) и (*)

$$\mathrm{o}_1 + \mathrm{o} = \mathrm{o}_1 \ \text{ и } \ \mathrm{o} + \mathrm{o}_1 = \mathrm{o},$$

то в силу (Iа) $\mathrm{o}_1 = \mathrm{o}$. Точно так же, поскольку из (IVб) и (**) имеем

$$\iota_1\iota = \iota_1 \ \text{ и } \ \iota\iota_1 = \iota,$$

то по (IIб) $\iota_1 = \iota$. ▶

Докажем теперь, что если $\alpha \supset \beta$, то существует *прямая разность* $\alpha - \beta$, т. е. такой элемент ξ, что

$$\alpha = \beta + \xi \ \text{ и } \ \beta\xi = \mathrm{o}.$$

◀ Мы утверждаем, что[2]

$$\xi = \alpha - \beta = \alpha\overline{\beta}.$$

---

[1] Возможны, впрочем, и другие аксиоматики, описывающие ту же структуру «группа» (см., например, [II, с. 76])

[2] Отсюда следует совпадение введенной здесь операции с определенным на с. 29 вычитанием двух элементов α и β (где «уменьшаемое» α и «вычитаемое» β связаны отношением $\alpha \supset \beta$), что и позволяет использовать в этих двух случаях один и тот же символ «—».

В самом деле,

$$\beta + \xi = \beta + \alpha\overline{\beta} = \alpha\beta + \alpha\overline{\beta} = \alpha(\beta + \overline{\beta}) = \alpha\iota = \alpha$$

(см. аксиомы (XVII б), (IIIа) и (I б), (VIII а), (IV б)) и

$$\beta\xi = \beta(\alpha\overline{\beta}) = \alpha(\beta\overline{\beta}) = \alpha o = o$$

(см. (Iб) и (II б), (VIII б), (V б)). ▶

Для каждого определения математического объекта, состоящего в указании системы аксиом, которые должны иметь место, сразу встает вопрос о непротиворечивости, полноте и независимости выбранной системы аксиом. Система аксиом называется *непротиворечивой*, если из этих аксиом нельзя сделать два взаимно исключающих друг друга вывода, другими словами, если в результате развития дедуктивной системы, базирующейся на этой системе аксиом, мы никогда не придем к противоречию. Ясно, что внимания заслуживают только непротиворечивые системы аксиом. Непротиворечивость системы аксиом устанавливается построением модели, или интерпретации соответствующей аксиоматики, т. е. системы каких-то известных ранее объектов, между которыми можно установить отношения, подчиняющиеся всем требованиям, содержащимся в наших аксиомах. В случае булевой структуры такая модель доставляется системой множеств, где под суммой множеств понимается их объединение, под произведением множеств — их пересечение, под элементами o и ι — пустое множество и универсальное множество, под унарной операцией «черта» — образование множества, составленного из всех элементов универсального множества, не принадлежащих данному множеству, и соотношение $\supset$ означает принадлежность одного множества другому (см. § 1—4). Эта модель доказывает, что выписанная выше система аксиом, определяющих булеву структуру, *непротиворечива*.

Система аксиом называется *полной*, если она допускает лишь одну-единственную реализацию, точнее, если любые две модели или интерпретации этой системы аксиом по существу совпадают, изоморфны (ср., впрочем, обсуждение этого вопроса в [2.8]). Две модели аксиоматической системы называются *изоморфными*, если между образующими эти модели элементами можно установить взаимно-однозначное (биективное) соответствие, причем так, что каждому отношению между элементами первой модели отвечает такое же отношение между отвечающими им элементами второй модели. Другими словами, две изоморфные модели представляют собой один и тот же математический объект, только описанный на разных языках: так, изоморфны, скажем, множество векторов трехмерного пространства и множество троек чисел — координат этих векторов. Ясно, что аксиоматика алгебры Буля является *неполной*: ведь уже рассмотренные выше две модели этой аксиоматики — совокупность всевозможных множеств шахматных фигур и совокупность всевозможных множеств целых чисел —

не изоморфны (ибо совокупность множеств шахматных фигур конечна, а совокупность множеств целых чисел бесконечна, и поэтому между этими двумя совокупностями множеств нельзя установить взаимно-однозначного соответствия).

Наконец, система аксиом называется *независимой*, если ни одну из аксиом этой системы нельзя вывести из других аксиом, т. е. доказать как теорему, базируясь на всех остальных аксиомах системы (ср. [2.8]). Конечно, выписанная выше система аксиом алгебры Буля является *зависимой*. Так, мы уже отмечали, что идемпотентные законы (VI) являются непосредственными следствиями условий (XVII) и правила (XII), а законы поглощения (VII) — следствиями тех же правил (XVII) и соотношений (XVI); поэтому нет никакой необходимости включать равенства (VI) и (VII) в систему аксиом. Аналогично отмечалось, что (XVIIIа) есть не что иное, как объединение соотношений (XVIа) и (XIXа), а (XVIIIб) — объединение (XVIб) и (XIXб). Таким образом, в список аксиом достаточно включить законы (XVIII), после чего как (XVI), так и (XIX) станут не нужны.

Мы указывали также, что правила де Моргана (XI) и соотношения (X), (IX) и (XXI) позволяют доказать принцип двойственности, используя который можно вывести правила (Iб)—(VIIIб) и (XV б) — (XX б) из правил (Iа)—(VIIIа) и (XVа)—(XXа); поэтому первые 14 правил следует считать не аксиомами, а теоремами, поскольку их справедливость следует из остальных правил. Нетрудно обнаружить и ряд других зависимостей между аксиомами (I)—(XXI).

Остановимся подробнее на вопросе о зависимостях между отдельными аксиомами, фигурирующими в определении булевой структуры. Заметим прежде всего, что отношение $\alpha \supset \beta$ можно не вводить в число первоначальных, неопределяемых отношений, так как его можно о п р е д е л и т ь условиями (XVII): $\alpha + \beta = \alpha$ или $\alpha\beta = \beta$

◀ Эти последние два условия *равносильны*, что следует из того, что каждое из них эквивалентно условию $\bar{\alpha}\beta = o$. В самом деле, если $\alpha + \beta = \alpha$, то $\bar{\alpha}(\alpha + \beta) = \bar{\alpha}\alpha = o$; но

$$\bar{\alpha}(\alpha+\beta) \underset{(\text{IIIa})}{=} \bar{\alpha}\alpha+\bar{\alpha}\beta \underset{(\text{VIIIб})}{=} o+\bar{\alpha}\beta \underset{(\text{IVa})}{=} \bar{\alpha}\beta.$$

Напротив, если $\bar{\alpha}\beta = o$, то $\bar{\alpha}\beta + \alpha = \alpha$; но

$$\bar{\alpha}\beta+\alpha \underset{(\text{IIIб})}{=} (\bar{\alpha}+\alpha)(\beta+\alpha) \underset{(\text{VIIIa})}{=} \iota(\alpha+\beta) \underset{(\text{IVб})}{=} \alpha+\beta.$$

Аналогично этому, если $\alpha\beta = \beta$, то $\bar{\alpha}\beta = \bar{\alpha}(\alpha\beta)$; но

$$\bar{\alpha}(\alpha\beta) \underset{(\text{IIб})}{=} (\bar{\alpha}\alpha)\beta \underset{(\text{VIIIб})}{=} o\beta \underset{(\text{Vб})}{=} o.$$

Обратно: если $\bar{\alpha}\beta = o$, то $\alpha\beta + \bar{\alpha}\beta = \alpha\beta$; но

$$\alpha\beta+\bar{\alpha}\beta \underset{(\text{IIIa})}{=} (\alpha+\bar{\alpha})\beta \underset{(\text{VIIIa})}{=} \iota\beta \underset{(\text{IVб})}{=} \beta.$$

[Заметим, что в процессе доказательства мы использовали коммутативность сложения и умножения.] ▶

Далее, из предложенного определения отношения $\supset$ вытекают все его свойства (XII)—(XVI), (XVIII)—(XXI).

◀ В самом деле,

так как $\alpha + \alpha = \alpha$, то $\alpha \supset \alpha$, что доказывает (XII);

если $\alpha + \beta = \alpha$ и $\beta + \gamma = \beta$, то $\alpha + \gamma = (\alpha + \beta) + \gamma \underset{(\mathrm{IIa})}{=} \alpha + (\beta + \gamma) =$

$= \alpha + \beta = \alpha$, что доказывает (XIII);

если $\alpha + \beta = \alpha$ и $\beta + \alpha = \beta$, то в силу (Ia) $\alpha = \beta$ что доказывает (XIV)

так как в силу (Va) $\iota + \alpha = \iota$, то $\iota \supset \alpha$, что доказывает (XVa);

так как в силу (IVa) $\alpha + o = \alpha$, то $\alpha \supset o$, что доказывает (XVб);

$(\alpha + \beta) + \alpha \underset{(\mathrm{Ia},\ \mathrm{IIa})}{=} (\alpha + \alpha) + \beta \underset{(\mathrm{VIa})}{=} \alpha + \beta$, что доказывает (XVIa);

$\alpha(\alpha\beta) \underset{(\mathrm{II}б)^1}{=} (\alpha\alpha)\beta \underset{(\mathrm{VI}б)}{=} \alpha\beta$, что доказывает (XVIб);

если $\alpha + \beta = \alpha$, то $(\alpha + \gamma) + (\beta + \gamma) \underset{(\mathrm{Ia},\ \mathrm{IIa})}{=} (\alpha + \beta) + (\gamma + \gamma) \underset{(\mathrm{VIa})}{=} \alpha + \gamma$, что доказывает (XXa);

если $\alpha\beta = \beta$, то $(\alpha\gamma)(\beta\gamma) \underset{(\mathrm{I}б,\ \mathrm{II}б)}{=} (\alpha\beta)(\gamma\gamma) \underset{(\mathrm{VI}б)}{=} \beta\gamma$. что доказывает (XXб);

если $\mu + \alpha = \mu$ и $\mu + \beta = \mu$, то $\mu + (\alpha + \beta) \underset{(\mathrm{VIa})}{=} (\mu + \mu) + (\alpha + \beta) \underset{(\mathrm{Ia},\ \mathrm{IIa})}{=} (\mu +$

$+ \alpha) + (\mu + \beta) = \mu + \mu \underset{(\mathrm{VIa})}{=} \mu$, что совместно с (XVIa) и (Ia) доказывает (XVIIIa)

(а значит, и (XIXa));

если $\mu\alpha = \mu$ и $\mu\beta = \mu$, то $\mu(\alpha\beta) \underset{(\mathrm{VI}б)}{=} (\mu\mu)(\alpha\beta) \underset{(\mathrm{I}б,\ \mathrm{II}б)}{=} (\mu\alpha)(\mu\beta) = \mu\mu \underset{(\mathrm{VI}б)}{=} \mu$,

что совместно с (XVIб) и (Iб) доказывает (XVIIIб) и (XIXб)

если $\alpha + \beta = \alpha$, то, в силу (XIa), $\bar\alpha\,\bar\beta = \bar\alpha$, что доказывает (XXI). ▶

Таким образом, можно исключить из числа основных (неопределяемых) отношений структуры **B** отношение $\supset$, а из числа характеризующих эту структуру аксиом — аксиомы (XII) — (XXI). [Аксиомы (XVII) становятся теперь о п р е д е л е н и я м и, а остальные аксиомы — т е о р е м а м и.]

Далее потребуем, чтобы *для каждого элемента* $\alpha \in \mathscr{B}$ *существовал такой элемент* $\bar\alpha \in \mathscr{B}$, *что имеют место условия* (VIII). Такой элемент может быть только о д и н. ◀ Действительно, если

$\alpha + \bar\alpha = \iota$, $\alpha\bar\alpha = o$ и $\alpha + \bar\alpha_1 = \iota$, $\alpha\bar\alpha_1 = o$,

то

$$\bar\alpha_1 \underset{(\mathrm{IV}б)}{=} \bar\alpha_1\iota = \bar\alpha_1(\alpha + \bar\alpha) \underset{(\mathrm{IIIa})}{=} \bar\alpha_1\alpha + \bar\alpha_1\bar\alpha = o + \bar\alpha_1\alpha \underset{(\mathrm{IVa})}{=} \bar\alpha_1\bar\alpha$$

(здесь также попутно используется коммутативность сложения и умножения) и

$$\bar\alpha \underset{(\mathrm{IV}б)}{=} \bar\alpha\iota = \bar\alpha(\alpha + \bar\alpha_1) \underset{(\mathrm{IIIa})}{=} \bar\alpha\alpha + \bar\alpha\bar\alpha_1 = o + \bar\alpha\bar\alpha_1 \underset{(\mathrm{IVa})}{=} \bar\alpha\bar\alpha_1,$$

откуда в силу коммутативности умножения следует, что $\bar\alpha_1 = \bar\alpha$. ▶ Поэтому далее можно принять условия (VIII) за о п р е д е л е н и е операции $^-$.

Очень важно, что из (VIII) следуют все остальные свойства (IX) — (XI) операции $^-$. ◀ В самом деле,

условия (VIII) симметричны относительно α и $\bar\alpha$, откуда следует (IX);

в силу (V) $o + \iota = \iota$ и $o\iota = o$, откуда следует (X);

$$(\alpha+\beta)+\bar\alpha\,\bar\beta \underset{(III6)}{=} ((\alpha+\beta)+\bar\alpha)((\alpha+\beta)+\bar\beta) \underset{(IIa)}{=} ((\alpha+\bar\alpha)+\beta)(\alpha+(\beta+\bar\beta)) \underset{(VIIIa)}{=}$$

$$=(\iota+\beta)(\alpha+\iota) \underset{(Va)}{=} \iota\iota \underset{(VI6)}{=} \iota$$

и

$$(\alpha+\beta)(\bar\alpha\,\bar\beta) \underset{(IIIa)}{=} \alpha(\bar\alpha\,\bar\beta)+\beta(\bar\alpha\,\bar\beta) \underset{(II6)}{=} (\alpha\bar\alpha)\bar\beta+\bar\alpha(\bar\beta\beta) \underset{(VIII6)}{=} o\beta+\bar\alpha o \underset{(V6)}{=} o+o \underset{(VIa)}{=} o$$

(здесь также используются коммутативные законы), откуда и вытекает (XIa). [(XIб) вытекает из (XIa) и (IX): достаточно изменить обозначения в равенстве (XIa), заменив α на $\bar\alpha$ и β на $\bar\beta$.] ▶

Таким образом, мы можем исключить из числа основных операций структуры **B** унарную операцию $^-$, сохранив в числе аксиом требование разрешимости для каждого заданного $\alpha \in \mathcal{B}$ уравнений (VIII), в которых $\bar\alpha$ считается неизвестным, после чего из системы аксиом исключаются аксиомы (VIII)—(XI) (первые две из них становятся о п р е д е л е н и я м и, последующие — т е о р е м а м и[1]).

Далее, имея уже соотношения (VIII), мы сразу получаем (V)

$$◀\ \alpha+\iota \underset{(VIIIa)}{=} \alpha+(\alpha+\bar\alpha) \underset{(IIa)}{=} (\alpha+\alpha)+\bar\alpha \underset{(VIa)}{=} \alpha+\bar\alpha \underset{(VIIIa)}{=} \iota;$$

$$\alpha o \underset{(VIII6)}{=} \alpha(\alpha\bar\alpha) \underset{(II6)}{=} (\alpha\alpha)\bar\alpha \underset{(VI6)}{=} \alpha\bar\alpha \underset{(VIII6)}{=} o.\ ▶$$

Не сложнее доказываются идемпотентные законы (VI) и законы поглощения (VII):

$$◀\ \alpha+\alpha \underset{(IV6)}{=} (\alpha+\alpha)\iota \underset{(VIIIa)}{=} (\alpha+\alpha)(\alpha+\bar\alpha) \underset{(III6)}{=} \alpha+\alpha\bar\alpha \underset{(VIII6)}{=} \alpha+o \underset{(IVa)}{=} \alpha$$

и

$$\alpha\alpha \underset{(IVa)}{=} \alpha\alpha+o \underset{(VIII6)}{=} \alpha\alpha+\alpha\bar\alpha \underset{(IIIa)}{=} \alpha(\alpha+\bar\alpha) \underset{(VIIIa)}{=} \alpha\iota \underset{(IV6)}{=} \alpha;$$

$$\alpha+\alpha\beta \underset{(IV6)}{=} \alpha\iota+\alpha\beta \underset{(IIIa)}{=} \alpha(\iota+\beta) \underset{(Va)}{=} \alpha\iota \underset{(IV6)}{=} \alpha,$$

---

[1] Заметим, что место «равенств—определений» (XVII) и (VIII) в конструируемой нами «экономной» аксиоматике булевой структуры будет совершенно разным: (XVII) суть «чистые» определения (одного и того же отношения $\supset$, в силу чего приходится доказывать их эквивалентность), в то время как (VIII) суть «аксиомы—определения» в том смысле, что нам приходится специально требовать существования элемента $\bar\alpha \in \mathcal{B}$, удовлетворяющего равенствам (VIII) (в которых элемент $\alpha \in \mathcal{B}$ считается заданным). При этом место унарной операции $^-$ в структуре (I) оказывается родственным месту унарной операции $^{-1}$ в структуре (I″) (в группе): аксиомы структуры требуют с у щ е с т в о в а н и я для каждого $g \in \mathcal{G}$ (соответственно для каждого $\alpha \in \mathcal{B}$) элемента $g^{-1} \in \mathcal{G}$ (элемента $\bar\alpha \in \mathcal{B}$), после чего с привлечением других аксиом доказывается е д и н с т в е н н о с т ь этого элемента, что и позволяет рассматривать $^{-1}$ и $^-$ как (унарные) алгебраические операции, действующие соответственно на $\mathcal{G}$ и на $\mathcal{B}$.

и

$$\alpha(\alpha+\beta) \underset{(\mathrm{IIIa})}{=} \alpha\alpha+\alpha\beta \underset{(\mathrm{VIa})}{=} \alpha+\alpha\beta \underset{(\mathrm{VIIa})}{=} \alpha$$

(заметьте, что мы каждый раз ссылаемся лишь на соотношения справедливость которых нами принимается или уже доказана!). ▶

Наконец, также и ассоциативные законы (II), можно вывести из других аксиом, хотя это и требует чуть бо́льших усилий. ◀ Обозначим

$$(\alpha+\beta)+\gamma=\xi, \quad \alpha+(\beta+\gamma)=\eta$$

и докажем, что $\xi=\eta$. Для этого составим произведения $\alpha\xi$ и $\alpha\eta$:

$$\alpha\xi=\alpha((\alpha+\beta)+\gamma) \underset{(\mathrm{IIIa})}{=} \alpha(\alpha+\beta)+\alpha\gamma \underset{(\mathrm{VIIб})}{=} \alpha+\alpha\gamma \underset{(\mathrm{VIIa})}{=} \alpha$$

и

$$\alpha\eta=\alpha(\alpha+(\beta+\gamma)) \underset{(\mathrm{VIa})}{=} (\alpha+\alpha)(\alpha+(\beta+\gamma)) \underset{(\mathrm{IIIб})}{=} \alpha+\alpha(\beta+\gamma) \underset{(\mathrm{VIIa})}{=} \alpha$$

(ясно, что в (VIIa) можно заменить β на $\beta+\gamma$).

Далее найдем $\bar{\alpha}\xi$ и $\bar{\alpha}\eta$:

$$\bar{\alpha}\xi=\bar{\alpha}((\alpha+\beta)+\gamma) \underset{(\mathrm{IIIa})}{=} \bar{\alpha}(\alpha+\beta)+\bar{\alpha}\gamma \underset{(\mathrm{IIIa})}{=} (\alpha\bar{\alpha}+\bar{\alpha}\beta)+\bar{\alpha}\gamma \underset{(\mathrm{VIIIб})}{=}$$

$$=(o+\bar{\alpha}\beta)+\bar{\alpha}\gamma \underset{(\mathrm{IVa})}{=} \bar{\alpha}\beta+\bar{\alpha}\gamma \underset{(\mathrm{IIIa})}{=} \bar{\alpha}(\beta+\gamma)$$

и

$$\bar{\alpha}\eta=\bar{\alpha}(\alpha+(\beta+\gamma)) \underset{(\mathrm{IIIa})}{=} \bar{\alpha}\alpha+\bar{\alpha}(\beta+\gamma) \underset{(\mathrm{VIIIб})}{=} o+\bar{\alpha}(\beta+\gamma) \underset{(\mathrm{IVa})}{=} \bar{\alpha}(\beta+\gamma).$$

Таким образом, мы имеем

$$\alpha\xi=\alpha\eta \quad \text{и} \quad \bar{\alpha}\xi=\bar{\alpha}\eta,$$

откуда следует

$$\xi \underset{(\mathrm{IVб})}{=} \iota\xi \underset{(\mathrm{VIIIa})}{=} (\alpha+\bar{\alpha})\xi \underset{(\mathrm{IIIa})}{=} \alpha\xi+\bar{\alpha}\xi=\alpha\eta+\bar{\alpha}\eta \underset{(\mathrm{IIIa})}{=}$$

$$=(\alpha+\bar{\alpha})\eta \underset{(\mathrm{VIIIa})}{=} \iota\eta \underset{(\mathrm{IVб})}{=} \eta,$$

что и требовалось доказать. После этого справедливость (IIб) может быть выведена из (IIa) стандартным приемом (принцип двойственности!): если

$$\xi_1=(\alpha\beta)\gamma \quad \text{и} \quad \eta_1=\alpha(\beta\gamma),$$

то (см. уже доказанное соотношение (XIб))

$$\bar{\xi}_1=\overline{(\alpha\beta)\gamma}=\overline{\alpha\beta}+\bar{\gamma}=(\bar{\alpha}+\bar{\beta})+\bar{\gamma}$$

и

$$\bar{\eta}_1=\overline{\alpha(\beta\gamma)}=\bar{\alpha}+\overline{\beta\gamma}=\bar{\alpha}+(\bar{\beta}+\bar{\gamma}),$$

откуда в силу (IIa) $\bar{\xi}_1=\bar{\eta}_1$. А теперь имеем

$$\xi_1=\overline{(\bar{\xi}_1)}=\overline{(\bar{\eta}_1)}=\eta_1,$$

что и завершает доказательство ассоциативных законов. ▶

Итак, правила (II), (V), (VI) и (VII) тоже можно исключить из числа аксиом булевой структуры.

Окончательно мы приходим к следующему определению: *Булевой структурой* называется структура[1]

$$\mathbf{B} = <\mathscr{B};\ +,\ \cdot\ >, \qquad (5.1''')$$

где действующие в множестве $\mathscr{B} = \{\alpha, \beta, \gamma, \ldots; o, \iota\}$ бинарные операции $+$ и $\cdot$ коммутативны:

$Б_1: \alpha + \beta = \beta + \alpha, \quad Б_2: \alpha\beta = \beta\alpha$

и дистрибутивны одна относительно другой:

$Б_3: \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, \quad Б_4: \alpha + \beta\gamma = (\alpha + \beta)(\alpha + \gamma);$

далее существуют два таких элемента $o, \iota \in \mathscr{B}$, что для каждого $\alpha \in \mathscr{B}$

$Б_5: o + \alpha = \alpha, \quad Б_6: \iota\alpha = \alpha;$

наконец, для каждого $\alpha \in \mathscr{B}$ существует такой элемент $\bar{\alpha} \in \mathscr{B}$, что

$Б_7: \alpha + \bar{\alpha} = \iota, \quad Б_8: \alpha\bar{\alpha} = o$

(в аксиомах $Б_{1-4}$, разумеется, как всегда α, β, γ — произвольные элементы множества $\mathscr{B}$; также и в $Б_{5-8}$ специально отмечается, что элемент $\alpha \in \mathscr{B}$ — любой). При этом из $Б_{1-8}$ вытекают (при оговоренном выше определении отношения $\supset$ и задаваемой $Б_{7,8}$ операции $^{-}$) все 37 предложений (I) — (XXI), так что новое определение структуры **B** вполне равносильно первому ее определению.

Бросается в глаза «самодвойственный» характер аксиом $Б_{1-8}$ (как, впрочем, и первоначальных аксиом (I)—(XXI)): если заменить в этих аксиомах $+$ на $\cdot$ и наоборот, ι на o и наоборот (и $\supset$ на $\subset$ и наоборот, а операцию $^{-}$ сохранить всюду, где она встречается), то каждая аксиома булевой структуры переходит в новую, также справедливую (выше мы специально выписали рядом двойственные друг другу аксиомы — $Б_1$ и $Б_2$ и т. д.). А так как каждая «булева теорема» (теорема теории булевых структур) выводится из аксиом, то отсюда следует справедливость в теории булевых структур **принципа двойственности**, согласно которому *каждое верное булево предложение* (например, каждое тождественно выполняющееся булево равенство или неравенство) *переходит при замене*

$+ \leftrightarrow \cdot, \quad \iota \leftrightarrow o, \quad ^{-} \leftrightarrow {}^{-}, \quad \supset \leftrightarrow \subset$

снова в истинное предложение (выводимое из аксиом в точности как исходное предложение, однако с заменой каждой аксиомы двойственной ей); этот принцип (ср. выше § 2) играет в теории булевых структур весьма важную роль.

[1] Ясно, что так определенная структура является *алгебраической структурой* в смысле Н. Бурбаки (см. первую из книг [5] или [II, с. 73]).

Система $Б_{1-8}$ аксиом алгебры Буля является уже «почти независимой». Единственное дальнейшее упрощение этой системы, которое еще возможно, — это исключение из списка аксиом одной из аксиом $Б_5$ и $Б_6$, поскольку, например, $Б_5$ может быть выведена из аксиом $Б_{1-4}$, $Б_{6-8}$ (и $Б_6$ выведена из $Б_{1-5}$ и $Б_{7-8}$); система же, состоящая, скажем, из аксиом $Б_{1-5}$, $Б_{7-8}$, будет уже независимой. Впрочем, полная симметричность утверждений $Б_5$ и $Б_6$ ставит нас при желании сохранить лишь одну из этих двух аксиом в положение небезызвестного буриданова осла, умершего от голода между двумя совершенно одинаковыми вязанками сена, из которых он так и не сумел выбрать какую-либо одну. Чтобы избежать столь зловещей участи, математики предпочитают сохранять в списке аксиом булевой структуры оба предложения: и $Б_5$, и $Б_6$, что одновременно упрощает анализ этой аксиоматической системы.

◀ Для того чтобы вывести из $Б_{1-4}$ и $Б_{6-8}$ аксиому $Б_5$, заметим прежде всего, что равенство (Va), т. е. $\alpha + \iota = \iota$, может быть выведено из наших аксиом (где теперь ι определяется равенством $Б_7$) без участия $Б_5$:

$$\alpha+\iota \underset{Б_6}{=} (\alpha+\iota)\,\iota \underset{Б_7}{=} (\alpha+\iota)(\alpha+\bar{\alpha}) \underset{Б_4}{=} \alpha+\iota\bar{\alpha} \underset{Б_6}{=} \alpha+\bar{\alpha} \underset{Б_7}{=} \iota.$$

А теперь имеем

$$o+\alpha \underset{Б_1}{=} \alpha+o \underset{Б_8}{=} \alpha+(\alpha\bar{\alpha}) \underset{Б_6}{=} (\alpha\iota)+(\alpha\bar{\alpha}) \underset{Б_3}{=} \alpha(\iota+\bar{\alpha}) \underset{Б_1,\,(Va)}{=} \alpha\iota \underset{Б_2}{=} \iota\alpha \underset{Б_6}{=} \alpha.$$

Аналогично выводится и равенство $Б_6$ из аксиом $Б_{1-5}$ и $Б_{7-8}$ (см упр. 4а)). ▶

Независимость всех остальных аксиом устанавливается стандартным приемом: построением моделей, в которых выполняются все аксиомы из нашего списка, кроме выбранной нами. ◀ Ясно, что о б е аксиомы $Б_{5-6}$ нельзя исключить из нашего списка аксиом, ибо в системе из двух всего элементов α, ω (где и роль o, и роль ι играет элемент ω) со «сложением» и «умножением»:

+	α	ω
α	ω	ω
ω	ω	ω

,

	α	ω
α	ω	ω
ω	ω	ω

(5.2)

(с операциями $\alpha+\alpha=\alpha+\omega=\omega+\alpha=\omega+\omega=\alpha\alpha=\alpha\omega=\omega\alpha=\omega\omega=\omega$) выполняются все аксиомы $Б_{1-4}$, $Б_{7-8}$ (где $\bar{\alpha}$ и $\bar{\omega}$ можно определять как угодно!),— но не $Б_5$ и не $Б_6$.

Независимость $Б_1$ устанавливает существование структуры $\langle\{o, \iota\};\ +, \cdot, {}^{-}\rangle$ со следующим определением действий:

+	o	ι
o	o	ι
ι	o	ι

,

	o	ι
o	o	o
ι	o	ι

и

—	
o	ι
ι	ι

(5.3)

(т. е. $o+o=\iota+o=o$, $o+\iota=\iota+\iota=\iota$; $oo=o\iota=\iota o=o$, $\iota\iota=\iota$; $\bar{o}=\bar{\iota}=\iota$). Здесь, очевидно, выполняются $Б_2$ и $Б_{5-8}$, в то время как $Б_1$ места не имеет (ибо $o+\iota\neq o=\iota+o$). Далее, непосредственная проверка показывает, что равенства $Б_3$ и $Б_4$ также имеют место для любых α, β, $\gamma = o, \iota$. Так, например, $o(\iota+\iota)=o\iota=o$ и $o\iota+o\iota=o+o=o$ или $\iota+o\iota=\iota+o=o$ и $(\iota+o)(\iota+\iota)=o\iota=o$. Но если бы аксиома $Б_1$ была выводима из других аксиом нашей системы, то в каждой алгебраической структуре, для которой верны аксиомы $Б_{2-8}$, выполнялась бы и аксиома $Б_1$, чего, как мы видим, на самом деле нет. Аналогично с помощью структуры, «двойственной» рассмотренной нами, доказывается независимость аксиомы $Б_2$ (см. упр. 4б)).

Чтобы доказать, что аксиома $Б_4$ не может быть выведена из других аксиом, достаточно рассмотреть множество из двух элементов o и ι, в котором следующим образом определены бинарные операции $+$ и $\cdot$:

$$\begin{array}{c|cc} + & o & \iota \\ \hline o & o & \iota \\ \iota & \iota & o \end{array} \quad \text{и} \quad \begin{array}{c|cc} & o & \iota \\ \hline o & o & o \\ \iota & o & \iota \end{array} \tag{5.4}$$

(т. е. $o + o = \iota + \iota = o$; $o + \iota = \iota + o = \iota$; $oo = o\iota = \iota o = o$; $\iota\iota = \iota$). Очевидно, что для этой системы элементов выполняются аксиомы $Б_1$ и $Б_2$ (сложение и умножение коммутативно). Далее, очевидно, имеют место аксиомы $Б_5$ и $Б_6$, а также $Б_7$ и $Б_8$, где надо считать $\bar{o} = \iota$, $\bar{\iota} = o$.

Непосредственной проверкой убеждаемся, что и аксиома $Б_3$ также справедлива[1]. Однако

$\iota + o\iota = \iota + o = \iota$, а

$(\iota + o)(\iota + \iota) = \iota o = o$,

т. е. аксиома $Б_4$ здесь не выполняется.

Независимость аксиомы $Б_3$ от остальных аксиом устанавливается множеством двух элементов o и ι со следующими правилами сложения и умножения (ср. с (4)):

$$\begin{array}{c|cc} + & o & \iota \\ \hline o & o & \iota \\ \iota & \iota & \iota \end{array} \quad \text{и} \quad \begin{array}{c|cc} & o & \iota \\ \hline o & \iota & o \\ \iota & o & \iota \end{array}, \tag{5.4'}$$

Для этой алгебраической системы (где также надо положить $\bar{o} = \iota$ и $\bar{\iota} = o$) справедливы семь из выписанных выше восьми аксиом, но не аксиома $Б_3$. Наконец, независимость равенства $Б_7$ от равенств $Б_{1-6}$ и $Б_8$ следует из структуры $<\{o, \iota\}; +, \cdot, ^->$, где

$$\begin{array}{c|cc} + & o & \iota \\ \hline o & o & \iota \\ \iota & \iota & \iota \end{array} \quad \begin{array}{c|cc} \cdot & o & \iota \\ \hline o & o & o \\ \iota & o & \iota \end{array}, \quad \begin{array}{c|c} - & o \\ \hline o & o \\ \iota & o \end{array}, \tag{5.5}$$

а независимость $Б_8$ — из «двойственной структуры», отличающейся от (5) лишь тем, что здесь $\bar{o} = \bar{\iota} = \iota$. ▶

Заметим еще, что, определив дополнительно

$$\text{а) } \alpha \setminus \beta = \alpha\bar{\beta} \quad \text{и} \quad \text{б) } \alpha * \beta = \alpha\bar{\beta} + \bar{\alpha}\beta \tag{5.6}$$

(разность и симметрическая разность элементов булевой структуры; в том случае, когда $\alpha \supset \beta$, вместо $\alpha \setminus \beta$ можно писать также $\alpha - \beta$), мы сможем перенести в «абстрактную» структуру Буля все результаты, составляющие содержание § 4 (см. упр. 2). Так, для любых $\alpha, \beta, \gamma \in \mathcal{B}$

$$\text{а) } \alpha \setminus \alpha = o \quad \text{и} \quad \text{б) } \alpha * \alpha = o \tag{5.7}$$

---

[1] Это вытекает из того, что наша алгебраическая система представляет собой не что иное, как *поле вычетов по модулю* 2 (см. [II, с. 85] или любую из книг [3]).

(причем $\alpha * \beta = o$, лишь если $\beta = \alpha$);

а) $\alpha \searrow o = \alpha$ и б) $\alpha * o = \alpha$ (5.8)

(причем $\alpha * \beta = \alpha$, лишь если $\beta = o$);

а) $\iota \searrow \alpha = \overline{\alpha}$ и б) $\iota * \alpha = \overline{\alpha}$ (5.9)

(а также $o \searrow \alpha = o$ и $\alpha * \overline{\alpha} = \iota$);

$\alpha * \beta = \beta * \alpha$; (5.10)

а) $(\alpha \searrow \beta) \searrow \gamma = (\alpha \searrow \gamma) \searrow \beta$ и б) $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$; (5.11)

а) $(\alpha \searrow \beta)\gamma = \alpha\gamma \searrow \beta\gamma$ и б) $(\alpha * \beta)\gamma = (\alpha\gamma) * (\beta\gamma)$. (5.12)

Наряду с этим справедливо тождество

$\alpha * \beta * \alpha\beta = \alpha + \beta$ (5.13)

и предложения

если $\alpha * \gamma = \beta * \gamma$, то $\alpha = \beta$; (5.14)

если $\alpha * \beta = \gamma$, то $\alpha * \gamma = \beta$. (5.15)

В соответствии с общим определением подструктуры (см., например, [II, с. 58]) *подструктурой булевой структуры* (*подалгеброй алгебры Буля*) (1) или (1‴) называется такое подмножество $\mathscr{B}_1$ множества $\mathscr{B}$, которое само является булевой структурой относительно заданных в нем операций $+$, $\cdot$ и $-$, т. е. которое содержит элементы o и ι и замкнуто относительно операций $+$, $\cdot$, $-$ (скажем, если $\alpha, \beta \in \mathscr{B}_1$, то и $\alpha + \beta \in \mathscr{B}_1$). Так, например, элементы o и ι булевой структуры всегда образуют (минимальную) ее подструктуру, поскольку множество $\{o, \iota\}$, очевидно, относительно всех булевых операций замкнуто:

$$\begin{array}{c|cc} + & o & \iota \\ \hline o & o & \iota \\ \iota & \iota & \iota \end{array} \qquad \begin{array}{c|cc} & o & \iota \\ \hline o & o & o \\ \iota & o & \iota \end{array} \quad \text{и} \quad \begin{array}{c|c} - & \\ \hline o & \iota \\ \iota & o \end{array} . \qquad (5.16)$$

Подструктурой структуры всех заключенных внутри квадрата I фигур (см. выше рис. 4—5, 7—10, 12—16 и 18—26) является, например, алгебра заключенных внутри I *многоугольных* фигур (многоугольников, состоящих, возможно, из нескольких отдельных связных кусков, ограниченных прямолинейными отрезками), поскольку, очевидно, объединение и пересечение двух многоугольников снова является многоугольником и дополнение $\overline{M}$ многоугольника M также можно считать многоугольником, так как граница $\overline{M}$ состоит из прямолинейных отрезков.

Аналогично подструктурой алгебры всех подмножеств бесконечного универсального множества I является система всех *конечных* *или коконечных* (таких, дополнение которых конечно) подмножеств I: ведь ясно, что если A конечно, то $\bar{A}$ коконечно и наоборот; пересечение двух множеств, хотя бы одно из которых конечно, будет конечно, и объединение двух множеств, хотя бы одно из которых коконечно, будет коконечно; объединение двух конечных множеств, разумеется, конечно. Отсюда в силу формулы де Моргана (XIa) $\overline{AB} = \bar{A} + \bar{B}$ следует, что пересечение AB двух коконечных множеств (таких, что $\bar{A}$ и $\bar{B}$ конечны) коконечно. Наконец, пустое множество O можно считать конечным, а его дополнение I — коконечным. А вот, хотя система всех подмножеств множества четных натуральных чисел и образует, разумеется, при обычном определении суммы, пересечения и дополнения булеву структуру, эта структура никак не будет являться подструктурой системы всех множеств любых натуральных чисел, поскольку в этих двух булевых структурах единичные элементы I различны и операция взятия дополнения имеет разный смысл.

В дальнейшем (см. § 9) у нас будет возможность коснуться также и вопроса о *фактор-структурах* (см., например, [II, с. 59]) булевых структур.

Упражнения. 5.1. Определите операцию, двойственную (в смысле присущего булевой структуре принципа двойственности) определенному на с. 39 прямому вычитанию элементов структуры.

5.2. Выведите из аксиом булевой структуры все фигурировавшие в § 4 свойства операций $\setminus$ и $*$, в частности, те, которым были посвящены упр. 4.2 и 4.10.

5.3. Сколько существенно различных (не изоморфных) подструктур имеет структура подмножеств 3-, 4- и n-элементного множества?

5.4. Докажите зависимость (независимость)

а) аксиомы $Б_6$; б) аксиомы $Б_2$

от остальных аксиом $Б_{1-8}$ булевой структуры.

6. БУЛЕВЫ МНОГОЧЛЕНЫ; АДДИТИВНАЯ И МУЛЬТИПЛИКАТИВНАЯ ФОРМА БУЛЕВА МНОГОЧЛЕНА

Выше нам часто приходилось иметь дело с теми или иными выражениями, составленными из элементов основного множества $\mathcal{B}$ булевой структуры при помощи бинарных операций «сложение» и «умножение» и унарной операции «черта»: так, например, большинство аксиом (I)—(XXI) утверждает равенство двух подобных выражений.

При этом, в противоположность обычной алгебре чисел (скажем, вещественных), в булевой алгебре мы не имеем операции деления (и, тем более, операции извлечения корня), в силу чего все выражения, образованные из некоторого набора элементов $\mathcal{B}$, по строению напоминают «целые рациональные выражения» (многочлены) школьной алгебры. Мы их будем называть *булевыми многочленами*. [Еще одно отличие булевой алгебры от обычной заключается в том, что в силу идемпотентных законов (VI) здесь $\alpha \cdot \alpha = \alpha$ (а не α^2) и, следовательно, также $\underbrace{\alpha\cdot\alpha\cdot\ \dots\ \cdot\alpha}_{n\ \text{раз}} = \alpha$ (а не α^n; запись α^2, α^3 или α^n здесь просто не имеет никакого отличного от α смысла). Аналогично $\alpha + \alpha = \alpha$ (а не 2α), а также $\underbrace{\alpha + \alpha + \dots + \alpha}_{n\ \text{раз}} = \alpha$ (а не $n\alpha$) Имея в виду это свойство булевой структуры, говорят, что булева алгебра — это *алгебра без степеней и коэффициентов.* Булевыми многочленами являются, например, следующие выражения:

$$\alpha\beta,\ (\alpha+\bar{\beta}+\gamma)\,\bar{\alpha}\,\beta\,\bar{\gamma},\ (\alpha+\beta)(\beta+\gamma)(\gamma+\alpha),$$

$$\overline{\overline{\alpha+\beta\gamma}+\overline{\beta+\gamma\alpha}+\overline{\gamma+\alpha\beta}} \qquad (6.1)$$

или

$$\alpha\beta\bar{\gamma}\delta + \bar{\alpha}\beta\gamma\bar{\delta} + \alpha\bar{\beta}\gamma\delta + \bar{\alpha}\beta\bar{\gamma}\bar{\delta}. \qquad (6.1')$$

При изучении булевых многочленов основным является вопрос об их упрощении и идентификации (выяснении, отличаются ли по существу друг от друга два по-разному записанных многочлена или представляют лишь разные формы одного выражения). Так, например, вовсе не очевидно, что последний из многочленов (1) совпадает с предпоследним, а второй равен о.

В обычной (школьной) алгебре установление совпадения или несовпадения двух целых рациональных выражений (многочленов) осуществляется с помощью приведения многочленов к стандартному («каноническому») виду: каждый многочлен $P(x_1, \dots, x_k)$ от k переменных $x_1, x_2, \dots, x_k$ может быть записан в виде

$$P = \Sigma c_{i_1 i_2 \dots i_k} x_1^{i_1} x_2^{i_2} \dots x_k^{i_k}, \qquad (6.2)$$

где $c_{i_1 i_2 \dots i_k}$ — отличные от нуля (числовые) коэффициенты многочлена, а $i_1, i_2, \dots, i_k$ — (целые неотрицательные) степени, часть которых (или даже все) может и обращаться в нуль; наибольшая из сумм $i_1 + i_2 + \dots + i_k = N$ называется *степенью* многочлена P. Аналогичное положение справедливо и для булевой алгебры, где выполняется следующая

Теорема. Пусть $P = P(\xi_1, \xi_2, \dots, \xi_k)$ — булев многочлен, зависящий от (произвольных или переменных) элементов $\xi_1, \xi_2, \dots, \xi_k$ фиксированной структуры (5.1)[1]; тогда P либо тождественно (при любых $\xi_1, \xi_2, \dots, \xi_k$) равен о, либо P можно записать в виде

$$P = \Sigma \xi_1' \xi_2' \dots \xi_k', \qquad (6.3)$$

где множитель ξ_i' ($i = 1, 2, \dots,$ или k) в каждом члене стоящей справа суммы обозначает ξ_i или $\bar{\xi}_i$. При этом, если два многочлена

[1] Далее мы считаем, что для рассматриваемой структуры $о \neq \iota$ (ср. со сказанным на с. 38).

$P(\xi_1, \xi_2, \ldots, \xi_k)$ и $Q(\xi_1, \xi_2, \ldots, \xi_k)$ тождественны (т. е. совпадают при любых наборах $\xi_1, \xi_2, \ldots, \xi_k \in \mathcal{B}$), то они имеют одинаковую форму (3), а если они различны, то и формы (3) этих многочленов будут различаться.

Форма (3) булева многочлена (представление о которой может дать, например, многочлен (1′) от переменных $\alpha, \beta, \gamma, \delta \in \mathcal{B}$) называется его *совершенной нормальной аддитивной формой* (от лат. additio — сложение).

◀ Доказательство теоремы совсем просто. Прежде всего, с помощью соотношений де Моргана (XI) мы можем преобразовать многочлен

$$P = P(\xi_1, \ldots, \xi_k)$$

так, чтобы (унарная) операция $\bar{\ }$ в новой его записи применялась лишь к «булевым переменным» $\xi_1, \xi_2, \ldots, \xi_k$, но не к их комбинациям — суммам или произведениям. Далее, воспользовавшись (первым) дистрибутивным законом (IIIа), мы можем раскрыть скобки во всех случаях, когда они означают, что для получения выражения P надо перемножить между собой суммы каких-то элементов ξ_i и ξ_j булевой структуры или более сложных выражений. При раскрытии всех таких скобок мы приведем многочлен P к «аддитивной» форме, представляющей собой сумму ряда членов, каждый из которых является произведением элементов $\xi_i \in \mathcal{B}$ и выражений $\bar{\xi}_j$.

Далее, если какой-либо член A полученной суммы не содержит, скажем, ни множителя ξ_1, ни множителя $\bar{\xi}_1$, то мы заменим его выражением $A(\xi_1 + \bar{\xi}_1) = A\xi_1 + A\bar{\xi}_1$, т. е. суммой двух членов, один из которых содержит множитель ξ_1, а второй — множитель $\bar{\xi}_1$ (см. (VIIIа), (IVб), (IIIа)). Таким образом, мы можем придать P вид суммы, все слагаемые которой содержат (с чертой над соответствующим множителем или без нее) в с е переменные $\xi_1, \xi_2, \ldots, \xi_n$. При этом, если какой-либо член суммы P содержит сразу о б а множителя ξ_i и $\bar{\xi}_i$, то в силу (VIIIб), (Vб) и (IVа) его можно отбросить; если же в него один и тот же множитель ξ_j входит несколько раз, то в силу (VIб) этот множитель можно сохранить лишь один раз [здесь мы учитываем, разумеется, коммутативный закон (Iб) и ассоциативный закон (IIб)]. Наконец, если полученная сумма содержит несколько одинаковых слагаемых, то в силу (VIа) из всех этих слагаемых можно оставить лишь одно. Если в результате всех этих операций в сумме P выпадут все члены, то мы будем иметь $P = 0$; в противном случае мы приведем булев многочлен P к совершенной нормальной аддитивной форме (3).

Наконец, очевидно, что если два булева многочлена P и Q приводятся к о д н о й и т о й ж е форме (3), то они тождественно *равны*. С другой стороны, если формы (3) двух многочленов P и Q н е с о в п а д а ю т, то эти многочлены заведомо р а з л и ч н ы, т. е. при некотором выборе переменных $\xi_1, \xi_2, \ldots, \xi_k$ они будут принимать разные значения. В самом деле, пусть, например, $k = 4$ и аддитивная форма (3) многочлена P содержит слагаемое

$$\xi_1\bar{\xi}_2\xi_3\xi_4, \tag{6.4}$$

а форма (3) многочлена Q такого слагаемого не содержит. Подставим теперь в P и Q следующие значения переменных ξ:

$$\xi_1 = \iota, \quad \xi_2 = o, \quad \xi_3 = \iota, \quad \xi_4 = \iota. \tag{6.5}$$

Ясно, что член (4) суммы P при этих значениях ξ_i обратится в $\iota\iota\iota = \iota$, в то время как все другие слагаемые этой суммы будут содержать хотя бы один множитель o и, значит, в силу (Vб) будут равны o. Поэтому мы будем иметь $P(\iota,\ o,\ \iota,\ \iota) = \iota$. С другой стороны, так как сумма Q не содержит (4), то при подстановке в нее значений (5) все члены этой суммы обратятся в o (все они будут содержать множитель o); поэтому

$$Q(\iota,\ o,\ \iota,\ \iota) = o \neq \iota = P(\iota,\ o,\ \iota,\ \iota). \ ▶$$

Пример. Рассмотрим последний из многочленов (1):

$$P(\alpha,\ \beta,\ \gamma) = \overline{\overline{\alpha+\beta\gamma}+\overline{\beta+\gamma\alpha}+\overline{\gamma+\alpha\beta}}. \tag{6.6}$$

◀Обозначим $\overline{\alpha + \beta\gamma} = A$; $\overline{\beta + \gamma\alpha} = B$; $\overline{\gamma + \alpha\beta} = \Gamma$. В силу правила де Моргана (XIa)

$$P = \overline{A + B + \Gamma} = \overline{(A + B) + \Gamma} = \overline{(A + B)}\,\bar{\Gamma} = (\bar{A} \cdot \bar{B})\,\bar{\Gamma} = \bar{A}\bar{B}\bar{\Gamma}.$$

А так как $\bar{A} = \alpha + \beta\gamma$, $\bar{B} = \beta + \gamma\alpha$, $\bar{\Gamma} = \gamma + \alpha\beta$, то

$$P = (\alpha + \beta\gamma)(\beta + \gamma\alpha)(\gamma + \alpha\beta) = \alpha\beta\gamma + \alpha\beta(\alpha\beta) + \alpha(\gamma\alpha)\gamma + \alpha(\gamma\alpha)(\alpha\beta) +$$
$$+ (\beta\gamma)\beta\gamma + (\beta\gamma)\beta(\alpha\beta) + (\beta\gamma)(\gamma\alpha)\gamma + (\beta\gamma)(\gamma\alpha)(\alpha\beta) = \alpha\beta\gamma + \alpha\beta +$$
$$+ \alpha\gamma + \alpha\beta\gamma + \beta\gamma + \alpha\beta\gamma + \alpha\beta\gamma + \alpha\beta\gamma = \alpha\beta\gamma + \alpha\beta + \alpha\gamma + \beta\gamma$$

(здесь мы использовали коммутативный, ассоциативный, идемпотентный законы для умножения и идемпотентный закон для сложения).

Далее

$$\alpha\beta = \alpha\beta(\gamma + \bar{\gamma}) = \alpha\beta\gamma + \alpha\beta\bar{\gamma}$$

и аналогично

$$\alpha\gamma = \alpha\beta\gamma + \alpha\bar{\beta}\gamma, \quad \beta\gamma = \alpha\beta\gamma + \bar{\alpha}\beta\gamma,$$

так что окончательно получаем

$$P = \alpha\beta\gamma + \alpha\beta\gamma + \alpha\beta\bar{\gamma} + \alpha\beta\gamma + \alpha\bar{\beta}\gamma + \alpha\beta\gamma + \bar{\alpha}\beta\gamma = \alpha\beta\gamma + \alpha\beta\bar{\gamma} + \alpha\bar{\beta}\gamma +$$
$$+ \bar{\alpha}\beta\gamma. ▶ \tag{6.6'}$$

Наше доказательство однозначности представления булева многочлена, т. е. того, что никакой многочлен P не может иметь две разные формы (3), доставляет одновременно простой алгоритм приведения P к виду (3), не требующий обращения к сложным преобразованиям с использованием правил де Моргана. Для простоты предположим снова, что $k = 4$, т. е. что P зависит от четырех переменных

$\xi_1, \xi_2, \xi_3, \xi_4$. Мы видели выше, что форма (3) многочлена P содержит слагаемое (4) в том случае, если $P(\iota, o, \iota, \iota) = \iota$, и не содержит члена (4), если $P(\iota, o, \iota, \iota) = o$. [Так как множество $\{o, \iota\}$ замкнуто относительно всех операций булевой структуры, то ясно, что если все значения переменных многочлена P равны o или ι, то и значение P может быть равно лишь или o или ι.] Введем теперь «стандартные переменные» ω, равные o или ι; тогда форму (3) многочлена P можно будет записать так:

$$P = \Sigma P(\omega_1, \omega_2, \ldots, \omega_k)\, \xi_1' \xi_2' \ldots \xi_k', \tag{6.3'}$$

где в коэффициенте $P(\omega_1, \omega_2, \ldots, \omega_k)$ при произведении $\xi_1', \xi_2', \ldots, \xi_k'$ положено $\omega_i = \iota$, если ξ_i' равно ξ_i, и $\omega_i = o$, если ξ_i' — это $\bar{\xi}_i$. Ясно, что все коэффициенты $P(\omega_1, \omega_2, \ldots, \omega_k)$ будут равны либо o, либо ι, причем в силу (IVб) и (Iб) (а также (IVa)) члены суммы (3′) с коэффициентами o можно просто отбросить, а у членов с коэффициентом ι не выписывать этот коэффициент.

Следствие 1. Если два булева многочлена P и Q, зависящие от одних и тех же переменных $\xi_1, \xi_2, \ldots, \xi_k$, совпадают при подстановке вместо ξ_i всевозможных наборов из одних только элементов o и ι, то они *тождественно равны*, т. е. совпадают и при любых значениях $\xi_1, \xi_2, \ldots, \xi_k \in \mathcal{B}$.

◀ Утверждение о совпадении значений P и Q при подстановке вместо $\xi_1, \xi_2, \ldots, \xi_k$ всевозможных наборов $\omega_1, \omega_2, \ldots, \omega_k$ элементов ι и o равносильно предложению о совпадении всех коэффициентов $P(\omega_1, \omega_2, \ldots, \omega_k)$ и $Q(\omega_1, \omega_2, \ldots, \omega_k)$ соответственно совершенной нормальной аддитивной формы (3′) этих многочленов, т. е. тождественному равенству многочленов P и Q. ▶

Следствие 2. Булева структура **B** допускает 2^{2^k} (и только 2^{2^k}) различных многочленов от k переменных.

◀ В самом деле, совершенная нормальная форма (3′) булева многочлена P состоит из 2^k слагаемых, ибо каждый из k сомножителей ξ_1', ξ_2', ..., ξ_k' может иметь одно из двух значений (ξ_1 или $\bar{\xi}_1$, соответственно ξ_2 или $\bar{\xi}_2$, ..., ξ_k или $\bar{\xi}_k$). А так как каждый из коэффициентов $P(\omega_1, \omega_2, \ldots, \omega_k)$ при соответствующих слагаемых может иметь одно из двух значений o или ι, то, варьируя все возможные значения коэффициентов, мы получим всего 2^{2^k} разных форм (3) (или (3′)) булевых многочленов. [В частности, если все коэффициенты многочлена (3′) равны o, то многочлен тождественно равен o, а если все они равны ι, то многочлен тождественно равен ι (почему?).] Поскольку разные формы (3′) соответствуют разным многочленам, то мы и приходим к выводу, что общее число разных булевых многочленов равно 2^{2^k}. ▶

В частности, при $k = 1$ мы имеем следующие $2^{2^1} = 4$ булева выражения (многочлена):

o, ξ, $\bar{\xi}$ и ι $(= \xi + \bar{\xi})$.

а при $k = 2$ число многочленов будет уже равно $2^{2^2} = 16$:

$$o;\ \xi_1\xi_2,\ \xi_1\bar\xi_2,\ \bar\xi_1\xi_2,\ \bar\xi_1\bar\xi_2;\ \xi_1\xi_2+\xi_1\bar\xi_2,\ \xi_1\xi_2+\bar\xi_1\xi_2,\ \bar\xi_1\xi_2+\xi_1\bar\xi_2,\ \xi_1\xi_2+\bar\xi_1\bar\xi_2,$$
$$\xi_1\bar\xi_2+\bar\xi_1\bar\xi_2,\ \bar\xi_1\xi_2+\bar\xi_1\bar\xi_2;\ \xi_1\xi_2+\bar\xi_1\xi_2+\xi_1\bar\xi_2,\ \xi_1\xi_2+\xi_1\bar\xi_2+\bar\xi_1\bar\xi_2,\ \xi_1\xi_2+\bar\xi_1\xi_2+$$
$$+\bar\xi_1\bar\xi_2,\ \xi_1\bar\xi_2+\bar\xi_1\xi_2+\bar\xi_1\bar\xi_2;\ \xi_1\xi_2+\xi_1\bar\xi_2+\bar\xi_1\xi_2+\bar\xi_1\bar\xi_2=\iota.$$

Пример. Обратимся снова к многочлену (6) и приведем его к канонической форме (3), использовав новый алгоритм.

◀ Мы видели, что $P = \overline{A+B+\Gamma} = \bar A\bar B\bar\Gamma$, где $\bar A = \alpha + \beta\gamma$; $\bar B = \beta + \gamma\alpha$ и $\bar\Gamma = \gamma + \alpha\beta$; в силу (Vб) $\bar A\bar B\bar\Gamma \neq o$, лишь если $\bar A \neq o$ и $\bar B \neq o$, $\bar\Gamma \neq o$. Но, очевидно, что если $\alpha, \beta, \gamma = o$ или ι, то $\bar A = \alpha + \beta\gamma \neq o$, лишь если $\alpha = \iota$ или $\beta = \gamma = \iota$; аналогично $\bar B \neq o$, если $\beta = \iota$ или $\gamma = \alpha = \iota$, и $\bar\Gamma \neq o$, если $\gamma = \iota$ или $\alpha = \beta = \iota$. Поэтому, если какие-нибудь две из переменных α, β, γ равны o, то два из выражений $\bar A$, $\bar B$, $\bar\Gamma$ тоже равны o (так, если $\alpha = \beta = o$, то $\bar A = \bar B = o$), а если $\alpha = \beta = \gamma = o$, то и $\bar A = \bar B = \bar\Gamma = o$; если же из переменных α, β, γ значение o имеет только одно, а остальные равны ι, или, тем более, если $\alpha = \beta = \gamma = \iota$, то $\bar A = \bar B = \bar\Gamma = \iota$ и, значит, $P = \bar A\bar B\bar\Gamma = \iota$. Отсюда вытекает, что

$$P = \iota\alpha\beta\gamma + \iota\alpha\bar\beta\gamma + \iota\alpha\beta\bar\gamma + \iota\bar\alpha\beta\gamma + o\alpha\bar\beta\bar\gamma + o\bar\alpha\beta\bar\gamma + o\bar\alpha\bar\beta\gamma + o\bar\alpha\bar\beta\bar\gamma,$$

т. е. снова результат (6″). ▶

Заметим, наконец, что каждый булев многочлен $P = P(\xi_1, \ldots, \xi_k)$ может быть приведен также и к *совершенной нормальной мультипликативной форме* (от лат. multiplicatio — умножение):

$$P = \Pi\,(\xi_1' + \xi_2' + \ldots + \xi_k'), \tag{6.7}$$

где символы ξ_i' имеют тот же смысл, что и в (3) (или в (3′)), и все сомножители (греческая буква Π указывает на произведение ряда множителей, подобно тому как буква Σ символизирует сумму) в правой части различны; такая форма многочлена также является единстеенной и полностью характеризует класс тождественно равных (т. е. одинаковых) многочленов. Доказательство этого утверждения полностью аналогично рассуждениям, с помощью которых мы убедились, что каждый многочлен можно привести к форме (3); только вместо, скажем, первого дистрибутивного закона (IIIа) мы теперь должны будем использовать второй дистрибутивный закон (IIIб) (см. ниже упр. 3).

Упражнения. 6.1. Запишите зависящие соответственно от $\alpha, \beta \in \mathscr{B}$ и от $\alpha, \beta, \gamma \in \mathscr{B}$ многочлены

$$\alpha + \beta;\quad (\alpha + \beta)(\bar\alpha + \bar\beta);\quad \alpha(\bar\beta + \gamma) + \bar\gamma;\quad \alpha\beta + \alpha\gamma + \overline{\bar\alpha\beta}$$

а) в совершенной нормальной аддитивной форме;
б) в совершенной нормальной мультипликативной форме.

6.2. Выпишите все совершенные нормальные мультипликативные формы булевых многочленов от одного и от двух переменных.

6.3. Докажите теорему о возможности приведения каждого булева многочлена к совершенной нормальной мультипликативной форме и теорему об единственности такой формы.

6.4. Докажите, что множество всех булевых многочленов от k переменных по отношению к их булеву сложению, умножению и применению (унарной) операции $-$ («черта») образует булеву структуру с 2^{2^k} элементами; составьте таблицы операций $+$, $\cdot$ и $-$ для элементов таких структур, отвечающих значениям $k = 1$ и $k = 2$.

7. ИНЫЕ АКСИОМАТИКИ БУЛЕВОЙ СТРУКТУРЫ

Булеву структуру мы определили выше как структуру

$$\mathbf{B} = <\mathscr{B};\ +,\ \cdot,\ ^{-},\ \supset>, \tag{7.1}$$

задаваемую 37 аксиомам (I)—(XXI) (с. 37—38) или, короче, как структуру

а) $\mathbf{B} = <\mathscr{B};\ +,\ \cdot>$, $\qquad$ (7.1′)

задаваемую 8 аксиомами $Б_{1-8}$ (с. 45). Однако эти определения ни в коей мере не являются единственно возможными: в научной литературе имеются десятки различных эквивалентных между собой аксиоматик, описывающих один и тот же объект — булеву структуру (или алгебру Буля). Так, например, поскольку в силу формулы де Моргана (XIa) произведение $\alpha\beta$ элементов булевой структуры можно свести к комбинации операций $+$ и $^{-}$:

$$\alpha\beta = \overline{\bar{\alpha} + \bar{\beta}}, \tag{7.2a}$$

то имеется много аксиоматик булевой структуры, кладущих в основу ее определения одни лишь операции $+$ и $^{-}$ (или $\cdot$ и $^{-}$):

б) $\mathbf{B} = <\mathscr{B};\ +,\ ^{-}>$ или в) $\mathbf{B} = <\mathscr{B};\ \cdot,\ ^{-}>$. $\qquad$ (7.1′)

[Заметим, что операцию $^{-}$ через операции $+$ и $\cdot$ выразить нельзя — именно поэтому аксиоматика $Б_{1-8}$ специально постулирует существование отображения $\alpha \to \bar{\alpha}$.] Так, например, достаточно экономным и в то же время удобным является следующее.

О п р е д е л е н и е. *Булевой структурой* называется структура (1′б) с одной бинарной операцией $+$ («сложение») и одной унарной операцией $^{-}$ («черта»), определенными на множестве $\mathscr{B} = \{\alpha, \beta, \gamma, \ldots;\ \iota\}$ (в этом множестве выделен «единичный» элемент ι, обладающий специальными свойствами); эта структура задается следующими аксиомами:

сложение коммутативно, ассоциативно и идемпотентно, т. е.

$Б'_1 : \alpha + \beta = \beta + \alpha$;

$Б'_2 : (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

$Б'_3 : \alpha + \alpha = \alpha$;

кроме того,

$Б'_4 : \alpha + \beta = \alpha$ тогда и только тогда, когда $\alpha + \bar{\beta} = \iota$

(здесь, как всегда, всюду α, β, $\gamma \in \mathscr{B}$ — произвольные элементы множества $\mathscr{B}$).

Если теперь определить

$$\alpha\beta = \overline{\bar{\alpha} + \bar{\beta}}, \tag{7.2a}$$

$$o = \bar{\iota}, \tag{7.3}$$

то из аксиом $Б'_{1-4}$ можно будет вывести аксиомы $Б_{1-8}$ и наоборот.

◀ Мы уже знаем, что из $Б_{1-8}$ вытекают все предложения (I)—(XXI), в частности аксиомы $Б'_{1-3}$; кроме того, мы видели, что из (I)—(XXI) вытекает также равносильность равенства $\alpha + \beta = \alpha$ отношениям $\alpha \supset \beta$ и $\bar{\alpha}\beta = o$ (см. с. 41). Но из $\bar{\alpha}\beta = o$ вытекает $\overline{\bar{\alpha}\beta} = \bar{o}$ или $\alpha + \bar{\beta} = \iota$ — таким образом, и аксиома $Б'_4$ вытекает из $Б_{1-8}$.

Напротив, коммутативность $Б_1$ сложения требуется аксиомой $Б'_1$, а коммутативность $Б_2$ умножения следует из $Б_1$ и определения (2а):

$$\beta\alpha = \overline{\bar{\beta} + \bar{\alpha}} = \overline{\bar{\alpha} + \bar{\beta}} = \alpha\beta$$

Равенство $Б_7$ сразу следует из идемпотентности $Б'_3$ сложения и аксиомы $Б'_4$:

$Б_7$: так как $\alpha + \alpha = \alpha$, то $\alpha + \bar{\alpha} = \iota$.

Далее из $Б_7$, идемпотентности $Б'_3$ и ассоциативности $Б'_2$ сложения получаем

$$\alpha + \iota = \alpha + (\alpha + \bar{\alpha}) = (\alpha + \alpha) + \bar{\alpha} = \alpha + \bar{\alpha} = \iota. \tag{Va}$$

Однако мы пока не в силах установить двойственные $Б_7$ и (Va) предложения $Б_8$ и (Vб), поскольку вывод их из $Б_7$ и (Va) базируется на инволютивности (IX) операции «черта», установление которой на базе аксиом $Б'_{1-4}$ оказывается неожиданно сложным[1]. И вообще полное доказательство равносильности аксиоматик $Б_{1-8}$ и $Б'_{1-4}$ вовсе не просто — для того, чтобы получить его, нам придется еще немало потрудиться.

Прежде всего определим отношение $\supset$ между элементами нашей алгебраической системы:

$$\alpha \supset \beta, \text{ если } \alpha + \beta = \alpha. \tag{7.4}$$

Иногда нам будет полезно иметь в виду, что в силу $Б_4$ это определение можно переписать и так:

$$\alpha \supset \beta, \text{ если } \alpha + \bar{\beta} = \iota. \tag{7.4a}$$

При этом рефлексивность (XII), транзитивность (XIII) и антисимметричность (XIV) отношения $\supset$, так же как соотношение (XVIIa), «монотонность сложения» (XXa) и родственное (XXa) предложение (XIXa), совместно с (XVIa) записываемое в виде равенства (XVIIIa), выводятся из определения (4) в точности как на с. 42 (где при выводе всех этих фактов, помимо (4), использовались только коммутативность $Б'_1$, ассоциативность $Б'_2$ и идемпотентность $Б'_3$ сложения).

---

[1] Таким образом, включив в число аксиом еще и требование (IX) инволютивности операции «черта», мы заметно упростили бы анализ рассматриваемой аксиоматики (и не ухудшали бы ее особенно принципиально, поскольку и система аксиом $Б'_{1-4}$ независимой не является; см. с. 60). Нам, однако, кажется, что вывод соотношения (IX) из аксиом $Б'_{1-4}$ сам по себе достаточно поучителен.

Теперь мы можем доказать инволютивность (IX) операции «черта». В самом деле, в силу Б$_7$, коммутативности Б$'_1$ сложения и определения (4а),

так как $\bar{\alpha} + \bar{\bar{\alpha}} = \bar{\bar{\alpha}} + \bar{\alpha} = \iota$, то $\bar{\bar{\alpha}} \supset \alpha$. (7.5)

Точно так же, заменяя α на $\bar{\alpha}$ и на $\bar{\bar{\alpha}}$, получаем

а) $\bar{\bar{\bar{\alpha}}} \supset \bar{\alpha}$ и б) $\bar{\bar{\bar{\bar{\alpha}}}} \supset \bar{\bar{\alpha}}$. (7.6)

Но из (5) и (6б) в силу транзитивности (XIII) отношения $\supset$ следует

$\bar{\bar{\bar{\bar{\alpha}}}} \supset \alpha$, т. е. $\bar{\bar{\bar{\bar{\alpha}}}} + \alpha = \bar{\bar{\bar{\bar{\alpha}}}}$ и, значит, $\bar{\bar{\bar{\alpha}}} + \bar{\alpha} = \iota$ (7.7)

(см Б$'_1$) Из (7) в силу коммутативности Б$'_1$ сложения и определения (4а) вытекает

$\bar{\alpha} + \bar{\bar{\bar{\alpha}}} = \iota$ и, значит, $\bar{\bar{\alpha}} \supset \bar{\bar{\bar{\alpha}}}$. (7.8)

А неравенства (8) и (6а) в силу антисимметричности (XIV) отношения $\supset$ дают

$\bar{\bar{\bar{\alpha}}} = \bar{\alpha}$ (7.9)

(наконец-то из леса неравенств выплыло содержательное равенство!).

Равенство (9) позволяет переписать Б$_7$ так:

$\alpha + \bar{\bar{\bar{\alpha}}} = \iota$,

что в силу (4а) равносильно

$\alpha \supset \bar{\bar{\alpha}}$. (7.10)

Таким образом, мы имеем два противоположных неравенства (5) и (10), в силу (XIV) сразу приводящие нас к требуемому результату:

$\bar{\bar{\alpha}} = \alpha$. (IX)

Из (IX) прежде всего следует

$\bar{o} = \iota$ (Xб)

(см. определение (3)). А теперь из Б$_7$ и (Va) в силу определения (2а) получаем соответственно

Б$_8$: $\alpha\bar{\alpha} = \overline{\bar{\alpha} + \bar{\bar{\alpha}}} = \overline{\bar{\alpha} + \alpha} = \overline{\alpha + \bar{\alpha}} = \bar{\iota} = o$;

и

$\alpha o = \overline{\bar{\alpha} + \bar{o}} = \overline{\bar{\alpha} + \iota} = \bar{\iota} = o$. (Vб)

Инвалютивность (IX) операции «черта» позволяет далее установить последнее из основных свойств отношения $\supset$:

если $\alpha \supset \beta$, то $\alpha + \bar{\beta} = \iota$ или $\bar{\beta} + \bar{\bar{\alpha}} = \iota$, т. е. $\bar{\beta} \supset \bar{\alpha}$ (XXI)

(помимо (IX), здесь использованы коммутативность Б$'_1$ сложения и дважды определение (4а)). Из (IX) вытекает также идемпотентность (VIб) и ассоциативность (IIб) умножения:

$\alpha\alpha = \overline{\bar{\alpha} + \bar{\alpha}} = \bar{\bar{\alpha}} = \alpha$ (VI б) (здесь использована идемпотентность $Б_3'$ сложения) и

$$(\alpha\beta)\,\gamma=\overline{\bar\alpha+\bar\beta}\cdot\gamma=\overline{\overline{\overline{\bar\alpha+\bar\beta}}+\bar\gamma}=\overline{(\bar\alpha+\bar\beta)+\bar\gamma}=\overline{\bar\alpha+(\bar\beta+\bar\gamma)}=$$

$$=\overline{\bar\alpha+\overline{\overline{\bar\beta+\bar\gamma}}}=\alpha\cdot\overline{\bar\beta+\bar\gamma}=\alpha\,(\beta\gamma) \qquad \text{(IIб)}$$

(здесь работает ассоциативность $Б_2'$ сложения). Наконец, из (IX) следует также двойственное определению (2а) правило де Моргана (XIб):

$$\overline{\alpha\beta}=\overline{\overline{\overline{\bar\alpha+\bar\beta}}}=\bar\alpha+\bar\beta, \qquad \text{(XI б)}$$

откуда, в свою очередь, в силу того же соотношения (IX) вытекает возможность (2б) выразить сложение через умножение:

$$\overline{\bar\alpha\,\bar\beta}=\bar{\bar\alpha}+\bar{\bar\beta}=\alpha+\beta. \qquad \text{(7.2б)}$$

[Заметим, что из (IX) и (2а) следует также первая формула де Моргана:

$$\bar\alpha\,\bar\beta=\overline{\bar{\bar\alpha}+\bar{\bar\beta}}=\overline{\alpha+\beta} \qquad \text{(XVIa)}$$

— удивительно, как много плодов принесло скромное соотношение (IX)!]. Наконец, с помощью (IX) можно доказать и двойственное определению (4) предложение (XVIIб):

если $\alpha\supset\beta$, то $\bar\beta\supset\bar\alpha$, т. е. $\bar\beta+\bar\alpha=\bar\beta$,

откуда $\overline{\bar\beta+\bar\alpha}=\bar{\bar\beta}=\beta$, т. е. $\beta\alpha=\beta$ или $\alpha\beta=\beta$ (XVIIб)

(кроме (IX), здесь использованы (XXI), коммутативность $Б_2$ умножения и определения (4) и (2а)).

Очень важно заметить, что доказанные нами факты влекут за собой также справедливость утверждения двойственного аксиоме $Б_4'$:

равенство $\alpha\beta=\alpha$, т. е. $\overline{\bar\alpha+\bar\beta}=\alpha$ равносильно $\overline{\overline{\bar\alpha+\bar\beta}}=\bar\alpha$ или $\bar\alpha+\bar\beta=\bar\alpha$. Но из последнего равенства следует, что $\bar\alpha+\bar{\bar\beta}=\iota$, т. е. что $\overline{\bar\alpha+\bar\beta}=\bar\iota$; таким образом,

$$\alpha\beta=\alpha \quad \text{равносильно} \quad \alpha\bar\beta=o \qquad \text{(7.11)}$$

(здесь мы применяем аксиому $Б_4'$, определение (2а) и свойства (IX) и (Xб) операции «черта»). А это значит, что для задаваемой аксиомами $Б_{1-4}'$ алгебраической структуры справедлив сформулированный на с. 45 **принцип двойственности**, поскольку для нее выполняются двойственные всем аксиомам предложения (ссылками на которые можно заменить ссылки на аксиомы при выводе двойственного данной теореме предложения). Так, аксиоме $Б_1'$ двойствен результат $Б_2$, аксиоме $Б_2'$ — тождество (IIб), аксиоме $Б_3'$ — тождество (VIб) и аксиоме $Б_4'$ — результат (11).

В частности, мы можем считать доказанными предложения:

$$\alpha\subset\beta \quad \text{равносильно} \quad \alpha\bar\beta=o \qquad \text{(7.4б)}$$

(двойственно определению (4а));

$$\alpha\beta\subset\alpha \qquad \text{(XVIб)}$$

(двойственно (XVIa));

если $\alpha\subset\beta$, то $\alpha\gamma\subset\beta\gamma$ (XXб)

(двойственно (XXa)) и

если $\alpha\subset\beta$ и $\alpha\subset\gamma$, то $\alpha\subset\beta\gamma$ (XIXб) (двойственно (XIXа)). Отношения (XIXб) и (XVIб) совместно можно записать так:

$$\alpha\beta = \min[\alpha, \beta]. \qquad \text{(XVIIIб)}$$

Теперь уже нетрудно доказать тождества $Б_5$ и $Б_6$. В самом деле,

$Б_5$: так как $\alpha + \iota = \iota$, т. е. $\alpha + \bar{o} = \iota$, то $\alpha + o = \alpha$

(см. (Vа), (Xб) и $Б_4'$) и

$Б_6$: так как $\bar{\alpha} + o = \bar{\alpha}$ или $\bar{\alpha} + \bar{\iota} = \bar{\alpha}$, то $\overline{\bar{\alpha} + \bar{\iota}} = \bar{\bar{\alpha}} = \alpha$, т. е. $\alpha\iota = \alpha$

(см. $Б_5$, (Xб), (1) и (IX); впрочем, принцип двойственности позволяет вовсе не доказывать тождество $Б_6$, двойственное $Б_5$).

Более сложно, — но на этой стадии также уже доступно, — доказательство дистрибутивных законов $Б_3$ и $Б_4$. Заметим прежде всего, что из доказанного до сих пор почти немедленно следуют законы поглощения (VII):

$$\text{так как } \alpha\beta \subset \alpha, \text{ то } \alpha + \alpha\beta = \alpha \qquad \text{(VIIа)}$$

(см. (XIVб) и (4)); аналогично

$$\text{так как } \alpha + \beta \supset \alpha, \text{ то } \alpha(\alpha + \beta) = \alpha \qquad \text{(VIIб)}$$

(см. (XVIа) и (XVIIб); впрочем, (VIIб) двойственно (VIIа) и его можно не доказывать).

Менее очевидно нужное нам для дальнейшего тождество

$$\alpha(\bar{\alpha} + \beta) = \alpha\beta, \qquad (7.12)$$

которое в силу $Б_8$ можно считать частным случаем правила $Б_3$. Для того чтобы его доказать, заметим прежде всего, что в силу правила де Моргана (XIа) и тождества (IX)

$$\bar{\alpha} + \beta = \bar{\alpha} + \bar{\bar{\beta}} = \overline{\alpha\bar{\beta}};$$

поэтому, если обозначить левую часть (12) через ξ, то будем иметь

$$\xi = \alpha(\bar{\alpha} + \beta) = \alpha\overline{\alpha\bar{\beta}}. \qquad (7.13)$$

Отсюда следует, что

$$\xi\bar{\beta} = \alpha\overline{\alpha\bar{\beta}}\,\bar{\beta} = (\alpha\bar{\beta})\,\overline{\alpha\bar{\beta}} = o. \qquad (7.14)$$

Но в силу (11) из (14) следует

$$\xi = \xi\beta,$$

а $\xi\beta = [\alpha(\bar{\alpha} + \beta)]\,\beta = \alpha\,[\beta(\beta + \bar{\alpha})] = \alpha\beta$

в силу правила поглощения (VIIб) (а также коммутативности и ассоциативности умножения и коммутативности сложения), чем и завершается доказательство (12).

Теперь мы уже можем перейти к основным правилам $Б_3$ и $Б_4$. Обозначим

$$\alpha(\beta + \gamma) = \eta \text{ и } \alpha\beta + \alpha\gamma = \zeta. \qquad (7.15)$$

Так как в силу (XVIа) $\beta + \gamma \supset \beta$ и $\beta + \gamma \supset \gamma$, то согласно (XXб)

$$\alpha(\beta + \gamma) \supset \alpha\beta \text{ и } \alpha(\beta + \gamma) \supset \alpha\gamma; \qquad (7.16)$$

поэтому в силу (XXа)

$$\alpha(\beta + \gamma) \supset \alpha\beta + \alpha\gamma, \text{ т. е. } \eta \supset \zeta. \qquad (7.17)$$

Сложнее доказывается обратное неравенство

$$\eta \subset \zeta, \qquad (7.17')$$

в силу (4а) равносильное

$$\eta\bar{\zeta} = o. \quad (7.18)$$

Но

$$\eta\bar{\zeta} = \alpha(\beta+\gamma)\overline{\alpha\beta+\alpha\gamma} = \alpha(\beta+\gamma)\overline{\alpha\beta}\,\overline{\alpha\gamma} = \alpha(\beta+\gamma)(\bar{\alpha}+\bar{\beta})(\bar{\alpha}+\bar{\gamma}) =$$

$$= (\beta+\gamma)[\alpha(\bar{\alpha}+\bar{\beta})][\alpha(\bar{\alpha}+\bar{\gamma})]$$

согласно правилам де Моргана (XI), идемпотентности (VIб), коммутативности $Б_2$ и ассоциативности (IIб) умножения. А так как (см. (12))

$$\alpha(\bar{\alpha}+\bar{\beta}) = \alpha\bar{\beta} \quad \text{и} \quad \alpha(\bar{\alpha}+\bar{\gamma}) = \alpha\bar{\gamma},$$

то

$$\eta\bar{\zeta} = (\beta+\gamma)(\alpha\bar{\beta})(\alpha\bar{\gamma}) = \alpha(\beta+\gamma)(\bar{\beta}\bar{\gamma}) = \alpha[(\beta+\gamma)\overline{\beta+\gamma}] = \alpha o = o \quad (7.18')$$

(здесь использованы, помимо коммутативности, ассоциативности и идемпотентности умножения, правило де Моргана (XIa) и соотношение $Б_8$), чем и завершается доказательство неравенства (17′). А из (17) и (17′) в силу антисимметричности (XIV) отношения $\supset$ и вытекает дистрибутивный закон:

$$\eta = \zeta, \text{ т. е. } \alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma.$$

Наконец, второй дистрибутивный закон $Б_4$ двойствен $Б_3$ и, следовательно, может быть выведен из $Б_3$ по принципу двойственности (см. также ниже упр. 1б)).

Итак, мы убедились, что система аксиом $Б'_{1-4}$ равносильна аксиоматике $Б_{1-8}$, а тем самым и исходной аксиоматике (I—XXI)! ▶

Но и система аксиом $Б'_{1-4}$ все еще не является самой экономной из всех возможных! Эта, казалось бы, столь краткая аксиоматика (всего 4 аксиомы!) *не независима*: например, аксиому $Б'_3$ удается вывести из остальных аксиом. При этом аксиому $Б'_4$ удобно переформулировать так:

$Б''_4$: равенство $\alpha+\beta = \delta+\bar{\delta}$ при любом $\delta \in \mathcal{B}$ равносильно равенству $\alpha+\beta = \alpha$.

Такая ее формулировка избавляет нас от необходимости с самого начала фиксировать в множестве $\mathcal{B}$ «особый» элемент ι, который теперь можно определить так:

$$\iota = \delta+\bar{\delta}, \text{ где } \delta \in \mathcal{B} \text{ — любое} \quad (7.19)$$

(из аксиом $Б'_1$, $Б'_2$ и $Б'_4$ можно вывести, что при любом δ суммы (19) совпадают между собой). Но даже и аксиоматику из трех предложений $Б'_1$, $Б'_2$ и $Б''_4$ можно «укоротить», заменив требования $Б'_1$ коммутативности и $Б'_2$ ассоциативности сложения одной «смешанной» аксиомой $Б''_{1,2}$, так что булеву структуру можно задавать и как структуру (1′б), удовлетворяющую всего д в у м аксиомам (безусловный рекорд!):

$Б''_{1,2}$: $(\alpha+\beta)+\gamma = (\beta+\gamma)+\alpha$

(инвариантность «повторного сложения» относительно *циклической подстановки*: $(\alpha, \beta, \gamma) \to (\beta, \gamma, \alpha)$) и

$Б''_4$: $\alpha+\beta = \delta+\bar{\delta}$ равносильно $\alpha+\beta = \alpha$

(разумеется, фигурирующие в аксиомах элементы α, β, γ, $\delta \in \mathcal{B}$ совершенно произвольны, — и в частности $\alpha + \beta = \delta + \bar{\delta}$ при любом $\delta \in \mathcal{B}$ равносильно $\alpha + \beta = \alpha$). При этом, определяя булеву структуру как структуру (1'б), мы, конечно, как всегда, дополнительно вводим в ней бинарную операцию умножения элементов, (бинарное) отношение $\supset$ и особые элементы о и ι формулами:

$$\alpha\beta = \overline{\bar{\alpha} + \bar{\beta}}; \tag{7.2a}$$

$$\alpha \supset \beta \text{ равносильно } \alpha + \beta = \alpha; \tag{7.4}$$

$$\iota = \delta + \bar{\delta} \text{ (где } \delta \in \mathcal{B} \text{ — любое)}; \tag{7.9}$$

$$o = \bar{\iota}. \tag{7.3}$$

Вот еще один вариант задания булевой структуры тремя аксиомами, пожалуй, даже более простыми, чем аксиомы Б$'_1$, Б$'_2$ и Б$''_4$:

Булевой структурой называется структура (1'б), подчиняющаяся следующим аксиомам:

Б$'_1$: сложение коммутативно — для любых элементов α, $\beta \in \mathcal{B}$

$\alpha + \beta = \beta + \alpha$;

Б$'_2$: сложение ассоциативно — для любых элементов α, β, $\gamma \in \mathcal{B}$

$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;

Б$''_3$: для любых двух элементов α, $\beta \in \mathcal{B}$]

$\overline{\bar{\alpha} + \bar{\beta}} + \overline{\bar{\alpha} + \beta} = \alpha$.

Можно также предложить такие системы аксиом булевой структуры, в которых фигурирует лишь е д и н с т в е н н о е исходное отношение элементов (единственная операция булевой структуры). Так, часто оказывается полезным то обстоятельство, что все операции булевой структуры могут быть определены с помощью бинарной операции

$$\alpha \mid \beta = \bar{\alpha}\bar{\beta}, \tag{7.20a}$$

так называемой *операции Шеффера*[1]. Если элементы основного множества $\mathcal{B}$ булевой структуры — это множества A, B, C, ..., для которых операции сложения $A + B$, умножения AB и дополнения $\bar{A}$ определены, как в § 1—2, то операция Шеффера $A \mid B$ имеет смысл *пересечения дополнений* множеств A и B (рис. 27, *а*).

Операция Шеффера, очевидно, коммутативна:

$\alpha \mid \beta = \beta \mid \alpha$

[1] Генри Морис Ш е ф ф е р — американский логик начала XX в.

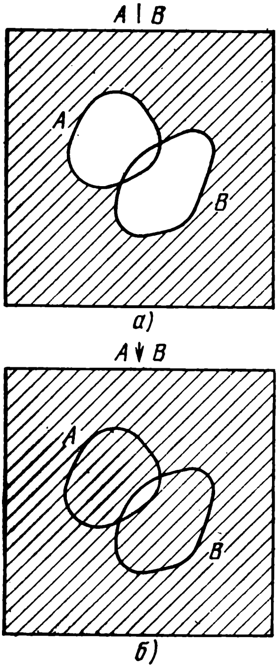


Рис. 27

для любых α, $\beta \in \mathcal{B}$. Далее из аксиом булевой структуры следует, что

$$(\alpha|\beta)|(\alpha|\beta)=\overline{(\bar\alpha\,\bar\beta)}\cdot\overline{(\bar\alpha\,\bar\beta)}=(\bar{\bar\alpha}+\bar{\bar\beta})(\bar{\bar\alpha}+\bar{\bar\beta})=$$
$$=\alpha+\beta;$$

$$(\alpha|\alpha)|(\beta\,|\,\beta)=\overline{(\bar\alpha\,\bar\alpha)}\;\overline{(\bar\beta\,\bar\beta)}=\bar{\bar\alpha}\cdot\bar{\bar\beta}=\alpha\beta;$$

$$(\alpha|\alpha)=\bar\alpha\bar\alpha=\bar\alpha.$$

Таким образом, приняв за основу операцию Шеффера $\alpha|\beta$, мы можем определить $\alpha+\beta$, $\alpha\beta$ и $\bar\alpha$ как $(\alpha|\beta)|(\alpha|\beta)$, $(\alpha|\alpha)|(\beta|\beta)$ и $\alpha|\alpha$; далее, элементы ι и o и отношение $\alpha\supset\beta$ определяются равенствами $\alpha+\bar\alpha=\iota$, $\alpha\bar\alpha=o$ и условием $\alpha+\beta=\alpha$ (или $\alpha\beta=\beta$). Используя эти определения, мы можем сформулировать все аксиомы булевой структуры так, чтобы в них фигурировала единственная операция — операция Шеффера $\alpha|\beta$

Роль операции Шеффера может также играть и другая бинарная операция

$$\alpha\downarrow\beta=\bar\alpha+\bar\beta \tag{7.20б}$$

(в алгебре множеств операция $A\downarrow B$ имеет смысл *объединения дополнений* множеств A и B; рис 27, *б*) Легко видеть, что

$$(\alpha\downarrow\alpha)\downarrow(\beta\downarrow\beta)=\overline{(\bar\alpha+\bar\alpha)}+\overline{(\bar\beta+\bar\beta)}=\bar{\bar\alpha}+\bar{\bar\beta}=\alpha+\beta;$$

$$(\alpha\downarrow\beta)\downarrow(\alpha\downarrow\beta)=\overline{\bar\alpha+\bar\beta}+\overline{\bar\alpha+\bar\beta}=\bar{\bar\alpha}\bar{\bar\beta}+\bar{\bar\alpha}\bar{\bar\beta}=\alpha\beta;$$

$$\alpha\downarrow\alpha=\bar\alpha+\bar\alpha=\bar\alpha;$$

поэтому операции $\alpha+\beta$, $\alpha\beta$ и $\bar\alpha$ можно определить в терминах операции $\alpha\downarrow\beta$

При использовании операции Шеффера, скажем, указанные на с. 61 аксиомы $Б_1'$, $Б_2'$, $Б_3'$, примут следующий вид:

$Ш_1: |(\alpha|\beta)|(\alpha|\beta)=(\beta|\alpha)|(\beta|\alpha);$

$Ш_2: \{[(\alpha|\beta)|(\alpha|\beta)]|\gamma\}|\{[(\alpha|\beta)|(\alpha|\beta)]|\gamma\}=$

$=\{\alpha|[(\beta|\gamma)|(\beta|\gamma)]\}|\{\alpha|[(\beta|\gamma)|(\beta|\gamma)]\};$

$Ш_3$: если $\alpha|\alpha=A$, $\beta|\beta=B$ и

$\{[(A|B)|(A|B)]|[(A|B)|(A|B)]\}|\{[(A|\beta)|(A|\beta)]|[(A|\beta)|(A|\beta)]\}=\Gamma,$

то $\Gamma|\Gamma=\alpha.$

Аксиомы $Ш_{1-3}$ имеют довольно сложную форму. Вместо них можно положить в основу определения булевой структуры три более простые аксиомы, также оперирующие с единственной операцией $\alpha \mid \beta$ (см. ниже упр. 4):

$Ш'_1$: $(\alpha \mid \alpha) \mid (\alpha \mid \alpha) = \alpha$;

$Ш'_2$: $\alpha \mid [\beta \mid (\beta \mid \beta)] = \alpha \mid \alpha$;

$Ш'_3$: $[\alpha \mid (\beta \mid \gamma)] \mid [\alpha \mid (\beta \mid \gamma)] = [(\beta \mid \beta) \mid \alpha] \mid [(\gamma \mid \gamma) \mid \alpha]$.

Таким образом, булеву структуру можно определить как систему

$B = \langle \mathscr{B}; \mid \rangle$

с одной бинарной алгебраической операцией $\mid$ подчиняющейся трем аксиомам $Ш'_{1-3}$.

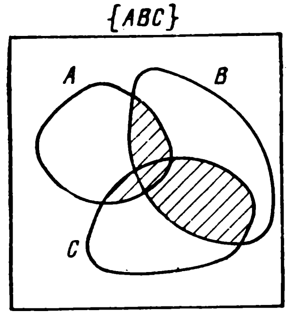


Рис. 28

Иногда в основу определения алгебры Буля кладут единственную *тернарную* операцию

$$\{\alpha\beta\gamma\} = \alpha\beta + \beta\gamma + \gamma\alpha = (\alpha + \beta)(\beta + \gamma)(\gamma + \alpha), \qquad (7.21)$$

сопоставляющую новый элемент $\{\alpha\beta\gamma\}$ с каждыми т р е м я элементами α, β, γ алгебры Буля (ср. Пример на с. 16). В алгебре множеств $\{ABC\} = AB + BC + CA$ представляет собой *объединение попарных пересечений* множеств A, B и C (рис. 28), или, что то же самое, *пересечение попарных объединений* этих трех множеств.

Тернарная операция (21), очевидно, коммутативна по любым двум входящим в нее элементам:

$$\{\alpha\beta\gamma\} = \{\alpha\gamma\beta\} = \{\beta\alpha\gamma\} = \{\beta\gamma\alpha\} = \{\gamma\alpha\beta\} = \{\gamma\beta\alpha\}. \qquad (7.22)$$

Далее, она обладает своеобразной дистрибутивностью:

$$\{\alpha\beta\{\gamma\delta\varepsilon\}\} = \{\{\alpha\beta\gamma\}\,\delta\,\{\alpha\beta\varepsilon\}\} \qquad (7.22а)$$

и (ослабленной) ассоциативностью:

$$\{\alpha\beta\{\gamma\beta\delta\}\} = \{\{\alpha\beta\gamma\}\,\beta\delta\}. \qquad (7.22б)$$

Наконец, для нее имеет место закон, аналогичный идемпотентным законам для сложения и умножения:

$$\{\alpha\alpha\beta\} = \alpha. \qquad (7.23а)$$

Операцию можно определить с помощью тернарной операции $\{\alpha\beta\gamma\}$ следующим условием, родственным идемпотентному закону (23а):

$$\{\alpha\bar{\alpha}\beta\} = \beta. \qquad (7.23б)$$

Так как это условие симметрично относительно элементов α и $\bar{\alpha}$, то из него, очевидно, следует

$\bar{\bar{\alpha}} = \alpha$.

Далее, если фиксировать в множестве элементов α, β, γ, ..., для которых определена тернарная операция $\{\alpha\beta\gamma\}$, «особый» элемент ι и положить $\bar{\iota} = o$, то можно будет определить и основные (бинарные) операции алгебры Буля через тернарную операцию $\{\alpha\beta\gamma\}$:

а) $\alpha + \beta = \{\alpha\beta\iota\}$, б) $\alpha\beta = \{\alpha\beta o\}$. $\qquad$ (7.24)

При этом в силу (24)

$$\alpha + o = \{\alpha o \iota\} = \{\alpha \bar{\iota}\, \iota\} = \alpha \quad \text{и} \quad \alpha\iota = \{\alpha\iota o\} = \{\alpha\bar{\iota}\,\iota\} = \alpha;$$

$$\alpha + \iota = \{\alpha\iota\iota\} = \iota \ \text{ и } \ \alpha o = \{\alpha o o\} = o.$$

Определения (23б) и (24а, б) позволяют сформулировать все аксиомы алгебры Буля таким образом, чтобы в них участвовала лишь тернарная операция $\{\alpha\beta\gamma\}$.

Существуют и многие другие способы аксиоматического определения алгебры Буля; двух из них мы еще коснемся ниже (см. § 8—9).

Упражнения. 7.1. Выведите непосредственно из аксиом $Б'_{1-4}$, не обращаясь к принципу двойственности:

а) двойственное (12) равенство $\alpha + \bar{\alpha}\beta = \alpha + \beta$;

б) второй дистрибутивный закон $\alpha + \beta\gamma = (\alpha + \beta)(\alpha + \gamma)$.

7.2. Составьте равносильный первоначальному набору аксиом (а значит, и аксиомам (I)—(XXI)) список аксиом, двойственный:

а) аксиомам $Б'_{1-4}$;

б) аксиомам $Б'_1$, $Б'_2$, $Б''_4$;

в) аксиомам $Б''_{1,2}$, $Б''_4$;

г) аксиомам $Б'_1$, $Б'_2$, $Б''_3$.

7.3. Запишите аксиомы $Б'_1$, $Б'_2$, $Б''_3$, используя единственную операцию $\downarrow$.

7.4. Проверьте равенства $Ш''_{1-3}$, подставив в них вместо операции $|$ ее определение (20а).

7.5. Проверьте тождества (22); (23); (24)

7.6. Выразите

а) операцию $|$ через операцию $\downarrow$ и наоборот;

б) операцию $|$ через операцию $\{\ \}$ и наоборот.

8. БУЛЕВЫ СТРУКТУРЫ И РЕШЕТКИ; КОНЕЧНЫЕ БУЛЕВЫ СТРУКТУРЫ

Выше мы уже встречались с понятием решетки — математической структуры

$$\mathrm{L} = \langle \mathcal{L}; \supset \rangle \qquad (8.1)$$

с одним (бинарным) отношением $\supset$ между элементами основного множества $\mathcal{L}$, являющимся *отношением* (частичного) *порядка*, т. е. удовлетворяющим аксиомам:

$P_1 : \lambda \supset \lambda$ для всех $\lambda \in \mathcal{L}$

(*рефлексивность* отношения $\supset$);

P_2: если $\lambda \supset \mu$ и $\mu \supset \lambda$, то $\lambda = \mu$

(*антисимметричность*);

P_3: если $\lambda \supset \mu$ и $\mu \supset \nu$, то $\lambda \supset \nu$

(*транзитивность*). Впоследствии вместо $\lambda \supset \mu$ мы иногда будем писать $\mu \subset \lambda$; мы также будем применять привычную для отношений порядка терминологию, говоря о «неравенствах», употребляя термины «больше» и «меньше», «максимум» и «минимум» и т. д.

Чтобы структура (1) являлась решеткой, необходимо выполнение для нее наряду с аксиомами P_{1-3} еще одного дополнительного условия:

P_4: для каждых $\lambda, \mu \in \mathcal{L}$ существует их (строгий) максимум $\max[\lambda, \mu]$ и (строгий) минимум $\min[\lambda, \mu]$, где строгий максимум (точная верхняя грань) и строгий минимум (точная нижняя грань) определяются описанными на с. 26 условиями.

Частично упорядоченные структуры принято изображать графическими схемами, подобными рис. 17, где элементы α и β, такие, что $\alpha \supset \beta$, изображаются (соединенными между собой) точками, причем точка α лежит выше β; такие схемы называются *диаграммами Гессе*[1]. При этом диаграмма Гессе решетки характеризуется тем, что для каждых двух ее вершин λ и μ существует ровно одна ближайшая к ним и не более низкая, чем λ и μ, вершина $\rho = \max[\lambda, \mu]$ и одна ближайшая к λ и μ не высшая, чем они, вершина $\sigma = \min[\lambda, \mu]$ (см. рис. 17 или рис. 29—32). Разумеется, (абстрактно заданное аксиомами P_{1-4}) отношение $\supset$ само по себе никак не связано с отношением включения для множеств или с отношением $\alpha \supset \beta$ элементов булевой структуры (которое можно определить, например, равенствами $\alpha + \beta = \alpha$ или $\alpha\beta = \beta$, а в нашем множестве $\mathcal{L}$ пока нет никакого сложения или умножения!). Однако выполнимость в кажой булевой структуре правил (XII)—(XIV) и (XVIII) доказывает, что *каждая булева структура по существующему в ней отношению $\supset$ представляет собой решетку*.

Итак, от понятия булевой структуры легко перейти к понятию решетки; интересно, однако, что и многие решетки могут быть сведены к булевым структурам. Чтобы доказать это пока еще достаточно неопределенное утверждение (что такое «многие»? и что такое «могут быть сведены»?), нам придется подробнее остановиться на общих свойствах решеток

Аксиома P_4 постулирует существование в каждой решетке двух бинарных операций max и min:

$$(\lambda, \mu) \to \rho = \max[\lambda, \mu] \text{ и } (\lambda, \mu) \to \sigma = \min[\lambda, \mu]. \qquad (8.2)$$

[1] Отто Гессе (1811—1874) — известный немецкий математик.

Исходя из свойств (XVIII) булевой структуры, мы условимся называть эти операции («решетчатыми») *сложением* и *умножением*, в соответствии с чем введем следующие обозначения:

$$\max[\lambda, \mu] = \lambda + \mu \text{ и } \min[\lambda, \mu] = \lambda\mu \tag{8.2'}$$

(разумеется, (2′)— это даже не определение, а просто введение новой терминологии и символики для имевшихся ранее понятий).

Докажем теперь основные свойства введенных операций: в каждой решетке для любых $\lambda, \mu, \nu \in \mathscr{L}$

$$\text{а) } \lambda + \mu = \mu + \lambda \text{ и б) } \lambda\mu = \mu\lambda \tag{I}$$

(*коммутативность* решетчатых *сложения и умножения*);

$$\text{а) } (\lambda + \mu) + \nu = \lambda + (\mu + \nu) \text{ и б) } (\lambda\mu)\nu = \lambda(\mu\nu) \tag{II}$$

(*ассоциативность* этих операций, позволяющая вместо фигурирующих в равенствах (III) выражений писать просто $\lambda + \mu + \nu$ и $\lambda\mu\nu$ без скобок);

$$\text{а) } \lambda + \lambda = \lambda \text{ и б) } \lambda\lambda = \lambda \tag{VI}$$

(*идемпотентность*);

$$\text{а) } \lambda + \lambda\mu = \lambda \text{ и б) } \lambda(\lambda + \mu) = \lambda \tag{VII}$$

(законы *поглощения*)

◀ В самом деле, равенства (I) и (VI) непосредственно следуют из определений (2′) решетчатого сложения и умножения. Почти столь же очевидна и выполнимость равенств (II). Так как

$$\pi = (\lambda + \mu) + \nu = \max[\max[\lambda, \mu], \nu],$$

то, очевидно, $\pi \supset \lambda$ и $\pi \supset \mu$ (ибо $\pi \supset \max[\lambda, \mu]$), а также $\pi \supset \nu$. Последние три неравенства можно записать так:

$$\pi = \mathrm{Max}[\lambda, \mu, \nu] \tag{8.3a}$$

(ср. с введенными на с. 25 обозначениями). Но, более того, π — наименьший из «максимумов» $\mathrm{Max}[\lambda, \mu, \nu]$ элементов λ, μ и ν, ибо, если $\Pi \supset \lambda$, $\Pi \supset \mu$ и $\Pi \supset \nu$, то $\Pi \supset \max[\lambda, \mu]$ (в силу самого определения строгого максимума) и $\Pi \supset \nu$, т. е. (снова в силу определения понятия max)

$$\Pi \supset \max[\max[\lambda, \mu], \nu] = \pi.$$

Поэтому π — «наименьший максимум» для λ, μ и ν или «наименьший из бо́льших и λ, и μ, и ν элементов», т. е. «строгий» максимум λ, μ и ν, что естественно записать так:

$$\pi = \max[\lambda, \mu, \nu] \tag{8.4a}$$

(ср. с. 97). Точно так же доказывается: если $\pi_1 = \lambda + (\mu + \nu) = \max[\lambda, \max[\mu, \nu]]$, то

$$\pi_1 = \max[\lambda, \mu, \nu] = \pi,$$

чем и устанавливается равенство (IIа). Совершенно аналогично доказывается и равенство (IIб), вытекающее из того, что в естественных обозначениях

$$(\lambda\mu)\nu = \lambda(\mu\nu) = \min[\lambda, \mu, \nu]. \qquad (8.4б)$$

Наконец,

$$\sigma = \lambda + \lambda\mu = \max[\lambda, \min[\lambda, \mu]],$$

откуда следует, что $\sigma \supset \lambda$. Но так как $\lambda \supset \lambda$ (рефлексивность P_1 отношения $\supset$!) и $\lambda \supset \min[\lambda, \mu]$, то по определению операции max имеем $\lambda \supset \max[\lambda, \min[\lambda, \mu]] = \sigma$. А два неравенства $\sigma \supset \lambda$ и $\lambda \supset \sigma$ в силу антисимметричности P_2 влекут (VIIа):

$$\sigma = \lambda.$$

Совершенно аналогично устанавливается и равенство (VIIб) (см. упр. 2). ▶

Докажем еще несколько свойств решеток, касающихся связи отношения $\supset$ с (решетчатыми) сложением и умножением. А именно, покажем, что в каждой решетке L для любых $\lambda, \mu, \nu \in \mathcal{L}$

а) $\lambda + \mu \supset \lambda$ и б) $\lambda \supset \lambda\mu$; (XVI)

$\lambda \supset \mu$ равносильно тому, что

а) $\lambda + \mu = \lambda$; б) $\lambda\mu = \mu$; (XVII)

а) если $\lambda \supset \mu$ и $\lambda \supset \nu$, то $\lambda \supset \mu + \nu$;

б) если $\lambda \supset \nu$ и $\mu \supset \nu$, то $\lambda\mu \supset \nu$ (XIX)

и

если $\lambda \supset \mu$, то а) $\lambda + \nu \supset \mu + \nu$; б) $\lambda\nu \supset \mu\nu$ (XX)

(согласованность отношения $\supset$ с решетчатыми сложением и умножением).

◀ Ясно, что правила (XVI), (XVII) и (XIX) непосредственно вытекают из определений (2′) (в частности, предложения (XIX) суть определения строгого максимума и минимума). А из (XVII) сразу следует и (XX): в самом деле,

если $\lambda \supset \mu$, то $\lambda + \mu = \lambda$ и $(\lambda + \nu) + (\mu + \nu) = (\lambda + \mu) + (\nu + \nu) = (\lambda + \mu) + \nu = \lambda + \nu$, т. е. $\lambda + \nu \supset \mu + \nu$;

совершенно так же из (XVIIб) выводится (XXб) (здесь используется коммутативность, ассоциативность и идемпотентность решетчатых сложения и умножения). ▶

Предложения (XVII) позволяют, считая заданными операции решетчатого сложения и умножения, с их помощью ввести отношение порядка $\supset$. А это, в свою очередь, приводит к (эквивалентному исходному) определению решетки как алгебраической структуры

$$\mathbf{L} = < \mathscr{L};\ +,\ \cdot > \tag{8.1'}$$

с двумя бинарными алгебраическими операциями $+$ (сложение) и $\cdot$ (умножение), удовлетворяющими следующим восьми аксиомам:

$P'_{1,2}$: а) $\lambda + \mu = \mu + \lambda$ и б) $\lambda\mu = \mu\lambda$

(*коммутативность*);

$P'_{3,4}$: а) $(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$ и б) $(\lambda\mu)\nu = \lambda(\mu\nu)$

(*ассоциативность*);

$P'_{5,6}$: а) $\lambda + \lambda = \lambda$ и б) $\lambda\lambda = \lambda$

(*идемпотентность*);

$P'_{7,8}$: а) $\lambda + \lambda\mu = \lambda$ и б) $\lambda(\lambda + \mu) = \lambda$

(законы *поглощения*; см., впрочем, ниже упр. 4). [Ясно, что из «самодвойственного» характера определяющих решетку аксиом следует справедливость в теории решеток *принципа двойственности*, позволяющего заменять во всех относящихся к решеткам формулах и предложениях сложение умножением и наоборот (ср. с. 18 или 45); при этом в силу двойственности определений:

$$\left.\begin{array}{l}\text{а) если } \lambda \supset \mu, \text{ то } \lambda + \mu = \mu;\\ \text{б) если } \lambda \subset \mu, \text{ то } \lambda\mu = \lambda\end{array}\right. \tag{XVII}$$

отношение $\supset$ по принципу двойственности заменяется на $\subset$.]

◀ В самом деле, мы видели выше, что в каждой решетке при определениях (2′) выполняются все правила P'_{1-8}. С другой стороны, пусть мы имеем структуру (1′), удовлетворяющую аксиомам P'_{1-8}; введем в ней отношение $\supset$ условием

$$\lambda \supset \mu \text{ равносильно равенству } \lambda + \mu = \lambda. \tag{XVIIa}$$

Заметим прежде всего, что (XVIIa) эквивалентно определению:

$$\lambda \supset \mu \text{ равносильно равенству } \lambda\mu = \mu \tag{XVIIб}$$

Действительно, пусть $\lambda \supset \mu$ в смысле определения (XVIIa); тогда в силу P'_8 и $P'_{1,2}$

$$\mu = \mu(\mu + \lambda) = \mu\lambda = \lambda\mu. \tag{8.5a}$$

Обратно, если выполняется (5а), то

$$\lambda = \lambda + \lambda\mu = \lambda + \mu, \tag{8.5б}$$

что и устанавливает эквивалентность равенств (5а) и (5б).

Далее, рефлексивность $\lambda \supset \lambda$ введенного согласно (XVIIa) отношения $\supset$ следует из идемпотентности сложения; транзитивность этого отношения вытекает из ассоциативности сложения, а антисимметричность — из коммутативности сложения (ср. с. 42). Наконец, равенство

$$\lambda + \mu = \max[\lambda, \mu] \qquad \text{(XVIa)}$$

базируется на законах поглощения:

из $\lambda(\lambda + \mu) = \lambda$ следует $\lambda \subset \lambda + \mu$ или $\lambda + \mu \supset \lambda$

(см. (XVIIб)); аналогично убеждаемся в том, что $\lambda + \mu \supset \mu$, так что

$$\lambda + \mu = \mathrm{Max}[\lambda, \mu]. \qquad (8.6)$$

Пусть теперь

$$M = \mathrm{Max}[\lambda, \mu], \text{ т. е. } M \supset \lambda \text{ и } M \supset \mu, \text{ или } M + \lambda = M + \mu = M. \qquad (8.7)$$

Тогда

$$M + (\lambda + \mu) = (M + \lambda) + \mu = M + \mu = M, \qquad (8.7')$$

откуда вытекает, что

$$M \supset \lambda + \mu. \qquad (8.8)$$

Из (6), (7) и (8) следует, что

$$\lambda + \mu = \max[\lambda, \mu]. \qquad \text{(XVIa)}$$

Аналогично устанавливается

$$\lambda\mu = \min[\lambda, \mu] \qquad \text{(XVIб)}$$

(см. ниже упр. 3), чем и завершается проверка выполнимости в системе (1′) всех аксиом P_{1-4}. ▶

Единичным элементом (или «единицей») решетки называется ее абсолютный максимум, т. е. такой элемент ι, что

$$\iota \supset \lambda \text{ для всех } \lambda \in \mathcal{L}. \qquad \text{(XVa)}$$

Аналогично *нулевым* элементом («нулем») решетки называется ее абсолютный минимум — такой элемент o, что

$$o \subset \lambda \text{ для все } \lambda \in \mathcal{L}. \qquad \text{(XVб)}$$

Разумеется, из одних лишь аксиом P_{1-4} еще вовсе не следует существование в решетке единичного или нулевого элемента. [Исключением являются лишь конечные решетки, для которых множество $\mathcal{L} = \{\lambda, \mu, \nu, \ldots, \xi\}$ конечно — здесь, очевидно,

$$\iota = \lambda + \mu + \ldots + \xi \quad (= \max[\lambda, \mu, \ldots, \xi]);$$

$$o = \lambda\mu \ldots \xi \quad (= \min[\lambda, \mu, \ldots, \xi]),$$

откуда ясно, что $\iota \in \mathcal{L}$ и $o \in \mathcal{L}$ (почему?).] Так, например, в упорядоченном по обычному включению множестве всех *конечных* подмножеств множества натуральных чисел (решетка!) существует абсолютный минимум — пустое множество O, но не абсолютный максимум (а в множестве всех *коконечных* — см. с. 49— подмножеств существует абсолютный максимум, но не абсолютный минимум). Множество всех (положительных и неположительных) целых (или рациональных, или вещественных) чисел, упорядоченное обычным образом, или схематически изображенная на рис. 29 (бесконечная) решетка не имеет ни единичного, ни нулевого элемента. Но если для решетки (1) дополнительно выполняется аксиома

P_5 : среди элементов решетки имеется как единичный элемент ι, так и нулевой элемент o,

то для этой решетки, очевидно,

$$а)\ \lambda + o = \lambda \ \text{ и } б)\ \lambda\iota = \lambda; \tag{IV}$$

$$а)\ \lambda + \iota = \iota \ \text{ и } б)\ \lambda o = o \tag{V}$$

для всех $\lambda \in \mathscr{L}$ (правила (IV) и (V) следуют из (2′) и (XV)).

Особое место среди решеток с нулем и единицей (решеток, удовлетворяющих аксиоме P_5) занимают так называемые «решетки с дополнениями». Решетка (1) называется *решеткой с дополнениями*, если, помимо аксиом P_{1-5}, для нее выполняется также и аксиома

P_6: для каждого $\lambda \in \mathscr{L}$ существует такое $\bar{\lambda} \in \mathscr{L}$, что $\max[\lambda, \bar{\lambda}] = \iota$, $\min[\lambda, \bar{\lambda}] = o$, или, что то же самое,

$$а)\ \lambda + \bar{\lambda} = \iota,\ б)\ \lambda\bar{\lambda} = o. \tag{VIII}$$

Элемент $\bar{\lambda}$ называется *дополнением* элемента λ.

Разумеется, из одного лишь факта существования в решетке нуля o и единицы ι вовсе не вытекает наличие дополнения у каждого элемента: так, например, изображенная на диаграмме Гессе (рис. 30) решетка не является решеткой с дополнениями (почему?); не являются решетками с дополнениями также решетки, составляющие содержание моделей 3 (где от числа N не требуется, чтобы оно было «свободно от квадратов») и 4 из § 10. Далее, из выполнения аксиомы P_6 вовсе не следует единственность дополнения: так, изображенные на рис. 31, *а*, *б* диаграммы Гессе отвечают решеткам с дополнениями, но на рис. 31,*а* $\lambda = \bar{\nu}$ и $\mu = \bar{\nu}$, а на рис. 31,*б* $\pi = \bar{\sigma}$ и $\rho = \bar{\sigma}$; $\pi = \bar{\rho}$ и $\sigma = \bar{\rho}$; $\rho = \bar{\pi}$ и $\sigma = \bar{\pi}$. Эти же примеры показывают, что известное нам из теории булевых структур утверждение

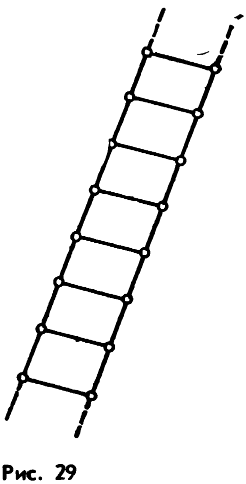


Рис. 29

$$\text{если } \lambda \supset \mu, \text{ то } \bar{\mu} \supset \bar{\lambda}, \tag{XXI}$$

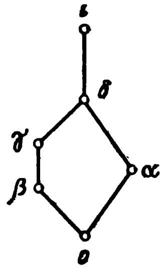


Рис. 30

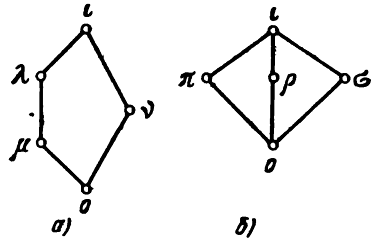


Рис. 31

вообще говоря, не обязано выполняться для решеток с дополнениями (почему?). Однако в силу (IV) и (V) дополнения элементов ι и o всегда единственны:

а) $\bar{\iota} = o$ и б) $\bar{o} = \iota$. (X)

Нетрудно видеть, что во всякой решетке — с нулем и единицей или без них — выполняется родственное дистрибутивному закону (IIIa) неравенство

$$\lambda(\mu + \nu) \supset \lambda\mu + \lambda\nu \tag{8.9}$$

(ср. также упр. 5 ниже).

◀ В самом деле в силу (XVIa) и (XIXб)

$$\lambda(\mu + \nu) \supset \lambda\mu \text{ и } \lambda(\mu + \nu) = \lambda(\nu + \mu) \supset \lambda\nu,$$

откуда (см. (XIXa) и (VIa))

$$\lambda(\mu + \nu) = \lambda(\mu + \nu) + \lambda(\mu + \nu) \supset \lambda(\mu + \nu) + \lambda\mu =$$
$$= \lambda\mu + \lambda(\mu + \nu) \supset \lambda\mu + \lambda\nu. \text{ ▶}$$

Однако равенство (дистрибутивный закон)

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu \tag{IIIa}$$

в решетке может и не выполняться. Так, например, в ситуации рис. 31, *а*

$$\lambda(\mu + \nu) = \lambda\iota = \lambda, \text{ а } \lambda\mu + \lambda\nu = \mu + o = \mu,$$

а для изображенной на рис. 31, *б* решетки

$$\pi(\rho + \sigma) = \pi\iota = \pi, \text{ а } \pi\rho + \pi\sigma = o + o = o.$$

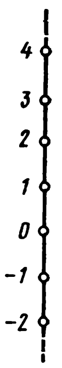


Рис. 32

Если же в решетке имеет место дистрибутивный закон (IIIa), т. е. выполняется аксиома[1]

$$P_7 : \lambda(\mu + \nu) = \lambda\mu + \lambda\nu \text{ для любых } \lambda,\ \mu,\ \nu \in \mathcal{L},$$

то решетка называется *дистрибутивной*. Так, например, дистрибутивной является, скажем, решетка (не имеющая нуля и единицы) всех целых чисел с естественным их упорядочением (рис. 32; заметьте, что здесь «решетчатые» сложение и умножение не имеют ничего общего с обычным сложением и умножением чисел: мы полагаем $a \oplus b = \max[a, b]$ и $a \otimes b = \min[a, b]$). В самом деле, легко видеть, что

$$a\otimes(b\oplus c) = \min[a, \max[b, c]] = \begin{cases} a, \text{ если } a \leqslant b \text{ или } a \leqslant c, \\ \max[b, c], \text{ если } a \geqslant b \text{ и } a \geqslant c \end{cases}$$

и также

$$(a\otimes b)\oplus(a\otimes c) = \max[\min[a, b], \min[a, c]] =$$

$$= \begin{cases} a, \text{ если } a \leqslant b \text{ или } a \leqslant c, \\ \max[b, c], \text{ если } a \geqslant b \text{ и } a \geqslant c. \end{cases}$$

Докажем теперь, что *во всякой дистрибутивной решетке выполняется второй дистрибутивный закон*:

$$(\lambda + \mu\nu = (\lambda + \mu)(\lambda + \nu). \qquad \text{(IIIб}$$

◀ Пусть аксиома P_7 выполняется, т. е. имеют место обычные правила раскрытия скобок. Тогда, в силу ассоциативности сложения и законов поглощения (VII),

$$(\lambda + \mu)(\lambda + \nu) = (\lambda + \mu)\lambda + (\lambda + \mu)\nu = \lambda + [(\lambda + \mu)\nu] =$$
$$= (\lambda + \lambda\nu) + \mu\nu = \lambda + \mu\nu \blacktriangleright.$$

Наконец, заметим, что в *дистрибутивной решетке с дополнениями дополнение* $\bar{\lambda}$ *элемента* λ *всегда единственно* — ведь приведенное на с. 42 доказательство этого же утверждения для булевой структуры опирается лишь на (выполняющиеся для дистрибутивных решеток с дополнениями!) коммутативность (Iб) умножения, свойства (IV) элементов ι и o и дистрибутивность (IIIa) (а также, разумеется, на определение (VIII) дополнения). А отсюда и из симметричности опре-

[1] Ясно, что вместо выполнения равенства (IIIa) можно было бы потребовать выполнения противоположного (9) неравенства $\lambda(\mu + \nu) \subset \lambda\mu + \lambda\nu$, из которого, совместно с (9), следует (IIIa).

деляющих дополнение равенств (VIII) уже следует, что операция взятия дополнения инволютивна:

$$\overline{\overline{\lambda}} = \lambda \quad \text{для всех} \quad \lambda \in \mathscr{L}. \tag{IX}$$

Далее, правила де Моргана

$$\text{а)}\ \overline{\lambda + \mu} = \overline{\lambda}\overline{\mu} \quad \text{и} \quad \text{б)}\ \overline{\lambda\mu} = \overline{\lambda} + \overline{\mu} \tag{XI}$$

также выполняются для таких решеток. ◀ Действительно, в силу ассоциативности сложения и умножения, свойств о и ι и дистрибутивных законов (III)

$$(\lambda + \mu) + \overline{\lambda}\,\overline{\mu} = \iota \quad \text{и} \quad (\lambda + \mu)\,(\overline{\lambda}\,\overline{\mu}) = o$$

(ср. с. 43) — откуда и вытекает правило (XIa). [Правило (XIб) может быть выведено из (XIa) и (IX) — см. с. 43.] ▶

Наконец, из единственности дополнения, определений (XVII) отношения $\supset$ и правил де Моргана (XI) вытекает соотношение (XXI) (см. с. 42).

Ясно, что аксиомы P_{1-7} выполняются в любой булевой структуре, т. е. что *булева структура* по присущему ей отношению $\supset$ *является дистрибутивной решеткой с дополнениями*. Но и обратно, как мы видели, для каждой дистрибутивной решетки с дополнениями выполняются все основные свойства (аксиомы) булевой структуры, так что *каждая дистрибутивная решетка с дополнениями одновременно является и булевой структурой*, в которой «булевы» сложение и умножение определяются равенствами (2′). Таким образом, аксиомы P_{1-7} дистрибутивной решетки с дополнениями можно рассматривать как еще один вариант аксиоматики булевой структуры.

Связь булевых структур с решетками может быть использована для исчерпывающего описания к о н е ч н ы х булевых структур, т. е. таких структур $\mathbf{B} = \langle \mathscr{B}; +, \cdot, ^{-}, \supset \rangle$, для которых множество $\mathscr{B}$ является *конечным*. Для того чтобы разобраться в том, как могут быть устроены такие булевы структуры, нам понадобятся некоторые новые понятия.

Условимся называть *атомами* решетки $\mathbf{L} = \langle \mathscr{L}; \supset \rangle$ с нулевым элементом о ее «элементы 1-го яруса», если считать, что «нулевой ярус» решетки составляет ее абсолютный минимум о; другими словами, атомы — это элементы, старшие одного лишь элемента о:

$$\alpha \text{ — атом, если } \alpha \neq o \text{ и из } \alpha \supset \beta \text{ следует } \beta = \alpha \text{ или } \beta = o. \tag{8.10}$$

[Это определение никак не фиксирует, существует ли в решетке $\mathbf{L}$ также и единичный элемент ι; является ли $\mathbf{L}$ решеткой с дополнениями; является ли она дистрибутивной или нет.] Так, например, атомами решетки (даже булевой структуры) подмножеств какого-либо универсального множества $I = \{x, y, z, \ldots\}$ являются его о д н о э л е м е н тные подмножества $\{x\}$, $\{y\}$, $\{z\}$, ... и т. д. (см. рис. 17, который здесь, безусловно, уместно вспомнить: на этом рисунке атомы — это множества $A_1 = \{a_1\}$, A_2, A_3 и A_4).

Единственным атомом решетки натуральных чисел с обычным отношением порядка (ср. с рис. 32) служит число *2* (нулем этой решетки служит число *1*); атомами изображенных на рис. 30 и 31, *а*, *б* решеток являются соответственно элементы α, β; μ, ν; π, ρ, σ этих решеток. При этом, вообще говоря, решетка может и вовсе не иметь атомов — не имеют, разумеется, атомов изображенные на рис. 29 и 32 решетки (у них нет нулевого элемента о); не имеет их также, например, решетка всех вещественных чисел x, где $0 \leqslant x \leqslant 1$, с естественным отношением порядка (нулем и единицей этой решетки служат числа 0 и 1). Однако если решетка имеет атомы α_1, α_2, α_3, ..., то

$$\alpha_i \alpha_j = \begin{cases} \alpha_i & \text{при } i = j \\ \mathrm{o} & \text{при } i \neq j \end{cases} \quad \text{для всех } i, j = 1, 2, 3, \ldots \tag{8.11}$$

— ведь $\alpha_i\alpha_j \subset \alpha_i$ и $\alpha_i\alpha_j \subset \alpha_j$, т. е. при $i \neq j$ произведение $\alpha_i\alpha_j$ является элементом нулевого яруса, или нулем нашей решетки.

Пусть теперь α — атом решетки $\mathbf{L}$; тогда про элемент $\lambda \supset \alpha$ этой решетки мы будем говорить, что он *произрастает* из атома α, а атом α назовем *корнем* элемента λ. Так, например, все ненулевые элементы изображенной на рис. 17 решетки произрастают из ее атомов A_1, A_2, A_3, A_4; вся (кроме нулевого элемента *1*) решетка натуральных чисел произрастает из единственного атома *2*; решетки рис. 30 и 31, *а*, *б* произрастают (в том же смысле) из множества атомов решетки, состоящего из двух и из трех элементов. Эта ситуация является достаточно типичной; она обусловливает следующее

Определение. Решетка $\mathbf{L} = \langle \mathscr{L}; \supset \rangle$ называется *атомарной*, если все ее ненулевые элементы имеют корни среди атомов этой решетки (если вся решетка произрастает из множества своих «атомов» в том смысле, в каком мы употребляли это выражение выше).

Так, схематически изображенные на рис. 17, 30, 31, *а*, *б* решетки все являются атомарными. Это обстоятельство отнюдь не является частным — оно является следствием следующего несложного факта:

Каждая конечная решетка (решетка $\mathbf{L} = \langle \mathscr{L}, \supset \rangle$, где множество $\mathscr{L}$ конечно) *с нулевым элементом* о *является атомарной*.

◀ В самом деле, пусть $\lambda \in \mathscr{L}$ — произвольный ненулевой элемент решетки. Если λ — атом, то он является своим собственным корнем; пусть теперь λ — не атом, т. е. существует такой элемент λ_1, что

$$\lambda_1 \subset \lambda, \quad \lambda_1 \neq \lambda \quad \text{и} \quad \lambda_1 \neq \mathrm{o}. \tag{8.12}$$

Введем временно (только для доказательства этого утверждения) отношение $>$ между элементами решетки:

$\lambda > \mu$, если $\lambda \supset \mu$ и $\lambda \neq \mu$;

это отношение очевидно,

антирефлексивно: ни для одного $\lambda \in \mathscr{L}$ не имеет место отношение $\lambda < \lambda$;

антисимметрично (в строгом смысле): нет таких $\lambda, \mu \in \mathscr{L}$, что $\lambda > \mu$ и $\mu > \lambda$;

транзитивно: если $\lambda > \mu$ и $\mu > \nu$, то $\lambda > \nu$.

Из (12) следует

$$\lambda > \lambda_1 \text{ (и } \lambda,\ \lambda_1 \neq o). \tag{8.13а}$$

Точно так же, если λ_1 — не атом, то существует $\lambda_2 \in \mathscr{L}$, где

$$\lambda_1 > \lambda_2 \text{ (и } \lambda_2 \neq o); \tag{8.13б}$$

если λ_2 — не атом, то существует $\lambda_3 \in \mathscr{L}$, где

$$\lambda_2 > \lambda_3 \text{ (и } \lambda_3 \neq o) \tag{8.13в}$$

и т. д. Таким образом, мы приходим к последовательности «строгих неравенств» (13, а, б, в, ...), которые в силу транзитивности отношения $>$ можно свести в одну цепочку:

$$\lambda > \lambda_1 > \lambda_2 > \lambda_3 > \ldots \text{(и все } \lambda,\ \lambda_1,\ \lambda_2,\ \lambda_3, \ldots \neq o). \tag{8.14}$$

Но так как в силу антирефлексивности и транзитивности отношения $>$ все элементы цепочки (14) различны, то в силу конечности числа элементов $\mathscr{L}$ эта цепочка не может быть бесконечной; следовательно, она кончается каким-либо атомом α — корнем элемента λ, т. е. все элементы решетки произрастают из ее корней. ▶

Для дальнейшего нам будет полезна также

Лемма. Если атом α дистрибутивной решетки $\mathbf{L}$ является корнем суммы $\lambda_1 + \lambda_2 + \ldots + \lambda_n$, то из α произрастает хотя бы один из элементов $\lambda_1, \lambda_2, \ldots, \lambda_n$.

◀ В самом деле, пусть α не является корнем ни одного из элементов $\lambda_1, \lambda_2, \ldots, \lambda_n$, т. е. не имеет места ни одно из неравенств $\lambda_i \supset \alpha$ или ни одно из равенств $\alpha\lambda_i = \alpha$, где $i = 1, 2, \ldots, n$. Но так как $\alpha\lambda_i \subset \alpha$, то по определению атома $\alpha\lambda_i = o$ для всех ι. А отсюда в силу дистрибутивного закона P_7 имеем

$$\alpha(\lambda_1 + \lambda_2 + \ldots + \lambda_n) = \alpha\lambda_1 + \alpha\lambda_2 + \ldots + \alpha\lambda_n = o + o + \ldots + o = o$$

(ср. упр. 13а)), что, однако, противоречит условию

$$\lambda_1 + \lambda_2 + \ldots + \lambda_n = \alpha \text{ (т. е. } \alpha(\lambda_1 + \lambda_2 + \ldots + \lambda_n) = \alpha\alpha = \alpha) \text{ ▶}$$

Следствие. Пусть $\mathbf{L}$ — дистрибутивная решетка с дополнениями (т. е. булева структура — вот тут, наконец, мы переходим от решеток к булевым структурам); тогда для любого элемента λ и любого атома α выполняется одно и только одно из неравенств

$$\lambda \supset \alpha \text{ и } \bar{\lambda} \supset \alpha \tag{8.15}$$

(т. е. из α произрастает один, и только один, элемент из каждой пары взаимно дополнительных элементов λ, $\bar{\lambda}$).

◀ Так как $\lambda + \bar{\lambda} = \iota \supset \alpha$, то α является корнем суммы $\lambda + \bar{\lambda}$, т. е. в силу нашей леммы корнем хоть одного из элементов λ и $\bar{\lambda}$. При этом быть одновременно корнем и λ и $\bar{\lambda}$ атом α не может: если выполняются оба неравенства (15), то в силу монотонности (XXб) умножения

$$o = \lambda\bar{\lambda} \supset \lambda\alpha \supset \alpha\alpha = \alpha,$$

что, однако, противоречит определению элемента o. ▶

Рассмотрим теперь конечную (и, следовательно, атомарную) булеву структуру $\mathbf{B} = \langle \mathcal{B}; +, \cdot, ^{-} \supset \rangle$ (дистрибутивную решетку $\mathbf{L} = \langle \mathcal{B}; \supset \rangle$ с дополнениями); число k атомов $\alpha_1, \alpha_2, \ldots, \alpha_k$ структуры $\mathbf{B}$ мы назовем ее *рангом*, а множество $A = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ — *корневым* множеством. Сопоставим каждому элементу $\lambda \in \mathcal{B}$ множество $A_\lambda = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}\}$ тех атомов, которые являются корнями λ:

$$\lambda \to A_\lambda = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}\}. \tag{8.16}$$

Ясно, что (16) есть отображение $\mathcal{B} \to \mathcal{A}$, где $\mathcal{A}$ — множество всех подмножеств множества A; при этом, очевидно, $A_\iota = A$ — это все множество A (ибо ι — абсолютный максимум решетки), а $A_o = O$, где O — пустое множество.

Имеет место следующая основная

Т е о р е м а. Отображение (16) взаимно-однозначно; оно является изоморфным отображением булевой структуры $\mathbf{B}$ на булеву структуру $\mathbf{A} = \langle \mathcal{A}; +, \cdot, ^{-}, \supset \rangle$ всевозможных подмножеств множества $\mathcal{A}$ (где операции над множествами определяются, как в гл. 1).

◀ Ясно, прежде всего, что (16) — это отображение $\mathcal{B}$ *на* $\mathcal{A}$, т. е. что в каждое подмножество $\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_q}\} \in \mathcal{A}$ отображается хоть один элемент из $\mathcal{B}$ — элемент

$$\lambda = \alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_q}. \tag{8.17}$$

В самом деле, разумеется, $\lambda \supset \alpha_{i_t}$, где $t = 1, 2, \ldots,$ или q. С другой стороны, если $\lambda \supset \alpha$, где $\alpha \in A$, то сумма (17) произрастает из α, откуда в силу Леммы следует, что α есть корень одного из элементов α_{i_t}. Но если $\alpha \neq \alpha_{i_t}$, то это противоречит определению атома: ведь если α_1 и α_2 — два р а з н ы х атома, то $\alpha_1\alpha_2 = o$ (см. (11)).

Далее, пусть λ и μ — два р а з н ы х элемента структуры; покажем, что $A_\lambda \neq A_\mu$. Так как $\lambda \neq \mu$ и отношение $\supset$ антисимметрично, то никак не могут иметь места сразу оба отношения $\lambda \supset \mu$ и $\mu \supset \lambda$; пусть, например, не выполняется первое из них. В таком случае $\bar{\lambda}\mu \neq o$ (ибо равенство $\bar{\lambda}\mu = o$ равносильно отношению $\lambda \supset \mu$ — см. с. 41). Так как наша структура атомарна, то элемент $\overline{\lambda\mu}$ произрастает из некоторого корня α, т. е. $\overline{\lambda\mu} \supset \alpha$. Но из неравенств

$$\bar{\lambda} \supset \overline{\lambda\mu} \supset \alpha \quad \text{и} \quad \mu \supset \overline{\lambda\mu} \supset \alpha$$

следует, что α есть корень элемента μ (т. е. $\alpha \in A_\mu$) и α есть корень $\bar{\lambda}$, т. е. α — не корень λ (см. следствие выше); таким образом, $\alpha \notin A_\lambda$. Поэтому при $\lambda \neq \mu$ также и $A_\lambda \neq A_\mu$, т. е. отображение (16) взаимнооднозначно.

Теперь мы можем записать (16) в виде явной формулы:

$$A_\lambda = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_q}\} \leftrightarrow \alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_q} = \lambda. \tag{8.16$'$}$$

Из (16′) прежде всего вытекает, что

$$\text{если } A_\lambda \supset A_\mu, \text{ то } \lambda \supset \mu$$

(где отношение $A_\lambda \supset A_\mu$ понимается в смысле алгебры множеств— см. гл. 1, а отношение $\lambda \supset \mu$ понимается в смысле структуры **B**); отсюда в силу взаимооднозначности отображения (16′) следует р а в н о с и л ь н о с т ь отношений $A_\lambda \supset A_\mu$ и $\lambda \supset \mu$. Далее,

$$\text{если } A_\lambda = A_\mu + A_\nu, \text{ то } \lambda = \mu + \nu. \tag{8.18а}$$

Затем из идемпотентного закона (VIб), равенства (11) (где положено $i \neq j$) и формулы (16′) получаем:

$$\text{если } A_\lambda = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_p}\} \leftrightarrow \alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_p} = \lambda$$

$$\text{и } A_\mu = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_q}\} \leftrightarrow \alpha_{j_1} + \alpha_{j_2} + \ldots + \alpha_{j_q} = \mu,$$

$$\text{то } A_\lambda A_\mu \leftrightarrow (\alpha_{i_1} + \ldots + \alpha_{i_p})(\alpha_{j_1} + \ldots + \alpha_{j_q}) = \lambda\mu. \tag{8.18б}$$

Наконец, так как, очевидно,

$$\alpha_1 + \alpha_2 + \ldots + \alpha_k = \iota \tag{8.19}$$

(ибо, как мы знаем, $A \leftrightarrow \iota$ в силу отображения (16)), то

$$\text{если } \bar{A}_\lambda = A_\mu, \text{ то } \lambda\mu = o$$

$$\text{и } \lambda + \mu = \alpha_1 + \alpha_2 + \ldots + \alpha_k = \iota, \text{ т. е. } \mu = \bar{\lambda}. \tag{8.18в}$$

Предложения (18а—в) и устанавливают, что отображение (16) — это изоморфизм. ▶

Итак, мы доказали, что каждая (конечная) булева структура $\mathbf{B}_k$ ранга k изоморфна алгебре $\mathbf{A}_k$ подмножеств (конечного) k-элементного множества; поэтому число ее элементов (называемое также *порядком* структуры) равно 2^k (см. упр. 1 ниже). Таким образом, порядок произвольной конечной булевой структуры обязательно является целой *степенью двойки*. При этом ранг (или порядок) конечной булевой структуры полностью эту структуру характеризует, подобно тому как, скажем, конечномерное векторное пространство полностью характеризуется своей размерностью: структура ранга k или порядка 2^k изоморфна алгебре подмножеств k-элементного множества[1].

Ясно, что 2^k элементов конечной структуры ранга k можно разбить на $k+1$ «ярусов», где i-й ярус образуют элементы структуры, отвечающие i-элементным подмножествам k-элементного множества A; при этом 0-й и k-й ярусы состоят из единственного элемента о и ι соответственно, а i-й ярус содержит C_k^i $(=k!/[i!\,(k-i)!])$ элементов булевой структуры (ср. рис. 17). При этом отношение $\supset$ может связывать лишь (различные) элементы разных ярусов, причем «большими» оказываются элементы старшего по номеру яруса; легко также видеть, что каждый элемент i-го яруса «больше» i (и только i) элементов $(i-1)$-го яруса и «меньше» $k-i$ (и только $k-i$) элементов $(i+1)$-го яруса. Однако эта наглядность и простота строения конечных булевых структур не переносится на случай б е с к о н е ч н ы х булевых структур. Правда, одна из основных теорем общей теории булевых структур (т е о р е м а С т о у н а; см. упр. 9.11 или, например, [2.19, 2.23, 3.1]) утверждает *возможность реализации каждой булевой структуры в виде системы подмножеств некоторого универсального множества I*. [Разумеется, эта система подмножеств должна образовывать так называемое *поле множеств*, т. е. включать универсальное множество I и пустое множество O и быть замкнутой относительно операций $+$ (объединение множеств), $\cdot$ (пересечение) и $\overline{}$ (образование дополнения множества).]

Однако, как нетрудно понять, (конечная или бесконечная) булева структура **B** в том и только в том случае изоморфна структуре в с е х подмножеств универсального множества I, если она является *атомарной*, что в силу существования неатомарных (бесконечных) булевых структур порождает определенную сложность классификации бесконечных структур.

Основная теорема об отображении (16′) кажется специфически «булевой» и далекой от всех привычных нам арифметических и алгебраических фактов и теорем; однако на самом деле она имеет глубокие (и, как мы увидим далее, неслучайные) аналогии в обычной арифметике. Условимся, прежде всего, называть элемент λ булевой структуры *аддитивно составным*, если он разбивается на сумму двух отличных от λ (и следовательно, «существенно меньших» λ, т. е. меньших λ и отличных от λ) слагаемых:

$$\lambda=\mu+\nu,\ \text{где}\ \mu\neq\lambda\ \text{и}\ \nu\neq\lambda \tag{8.20}$$

и (аддитивно) *простым*, если единственное разложение λ в сумму различных слагаемых имеет вид

$$\lambda=\lambda+o\ \text{или}\ \lambda=o+\lambda. \tag{8.21}$$

[1] Вот тут нам приходится считать, что пустое множество содержит единственное подмножество (одновременно — универсальное и пустое: ср. со сноской на с. 38) — случай пустого множества A приводит к 1-элементной структуре ранга 0 и порядка $2^0=1$.

[Ясно, что в булевой «арифметике без степеней и коэффициентов» не имеет смысла рассматривать разложение элементов на сумму одинаковых слагаемых и их разложение в произведение одинаковых множителей.] Простые элементы булевой структуры — это, очевидно, лишь ее *атомы*. В самом деле, из разложения $\lambda = \mu + \nu$ в силу (XVIа) вытекает, что $\lambda \supset \mu$ и $\lambda \supset \nu$; поэтому, если λ есть атом, то возможны лишь значения $\mu = \lambda$, о и $\nu = \lambda$, о. С другой стороны, если λ — не атом, то существует элемент $\mu \subset \lambda$, где $\mu \neq \lambda$ и $\mu \neq 0$; при этом за ν можно принять «прямую разность» $\lambda - \mu$ элементов λ и μ (см. с. 39) — тогда и $\nu \neq \lambda$.

Полученные выше результаты позволяют утверждать, что справедлива следующая

Теорема об однозначности разбиения на слагаемые. Каждая конечная булева структура **B** обладает конечным набором аддитивно простых элементов (*атомов*) $\alpha_1, \alpha_2, \ldots, \alpha_k$; при этом любой элемент структуры однозначно (с точностью до порядка слагаемых) разбивается на сумму простых слагаемых:

$$(\lambda = \alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_l} \tag{8.22a}$$

которая при $\lambda =$ о может и не содержать ни одного слагаемого).

Обратимся теперь к (присущему каждой булевой структуре) *принципу двойственности* (см. с. 45). В силу этого принципа аддитивно простым элементам (атомам) отвечают *мультипликативно простые* элементы булевой структуры, такие, что единственно возможным разложением λ в произведение различных множителей является разложение

$$\lambda = \lambda\iota = \iota\lambda; \tag{8.22б}$$

все же другие элементы, для которых возможно разложение

$\lambda = \mu\nu$, где μ, $\nu \neq \lambda$,

мы назовем (*мультипликативно*) *составными*. [В силу близости этой терминологии к принятой в элементарной арифметике, в дальнейшем прилагательное «мультипликативный» мы будем, как правило, опускать.] При этом справедлива следующая основная

Теорема об единственности разложения на простые множители. Каждая конечная булева структура обладает конечным набором (мультипликативно) простых элементов $\beta_1, \beta_2, \ldots, \beta_k$, причем любой элемент λ структуры однозначно (с точностью до порядка сомножителей) разлагается в произведение

$$\lambda = \beta_{i_1} \beta_{i_2} \ldots \beta_{i_p} \tag{8.22в}$$

простых множителей (при этом в разложения включаются «разложение» $\iota = \iota$ единичного элемента структуры, вовсе не имеющего простых множителей, и разложение $о = \beta_1\beta_2 \ldots \beta_k$).

Эта теорема родственна известной теореме об единственности разложения каждого натурального числа в произведение простых множителей, в силу своего значения ранее зачастую именовавшейся «основной теоремой арифметики» (об этой теореме см., например, [6]). На причинах, порождающих это сходство, мы остановимся ниже (см. с. 95).

Упражнения. 8.1. Докажите, что общее число подмножеств k-элементного множества I (включая сюда как пустое множество, так и все множество I) равно 2^k.

8.2. Докажите свойство (VIIб) решетчатых сложения и умножения.

8.3. Выведите из аксиом P'_{1-8} равенство (XVIб) (с. 69).

8.4. Докажите, что идемпотентные законы $P'_{5,6}$ могут быть выведены из аксиом P'_{1-4} и P'_{7-8}, так что в приведенной на с. 68 аксиоматике можно оставить лишь последние 6 аксиом, причем эти аксиомы являются уже *независимыми*.

8.5. Докажите, что

а) для каждой решетки $L = <\mathscr{L}; \supset>$ и любых $\lambda, \mu, \nu \in \mathscr{L}$

$\lambda + \mu\nu \subset (\lambda + \mu)(\lambda + \nu)$;

б) решетка L дистрибутивна тогда и только тогда, когда $(\lambda + \mu\nu \supset (\lambda + \mu)(\lambda + \nu)$ для любых $\lambda, \mu, \nu \in \mathscr{L}$

8.6. Докажите, что

а) для каждой решетки $L = <\mathscr{L}; \supset>$ и любых $\lambda, \mu, \nu, \pi \in \mathscr{L}$

$(\lambda + \mu)(\nu + \pi) \supset (\lambda\nu + \mu\pi)$;

б) для каждой решетки L и любых $\lambda, \mu, \nu \in \mathscr{L}$

$(\lambda + \mu)(\mu + \nu)(\nu + \lambda) \supset \lambda\mu + \mu\nu + \nu\lambda$;

в) решетка L дистрибутивна тогда и только тогдв, когда

$(\lambda + \mu)(\mu + \nu)(\nu + \lambda) = \lambda\mu + \mu\nu + \nu\lambda$

ср. с примером на с. 16).

8.7. Докажите, что решетка $L = <\mathscr{L}; \supset>$ в том и только в том случае является дистрибутивной, если L не содержит «подрешетки» $L_1 = <\mathscr{L}_1; \supset>$ (где $\mathscr{L}_1 \subset \mathscr{L}$ и отношение $\supset$ переносится на множество $\mathscr{L}_1$ с объемлющего его множества $\mathscr{L}$), изоморфной решетке рис. 31, *а* или решетке рис. 31, *б*.

8.8. Докажите, что если каждая подструктура $<\mathscr{L}_1; \supset>$ решетки $L = <\mathscr{L}; \supset>$ (здесь $\mathscr{L}_1 \subset \mathscr{L}$ и «порядок» $\supset$ перенесен на $\mathscr{L}_1$ с $\mathscr{L}$) является ее подрешеткой, то отношение $\supset$ устанавливает на $\mathscr{L}$ «полный» (или линейный) порядок.

8.9 Докажите, что

а) для каждой решетки $L = <\mathscr{L}; \supset>$ из $\lambda \supset \nu$ следует $\lambda(\mu + \nu) \supset (\lambda\mu) + \nu$;

б) решетка $L = <\mathscr{L}; \supset>$ дистрибутивна тогда и только тогда, когда для любых $\lambda, \mu, \nu \in \mathscr{L}$ имеет место неравенство $(\lambda\mu) + \nu \supset \lambda(\mu + \nu)$ (в силу а) обращающееся в равенство в случае $\lambda \supset \nu$).

8.10. Решетка $L = <\mathscr{L}; \supset>$ называется *модулярной*, если в ней из $\lambda \supset \nu$ следует $(\lambda\mu) + \nu = \lambda(\mu + \nu)$.

Докажите, что

а) решетка рис. 31, *б* является не дистрибутивной, но модулярной;

б) решетка рис. 31, *а* не является модулярной;

в) решетка $L = <\mathscr{L}; \supset>$ в том и только в том случае не является модулярной, если она содержит подрешетку, изоморфную решетке рис 31, *а*.

[В силу упр. 5 всякая дистрибутивная решетка является модулярной, так что условие модулярности слабее условия дистрибутивности.]

8.11. Сколько булевых подструктур имеет

а) конечная булева структура порядка 16 (см. рис. 17);

б) конечная булева структура ранга k?

8.12. Докажите, что атомарная булева структура конечна тогда и только тогда, когда число ее атомов конечно.

8.13. Перечислите (мультипликативно) простые элементы конечной булевой структуры

а) порядка 16 (см. рис. 17);

б) ранга k (задайте эти элементы их разложением (16')).

8.14. Докажите теорему о единственности разложения на простые множители, не обращаясь к принципу двойственности

8.15. Приведите пример

а) атомарной булевой структуры с бесконечным (скажем, счетным) множеством атомов;

б) неатомарной булевой структуры.

8.16. Докажите, что бесконечная булева структура всегда содержит бесконечное множество элементов, произведение каждых двух из которых равно нулевому элементу o.

9. БУЛЕВЫ СТРУКТУРЫ И КОЛЬЦА. ИДЕАЛЫ И ФАКТОР-СТРУКТУРЫ

Известно, что **кольцом** называется алгебраическая структура

$$\mathbf{K} = <\mathcal{K};\ +, \cdot>, \tag{9.1}$$

задаваемая следующей системой аксиом: множество $\mathcal{K} = \{\varkappa, \lambda, \mu, \ldots \ldots; o\}$ по отношению к операции сложения образует коммутативную группу, т. е. выполняются условия:

$K_1 : \varkappa + \lambda = \lambda + \varkappa$ (*коммутативность* сложения);

$K_2 : (\varkappa + \lambda) + \mu = \varkappa + (\lambda + \mu)$ (*ассоциативность* сложения);

$K_3 : \varkappa + o = \varkappa$;

K_4 : для каждого $\varkappa \in \mathcal{K}$ существует единственный элемент $-\varkappa \in \mathcal{K}$, такой, что

$\varkappa + (-\varkappa) = o$

(o называется *нулевым* элементом кольца, а $-\varkappa$ — элементом, *противоположным* $\varkappa$). Далее выполняются условия [1]

$K_5 : (\varkappa\lambda)\mu = \varkappa(\lambda\mu)$ (*ассоциативность* умножения);

$K_{6,6'}: \varkappa(\lambda + \mu) = \varkappa\lambda + \varkappa\mu;\ (\varkappa + \lambda)\mu = \varkappa\mu + \lambda\mu$ (дистрибутивность сложения относительно умножения).

Кольцо **K** называется *коммутативным*, если дополнительно выполняется аксиома

$K_7 : \varkappa\lambda = \lambda\varkappa$ (*коммутативность* умножения);

в этом случае, разумеется, из двух аксиом $K_{6,6'}$ достаточно оставить только одну. Наконец, кольцо **K** называется *кольцом с единицей*, или *унитальным* кольцом, если существует такой элемент $\iota \in \mathcal{K}$, что

$K_8 : \varkappa\iota = \iota\varkappa = \varkappa$ (ι есть *единица* кольца)

(см. например, [3] или [11, с. 82]; разумеется, во всех аксиомах элементы $\varkappa, \lambda, \mu \in \mathcal{K}$ произвольны).

---

[1] В настоящее время в разряд колец часто включаются и *неассоциативные* кольца, для которых не выполняется аксиома K_5; мы, однако, будем считать все кольца ассоциативными.

Пусть теперь

$$\mathbf{B} = <\mathscr{B};\ +,\ \cdot,\ \bar{\ },\ \supset> \tag{9.2}$$

— булева структура и

$$\alpha * \beta = \alpha\overline{\beta} + \overline{\alpha}\beta \tag{9.3}$$

— *симметрическая разность* элементов α и β (см. § 4 и с. 47). Перечислим свойства симметрической разности:

$CP_1 : \alpha * \beta = \beta * \alpha;$

$CP_2 : (\alpha * \beta) * \gamma = \alpha * (\beta * \gamma);$

$CP_3 : \alpha * o = \alpha;$

$CP_4 : \alpha * \alpha = o;$

$CP_5 : \alpha (\beta * \gamma) = \alpha\beta * \alpha\gamma.$

Если прибавить к свойствам CP_{1-5} симметрической разности еще известные свойства булева умножения:

$$(\alpha\beta)\gamma = \alpha(\beta\gamma); \tag{IIб}$$

$$\alpha\beta = \beta\alpha; \tag{Iб}$$

$$\alpha\iota = \alpha, \tag{IVб}$$

то мы придем к выводу, что *каждая булева структура* **B** *по отношению к операциям симметрического вычитания* $*$ (см. (3)) *и обычного* (булева) *умножения образует коммутативное унитальное кольцо*

$$\mathbf{K} = <\mathscr{B};\ *,\ \cdot > \tag{9.4}$$

(ср. аксиомы K_{1-8} и равенства CP_{1-5}, (IIб), (Iб) и (IVб)). При этом из сопоставления K_4 и CP_4 вытекает, что в рассматриваемом кольце каждый элемент *сам себе противоположен*:

$CP_4' : \dot{-}\alpha = \alpha$, т. е. $2\alpha = o$,

где противоположный (в «кольцевом» смысле) α элемент обозначен через $\dot{-}\alpha$, а через 2α, как обычно, обозначена (кольцевая) «сумма» $\alpha * \alpha$.

Кольцо (4) обладает дополнительным важным свойством *идемпотентности умножения*:

$K_9 : \alpha^2 = \alpha,$

где через α^2 обозначено произведение $\alpha \cdot \alpha$ (см. (VIб)). Вот еще некоторые факты, касающиеся булевой структуры (2) и порожденного ею кольца (4):

$$\alpha + \beta = \alpha * \beta * \alpha\beta; \tag{9.5}$$

$$\text{если } \alpha * \beta = o, \text{ то } \beta = \alpha; \tag{9.6}$$

$$\iota * \alpha = \bar{\alpha}; \tag{9.7}$$

$$\text{если } \alpha * \gamma = \beta * \gamma, \text{ то } \alpha = \beta; \tag{9.8}$$

$$\text{если } \alpha * \beta = \gamma, \text{ то } \alpha * \gamma = \beta, \tag{9.9}$$

откуда с учетом CP_1 и (5) также следует, что

$$\alpha * \bar{\alpha} = \iota. \tag{9.7'}$$

Связь свойства K_9 кольца **K** со свойствами булева умножения оправдывает следующее наименование.

Кольцо (1), обладающее свойством K_9, называется **булевым кольцом**. Таким образом, булево кольцо — это структура (1), для которой выполнены аксиомы $K_{1-6,6'}$ и K_9.

Т е о р е м а. Каждое булево кольцо коммутативно — в нем выполняется также и аксиома K_7. Далее, в булевом кольце обратным для любого элемента является сам этот элемент, т. е. это кольцо обладает свойством CP'_4 (а значит, и свойством, аналогичным (6)).

◀ Легче всего доказать тождество CP'_4. А именно: в виду K_9 и дистрибутивности $K_{6,6'}$ имеем

$$2\varkappa = \varkappa + \varkappa = (\varkappa + \varkappa)(\varkappa + \varkappa) = \varkappa^2 + \varkappa^2 + \varkappa^2 + \varkappa^2 =$$
$$= \varkappa + \varkappa + \varkappa + \varkappa = 2\varkappa + 2\varkappa. \tag{9.10}$$

Обозначим через $\dot{-}2\varkappa$ элемент кольца, противоположный $2\varkappa$, и прибавим к обеим частям (10) по $\dot{-}2\varkappa$. Мы получим (здесь, как, впрочем, и при выводе (10), используется ассоциативность K_2 сложения)

$$2\varkappa + (\dot{-}2\varkappa) = 2\varkappa + [2\varkappa + (\dot{-}2\varkappa)], \text{ т. е. } o = 2\varkappa. \tag{9.11}$$

Из (11) сразу следует родственное (6) свойство:

$$\text{если } \varkappa + \lambda = o, \text{ то } \varkappa + (\varkappa + \lambda) = \varkappa + o = \varkappa, \text{ т. е. } (\varkappa + \varkappa) + \lambda =$$
$$= \varkappa \text{ или } o + \lambda = \varkappa \text{ и } \lambda = \varkappa. \tag{9.6'}$$

Почти так же просто доказывается и коммутативность: в силу K_9 и дистрибутивности

$$\varkappa + \lambda = (\varkappa + \lambda)(\varkappa + \lambda) = \varkappa^2 + \varkappa\lambda + \lambda\varkappa + \lambda^2 = \varkappa + \varkappa\lambda + \lambda\varkappa + \lambda,$$

откуда, прибавляя к обеим частям равенства по $\varkappa + \lambda$, получаем

$$(\varkappa + \lambda) + (\varkappa + \lambda) = (\varkappa + \lambda) + (\varkappa + \lambda) + (\varkappa\lambda + \lambda\varkappa) \text{ или } o = o +$$
$$+ (\varkappa\lambda + \lambda\varkappa)$$

— и, значит, в силу (6′)

$K_7 : \varkappa\lambda = \lambda\varkappa$. ▶

Доказанная теорема подчеркивает близость понятий булева кольца и булевой структуры. На самом деле эта близость заходит даже еще дальше, ибо имеет место

Т е о р е м а. Пусть

$$\mathsf{K} = \langle \mathscr{K};\ *,\ \cdot \rangle \tag{9.12}$$

— унитальное булево кольцо с единицей ι (сложение в котором нам будет удобно обозначать через $*$). Определив дополнительно

$$\text{а) } \varkappa + \lambda = \varkappa * \lambda * (\varkappa\lambda) \quad \text{и} \quad \text{б) } \bar{\varkappa} = \iota * \varkappa, \tag{9.13}$$

мы придем к булевой структуре

$$\mathsf{B} = \langle \mathscr{K};\ +,\ \cdot,\ \bar{\ } \rangle. \tag{9.14}$$

[Ясно, что отношение $\supset$ можно и не включать в число основных отношений булевой структуры, а определить условиями (XVII) — см. с. 41.]

◀ Покажем, что из аксиом $К_{1-6,8'}$, $К_8$ и $К_9$ унитального булева кольца K и определений (13) вытекают аксиомы $Б_{1-8}$ булевой структуры. Коммутативность $Б_2$ умножения является, как мы знаем, непосредственным следствием «булевости» кольца K; отсюда и из симметричности определения (13а) вытекает и коммутативность $Б_1$ сложения (напомним, что в силу $К_1$ «кольцевое сложение» коммутативно). Роль нулевого и единичного элементов булевой структуры играют нуль o и единица ι кольца K; при этом булева аксиома $Б_6$ совпадает с кольцевой аксиомой $К_8$, а $Б_5$ следует из определения (13а):

$$o + \varkappa = o * \varkappa * (o\varkappa) = o * \varkappa * o = \varkappa.$$

Наконец, из определения (13б) без труда выводятся свойства $Б_7$ и $Б_8$: в силу $К_6$, $К_8$, $К_9$ и (11)

$$\varkappa\bar{\varkappa} = \varkappa(\iota * \varkappa) = \varkappa\iota * \varkappa\varkappa = \varkappa * \varkappa = o; \tag{9.15а}$$

аналогично в силу (13а), $К_1$, $К_2$, (15а) и $К_9$

$$\varkappa + \bar{\varkappa} = \varkappa + (\iota * \varkappa) = \varkappa * (\iota * \varkappa) * \varkappa(\iota * \varkappa) = (\varkappa * \varkappa) * \iota * (\varkappa\bar{\varkappa}) =$$
$$= o * \iota * o = \iota. \tag{9.15б}$$

Несколько более громоздко доказательство дистрибутивных законов $Б_3$, $Б_4$, но и оно не представляет никаких трудностей, кроме чисто технических. Начнем с более простого первого дистрибутивного закона. Мы имеем

$$\varkappa(\lambda + \mu) = \varkappa(\lambda * \mu * (\lambda\mu)) = \varkappa\lambda * (\varkappa\mu) * \varkappa(\lambda\mu) = \varkappa\lambda * (\varkappa\mu) * (\varkappa\lambda\mu). \tag{9.16}$$

С другой стороны,

$$\varkappa\lambda + \varkappa\mu = \varkappa\lambda * \varkappa\mu * [(\varkappa\lambda)(\varkappa\mu)] = (\varkappa\lambda) * (\varkappa\mu) * [(\varkappa\varkappa)(\lambda\mu)] =$$
$$= (\varkappa\lambda) * (\varkappa\mu) * (\varkappa\lambda\mu), \tag{9.16$'$}$$

— чем и устанавливается $Б_3$ (здесь используется коммутативность $К_7$ умножения в булевом кольце, ассоциативность $К_6$ и идемпотентность $К_9$). Далее,

$$\varkappa + \lambda\mu = \varkappa * (\lambda\mu) * (\varkappa\lambda\mu), \tag{9.17}$$

а в силу определения (13а), коммутативности K_7, умножения, первого дистрибутивного закона $Б_3$, идемпотентности K_9 умножения, правила (10), дистрибутивности K_6 умножения относительно кольцевого сложения, коммутативности K_1 и ассоциативности K_2 кольцевого сложения

$$\begin{aligned}(\varkappa+\lambda)(\varkappa+\mu) &= (\varkappa\varkappa)+(\varkappa\mu)+(\varkappa\lambda)+(\lambda\mu)=[\varkappa+(\varkappa\mu)]+[(\varkappa\lambda)+(\lambda u)] = \\ &= [\varkappa*(\varkappa\mu)*\varkappa(\varkappa\mu)]+[(\varkappa\lambda)*(\lambda\mu)*(\varkappa\lambda)(\lambda\mu)] = [\varkappa*(\varkappa\mu)*(\varkappa\mu)]+[(\varkappa\lambda)* \\ &*(\lambda\mu)*(\varkappa\lambda\mu)]=\varkappa+[(\varkappa\lambda)*(\lambda\mu)*(\varkappa\lambda\mu)]=\varkappa*[(\varkappa\lambda)*(\lambda\mu)*(\varkappa\lambda\mu)]*\varkappa[(\varkappa\lambda)* \\ &*(\lambda\mu)*(\varkappa\lambda\mu)]=\varkappa*(\varkappa\lambda)*(\lambda\mu)*(\varkappa\lambda\mu)*[(\varkappa\varkappa\lambda)*(\varkappa\lambda\mu)*(\varkappa\varkappa\lambda\mu)]=\varkappa*(\varkappa\lambda)* \\ &*(\lambda\mu)*(\varkappa\lambda\mu)*(\varkappa\lambda)*(\varkappa\lambda\mu)*(\varkappa\lambda\mu)=\varkappa*(\lambda\mu)+(\varkappa\lambda\mu)*[(\varkappa\lambda)*(\varkappa\lambda)]*[(\varkappa\lambda\mu)* \\ &*(\varkappa\lambda\mu)]=\varkappa*(\lambda\mu)*(\varkappa\lambda\mu)*o*o=\varkappa*(\lambda\mu)*(\varkappa\lambda\mu), \end{aligned}\tag{9.17'}$$

— что и завершает доказательство $Б_4$. ▶

Таким образом, с каждой булевой структурой **B** можно сопоставить унитальное булево кольцо **K** и, наоборот, от унитального булева кольца **K** можно перейти к булевой структуре **B**, что позволяет принять аксиомы $K_{1-6,6'}$, K_8 и K_9 унитального булева кольца за новую аксиоматику булевой структуры и рассматривать теорию булевых структур как главу теории колец (как учение об унитальных булевых кольцах). При этом «естественное» соответствие между булевыми структурами и булевыми кольцами является взаимным:

$$\mathbf{B} = \langle \mathscr{B};\ +,\ \cdot,\ \neg,\ \supset \rangle \leftrightarrow \mathbf{K} = \langle \mathscr{B};\ *,\ \cdot \rangle \tag{9.18}$$

в том смысле, что если перейти от булевой структуры **B** с помощью определения (3) к булевому кольцу **K**, то обратный переход (с помощью определений (13)) от **K** к булевой структуре **B** приведет нас к исходной структуре (см. ниже упр. 3).

В определении булева кольца мы не требовали коммутативности K_7 умножения, поскольку условие K_7 легко выводится из «булевости» K_9 кольца (из идемпотентности умножения). Но более того, также и коммутативность K_1 сложения можно не включать в число аксиом булева кольца, поскольку и она может быть выведена из условия K_9 (причем доказательство K_1 даже проще доказательства K_7). ◀ В самом деле, «нильпотентность сложения»

$$\varkappa + \varkappa = o \tag{9.11'}$$

выводится из K_9 без использования K_1. Далее, в силу (11″)

$$(\varkappa+\lambda)+(\varkappa+\lambda)=o \tag{9.19}$$

и по той же формуле (11′) с учетом ассоциативности K_2 сложения

$$(\varkappa+\lambda)+(\lambda+\varkappa)=\varkappa+(\lambda+\lambda)+\varkappa=(\varkappa+o)+\varkappa=\varkappa+\varkappa=o. \tag{9.19'}$$

Следовательно, и элемент $\varkappa+\lambda$, и элемент $\lambda+\varkappa$ являются противоположными для элемента $\varkappa+\lambda$ кольца, откуда, в силу единственности K_4 противоположного элемента, имеем

$K_1 : \varkappa+\lambda=\lambda+\varkappa.$

[Заметим, впрочем, что в аксиоме K_4 кольца достаточно требовать с у щ е с т в о в а н и я противоположного элемента, откуда уже с учетом других кольцевых аксиом выводится его е д и н с т в е н н о с т ь.] ▶

Таким образом, список аксиом булевой структуры можно также сократить до $K_{2-6,8'}$, K_8, и K_9.

Как известно (см., например, [3] или [(1I, с. 87—88 и 137]) *идеалом кольца* (12) называется такое подкольцо $J = <\mathcal{J}; *, \cdot>$ (где $\mathcal{J} \subset \mathcal{K}$, а действия сложения и умножения переносятся на $\mathcal{J}$ с $\mathcal{K}$), что произведение любого $\varkappa \in \mathcal{K}$ на элемент $\varkappa_1 \in \mathcal{J}$ также принадлежит $\mathcal{J}$. Эти условия можно записать в виде следующих двух правил: J есть идеал, если

из $\varkappa, \lambda \in \mathcal{J}$ следует $\varkappa \dot{-} \lambda \in \mathcal{J}$; (9.20а)

из $\varkappa \in \mathcal{K}$ и $\lambda \in \mathcal{J}$ следует $\varkappa\lambda \in \mathcal{J}$, (9.20б)

где под $\varkappa \dot{-} \lambda$ («кольцевая разность») понимается элемент $\varkappa * (\dot{-}\lambda)$. Аналогично под *идеалом булевой структуры* $B = <\mathcal{B}; +, \cdot, ^-, \supset>$ понимается подмножество $\mathcal{J}$ основного множества $\mathcal{B}$, замкнутое относительно (булева) сложения и такое, что произведение любого $\alpha \in \mathcal{B}$ на элемент $\alpha_1 \in \mathcal{J}$ также принадлежит $\mathcal{J}$. Другими словами, булев идеал $J = <\mathcal{J}; +, \cdot>$ (ведь множество $\mathcal{J} \subset \mathcal{B}$ «замкнуто» относительно сложения и относительно умножения) определяется родственными (20) условиями:

из $\varkappa, \lambda \in \mathcal{J}$ следует $\varkappa + \lambda \in \mathcal{J}$; (9.21а)

из $\varkappa \subset \mathcal{B}$ и $\lambda \in \mathcal{J}$ следует $\varkappa\lambda \in \mathcal{J}$. (9.21б)

Впрочем, нам даже нет необходимости определять специально «булевы идеалы», поскольку они в точности отвечают идеалам соответствующего (булева) кольца:

Теорема: Пусть $B = <\mathcal{B}; +, \cdot, ^-, \supset>$ — булева структура и $K = <\mathcal{B}; *, \quad>$ — отвечающее B булево кольцо (где «кольцевое сложение» $*$ определяется по формуле (3)). Тогда множество $\mathcal{J} \in \mathcal{B}$ в том и только в том случае представляет собой идеал структуры B, если оно является и («кольцевым») идеалом (булева) кольца K; другими словами, условия (20), (21) равносильны.

◀ Предположим сначала, что $J = <\mathcal{J}; +, \cdot>$ — булев идеал (идеал *булевой структуры* B). Заметим, что в случае *булева* кольца K условие (20а) в определении идеала может быть заменено на

из $\varkappa, \lambda \in \mathcal{J}$ следует $\varkappa * \lambda \in \mathcal{J}$, (9.20′а)

ибо в этом случае в силу (11) $\dot{-}\lambda = \lambda$. Пусть, далее, $\varkappa, \lambda \in \mathcal{J}$. Поскольку $\varkappa * \lambda = \varkappa\bar{\lambda} + \bar{\varkappa}\lambda$ и $\varkappa, \lambda \in \mathcal{J}$, то в силу (21б) $\bar{\varkappa}\lambda \in \mathcal{J}$ и $\varkappa\bar{\lambda} = \bar{\lambda}\varkappa \in \mathcal{J}$; поэтому в силу (21а) $\varkappa * \lambda \in \mathcal{J}$, т. е. условие (20′а) является следствием условий (21). С другой стороны, условия (20б) и (21б) просто совпадают, ибо «кольцевое» умножение совпадает с булевым. Таким образом, J является также и кольцевым идеалом булева кольца K.

Обратно, пусть $\mathcal{J} \subset \mathcal{B}$ идеал *кольца* K и пусть $\varkappa, \lambda \in \mathcal{J}$. Так как (см. (13а)) $\varkappa + \lambda = \varkappa * \lambda * (\varkappa\lambda)$ и так как по (20б) $\varkappa, \lambda, \varkappa\lambda \in \mathcal{J}$, то в силу (20′а) $\varkappa + \lambda \in \mathcal{J}$. А так как условие (21б) совпадает с (20б), то $\mathcal{J}$ есть также и булев идеал. ▶

Укажем еще, что условие (21б) в определении булева идеала можно заменить следующим:

из $\lambda \in \mathcal{J}$ и $\lambda \supset \varkappa$ следует, что и $\varkappa \in \mathcal{J}$. (9.21′б)

◀ Действительно, так как $\varkappa\lambda \subset \varkappa$ при любом $\varkappa$ (см. свойство (XVIб) булевых структур), то (21б) вытекает из (21′б). С другой стороны, поскольку при $\lambda \supset \varkappa$ элемент $\varkappa$ можно представить в виде $\lambda\varkappa$ (где $\lambda \in \mathcal{J}$, а про $\varkappa$ пока известно лишь, что $\varkappa \in \mathcal{B}$), то из (21б) вытекает (21′б). ▶

Примеры. Ясно, что один лишь нулевой элемент {o} и все множество $\mathcal{B}$ составляют идеалы любой булевой структуры $B = <\mathcal{B}; +, \cdot, ^-, \supset>$; все идеалы, отличные от этих двух «тривиальных» идеалов, называются *собственными*. В алгебре подмножеств данного универсального множества I семейство всех конечных подмножеств составляет идеал (собственный, если I бесконечно — см. упр. 9). Для любого элемента $\alpha \in \mathscr{B}$ множество J_α всех «меньших» α элементов:

$$J_\alpha = \{\beta \mid \beta \in \mathscr{B} \text{ и } \beta \subset \alpha\} \tag{9.22}$$

составляет идеал (в силу (XVa) и эквивалентности (21б) и (21′б)); этот идеал называется *главным идеалом, порожденным элементом* α (он является собственным, если $\alpha \neq o$ и $\alpha \neq \iota$).

Рассмотрим теперь произвольное *отношение эквивалентности* ∞ (см., например, [1.2, 1.5, 2.16] или [II, с. 54]) на множестве элементов булевой структуры $\mathbf{B} = \langle \mathscr{B}; +, \cdot, ^-, \supset \rangle$, «согласованное» с булевой структурой, т. е. такое, что

$Э_1$: $\alpha \infty \alpha$ (*рефлективность*);

$Э_2$: если $\alpha \infty \beta$, то $\beta \infty \alpha$ (*симметричность*);

$Э_3$: если $\alpha \infty \beta$ и $\beta \infty \gamma$, то $\alpha \infty \gamma$ (*транзитивность*);

$Э_4$: если $\alpha \infty \alpha_1$ и $\beta \infty \beta_1$, то $\alpha + \beta \infty \alpha_1 + \beta_1$;

$Э_5$: если $\alpha \infty \alpha_1$ и $\beta \infty \beta_1$, то $\alpha\beta \infty \alpha_1\beta_1$;

$Э_6$: если $\alpha \infty \alpha_1$, то $\bar{\alpha} \infty \bar{\beta}$;

$Э_7$: $\alpha \supset \beta$, $\alpha \infty \alpha_1$ и $\beta \infty \beta_1$, то $\alpha_1 \supset \beta_1$.

[Заметим прежде всего, что $Э_7$ следует из $Э_4$:

◀ если $\alpha \supset \beta$, т. е. $\alpha + \beta = \alpha$ и $\alpha \infty \alpha_1$, $\beta \infty \beta_1$, то в силу $Э_4$
$\alpha_1 + \beta_1 = \alpha_1$, т. е. $\alpha_1 \supset \beta_1$. ▶

Далее, $Э_5$ можно вывести из $Э_4$ и $Э_6$:

◀ если $\alpha \infty \alpha_1$ и $\beta \infty \beta_1$, то $\bar{\alpha} \infty \bar{\alpha}_1$ и $\bar{\beta} \infty \bar{\beta}_1$, а значит, $\bar{\alpha} + \bar{\beta} \infty \bar{\alpha}_1 + \bar{\beta}_1$ и
$\overline{\bar{\alpha} + \bar{\beta}} \infty \overline{\bar{\alpha}_1 + \bar{\beta}_1}$, т. е. $\alpha\beta \infty \alpha_1\beta_1$
(см. (7.2а)). ▶ Таким образом, из условий $Э_{4-7}$ согласованности отношения ∞ с булевой структурой достаточно сохранить лишь $Э_4$ и $Э_6$.]

Теорема. Пусть на булевой структуре $\mathbf{B} = \langle \mathscr{B}; +, \cdot, ^-, \supset \rangle$ задано отношение эквивалентности ∞, согласованное со структурой. Тогда множество

$$J = \{\alpha \mid \alpha \infty o\} \tag{9.23}$$

элементов структуры $\mathbf{B}$, эквивалентных нулевому элементу o, образует некоторый идеал, а отношение ∞ в терминах структуры $\mathbf{B}$ и идеала J можно определить так:

$\alpha \infty \beta$ тогда и только тогда, когда $\alpha \dot{-} \beta \in \mathscr{J}$ или, что равносильно,

$$\alpha * \beta \in \mathscr{J} \tag{9.24}$$

где под $\alpha \dot{-} \beta$, как обычно, понимается «кольцевая разность»: $\alpha \dot{-} \beta = \gamma$ означает, что $\alpha = \beta * \gamma$ (мы знаем, что при этом $\alpha \dot{-} \beta = \alpha * \beta$). [Отношение (24) называют *J-эквивалентностью*, или *сравнимостью по модулю J*, и записывают следующим образом: $\alpha \underset{J}{\infty} \beta$ или $\alpha \equiv \beta \pmod{J}$.]

◀ Если $\alpha \in J$ и $\beta \in J$, то в силу $\alpha \infty o$ и $\beta \infty o$ из $Э_4$ вытекает, что $\alpha + \beta \infty \infty o + o = o$, т. е. что $\alpha + \beta \in J$; это доказывает выполнимость свойства (21а) идеала. Далее, если $\alpha \in J$ и $\gamma \in \mathscr{B}$, то, поскольку $\alpha \infty o$ и $\gamma \infty \gamma$ (см. $Э_1$), по $Э_5$ имеем $\alpha\gamma \infty o\gamma = o$, т. е. $\alpha\gamma \in J$ что и доказывает (21б). Следовательно, J — идеал

Далее, если $\alpha \infty \beta$, то в силу $Э_{4-6}$ $\bar{\alpha} \infty \bar{\beta}$, $\alpha\bar{\beta} \infty \alpha\bar{\alpha} = o$ и $\bar{\alpha}\beta \infty \bar{\alpha}\alpha = o$, т. е. $\alpha * \beta = \alpha\bar{\beta} + \bar{\alpha}\beta \infty o + o = o$, а значит, если $\alpha \infty \beta$, то $\alpha * \beta \infty 0$, т. е. $\alpha * \beta \in J$. Обратно, если $\alpha * \beta \in J$, то

$$\alpha\bar{\beta} + \bar{\alpha}\beta \infty o; \tag{9.25}$$

умножая обе части (25) на α и на β, получаем, используя $Э_{4-6}$ и $Э_{2-3}$:

$$\alpha\alpha\bar{\beta}+\alpha\bar{\alpha}\beta \sim \alpha o, \text{ т. е. } \alpha\bar{\beta}+o\sim o \text{ или } \alpha\bar{\beta}\sim o \text{ и } \bar{\alpha}\beta\sim o, \text{ а значит } \alpha\bar{\beta}\sim\bar{\alpha}\beta \quad (9.25')$$

Наконец, прибавив к обеим частям (25′) по $\alpha\beta$ и воспользовавшись $Э_1$ (эквивалентностью $\alpha\beta \sim \alpha\beta$), дистрибутивностью (IIIа), законами (VIIIа) и (IVб), получим:

$$\alpha\bar{\beta}+\alpha\beta\sim\bar{\alpha}\beta+\alpha\beta, \text{ т. е. } \alpha(\bar{\beta}+\beta)\sim(\bar{\alpha}+\alpha)\beta, \quad (9.26)$$

или $\alpha\iota\sim\iota\beta$, что равносильно $\alpha\sim\beta$. ▶

Таким образом, мы видим, что полный перечень всех отношений эквивалентности, которые можно задать на множестве $\mathcal{B}$ так, чтобы они были согласованы с булевой структурой $\mathbf{B} = \langle\mathcal{B};\ +,\ \cdot,\ ^{-},\ \supset\rangle$, доставляется списком всех идеалов структуры (с чем, кстати сказать, и связана, в первую очередь, важность понятия идеала): каждому идеалу J отвечает отношение (24) эквивалентности и каждому согласованному со структурой отношению $\sim$ эквивалентности отвечает идеал (23), причем эта связь идеалов с отношениями эквивалентности является взаимно однозначной.

Пусть теперь $\mathbf{B} = \langle\mathcal{B};\ +\ \cdot\ ^{-}\ \supset\rangle$ — булева структура и $\underset{J}{\sim}$ — отношение J-эквивалентности, разбивающее множество $\mathcal{B}$ на классы J-эквивалентных элементов; множество этих классов называется *фактор-множеством* множества $\mathcal{B}$ по отношению эквивалентности $\underset{J}{\sim}$ и обозначается через $\mathcal{B}/\underset{J}{\sim}$, или короче, через $\mathcal{B}/J$. Условимся обозначать через $\{\alpha\}, \{\beta\}, \ldots$ и т. д. классы эквивалентности, содержащие элементы $\alpha, \beta, \ldots$, и т. д., и определим:

$$\{\alpha\} + \{\beta\} = \{\alpha + \beta\};\ \{\alpha\}\cdot\{\beta\} = \{\alpha\beta\};$$
$$\overline{\{\alpha\}} = \{\bar{\alpha}\};\ \{\alpha\} \supset \{\beta\}, \text{ если } \alpha \supset \beta \quad (9.27)$$

[Все эти определения «корректны», т. е. не зависят от выборов представителей в классах эквивалентности. В самом деле, если $\{\alpha\} = \{\alpha_1\}$, т. е. $\alpha \sim \alpha_1$ и $\{\beta\} = \{\beta_1\}$, т. е. $\beta \sim \beta_1$, то $\alpha + \beta \sim \alpha_1 + \beta_1$, т. е. $\{\alpha + \beta\} = \{\alpha_1 + \beta_1\}$ и т. д.] Множество $\mathcal{B}/J$ классов эквивалентности относительно операций и отношения (27) само является булевой структурой, нулевым элементом которой является класс $\{o\}$ (т. е. идеал J), а единичным — класс $\{\iota\}$ (почему?). Эта структура обозначается через $\mathbf{B}/J$:

$$\mathbf{B}/_J = \langle\mathcal{B}/_J;\ +,\ \cdot,\ ^{-}\ \supset\rangle$$

и называется *фактор-структурой* структуры $\mathbf{B}$ по идеалу J.

Примеры. Ясно, что фактор-структура $\mathbf{B}/\{o\}$, где $\{o\}$ — нулевой идеал структуры $\mathbf{B}$, просто совпадает со структурой $\mathbf{B}$, поскольку в этом случае каждый класс $\{\alpha\}$ состоит из единственного элемента α. Аналогично фактор-структура $\mathbf{B}/\mathcal{B}$ представляет собой «тривиальную» булеву структуру, состоящую из одного элемента; эти два случая фактор-структур, разумеется, интереса не представляют. Больший интерес представляет фактор-структура $\mathbf{B}_{\alpha_0} = \mathbf{B}/J_{\alpha_0}$, где J_{α_0} — г л а в н ы й идеал, порожденный фиксированным элементом $\alpha_0 \neq o, \iota$ булевой структуры (см. с. 87). В этом случае класс $|\alpha| = \alpha * J_{\alpha_0}$, состоящий из всех элементов $\alpha * \beta$, где $\beta \subset \alpha_0$, содержит единственный элемент $\beta_0 \subset \alpha_0$ (почему?), так что основное множество фактор-структуры $\mathbf{B}_{\alpha}$ можно отождествить с идеалом $J_{\alpha_0} = \{\alpha \mid \alpha \in \mathcal{B} \text{ и } \alpha \subset \alpha_0\}$; при этом операции $+, \cdot$ и отношение $\supset$ определяются в этом множестве как обычно, под $\bar{\beta}$ понимается «дополнение β до α_0», т. е. элемент $\alpha_0\setminus\beta$ или $\alpha_0 - \beta$ (см. с. 39); роль элементов o и ι играют тот же элемент o и элемент α_0 (докажите это).

Упражнения. 9.1. Будет ли кольцевое сложение $*$ в произвольной булевой структуре

а) дистрибутивным относительно умножения (т. е. всегда ли $\alpha * (\beta\gamma) = (\alpha * \beta)(\alpha * \gamma)$);

б) монотонным (т. е. следует ли отношение $\alpha * \gamma \supset \beta * \gamma$ из того, что $\alpha \supset \beta$)?

9.2. Выразите «кольцевое вычитание» $\dot{-}$ в произвольной булевой структуре $B = <\mathscr{B}; +, \cdot, ^-, \supset>$ через основные операции этой структуры (т. е. запишите «кольцевую разность» $\alpha \dot{-} \beta$ в виде «булева многочлена» от переменных α и β — ср. § 6). Перечислите свойства операции $\dot{-}$.

9.3. Докажите взаимный характер соответствия (18) между булевыми структурами и булевыми кольцами (инволютивный характер отображения, переводящего булеву структуру в кольцо и обратно); другими словами, покажите, что если $\mathbf{B}(\mathbf{K})$ — построенная с помощью определений (13) по булеву кольцу $\mathbf{K}$ булева структура, а $\mathbf{K}(\mathbf{B})$, напротив, булево кольцо, отвечающее данной булевой структуре $\mathbf{B}$, то $\mathbf{B}(\mathbf{K}(\mathbf{B})) = \mathbf{B}$ и $\mathbf{K}(\mathbf{B}(\mathbf{K})) = \mathbf{K}$.

9.4. Пусть $\mathbf{K} = <\mathscr{K}; +, \cdot>$ — унитальное коммутативное кольцо и $\mathscr{K}_1 \in \mathscr{K}$ — множество идемпотентных элементов $\varkappa$ этого кольца (таких, что $\varkappa^2 = \varkappa$; ясно, что $\iota \in \mathscr{K}_1$, где ι — единица кольца). Докажите, что $\mathbf{K}_1 = <\mathscr{K}_1; *, \cdot>$, где $\varkappa * \lambda = \varkappa + \lambda \dot{-} 2\varkappa\lambda$ (здесь знак $\dot{-}$ означает «кольцевое вычитание») — булево кольцо; опишите операции отвечающей $\mathbf{K}_1$ булевой структуры $\mathbf{B}(\mathbf{K}_1) = \mathbf{B}(\mathbf{K})$ (ср. упр. 3) в терминах исходного кольца $\mathbf{K}$.

9.5. Докажите, что непустое подмножество J «основного множества» $\mathscr{B}$ булевой структуры $\mathbf{B} = <\mathscr{B}; +, \cdot, ^-, \supset>$ в том и только в том случае образует идеал этой структуры, если $\alpha\beta \in J$ тогда и только тогда, когда либо $\alpha \in J$, либо $\beta \in J$ (либо и $\alpha \in J$, и $\beta \in J$).

9.6. Докажите, что J-эквивалентность $\underset{J}{\infty}$ элементов булевой структуры (см. с. 87) можно определить так: $\alpha \underset{J}{\infty} \beta$ в том и только в том случае, когда $\alpha + \gamma = \beta + \gamma$ для некоторого $\gamma \in J$.

9.7. Докажите, что

а) как пересечение $J_1 \cap J_2$ двух идеалов J_1 и J_2 булевой структуры, так и их «прямая сумма» $J_1 \oplus J_2$ — множество всех элементов вида $\alpha_1 + \alpha_2$, где α_1 и α_2 принадлежат соответственно первому и второму идеалу:

$$J_1 \oplus J_2 = \{\alpha_1 + \alpha_2 \mid \alpha_1 \in J_1, \ \alpha_2 \in J_2\}$$

— тоже являются идеалами;

б) множество идеалов образует решетку по отношению к операциям $\oplus$ как решетчатому сложению и $\cap$ как решетчатому умножению. Каковы свойства этой решетки? Может ли она обращаться в булеву структуру (дистрибутивную решетку с дополнениями)?

9.8. а) Собственный идеал J булевой структуры $\mathbf{B}$ называется *максимальным*, если он не содержится ни в одном другом собственном идеале $\mathbf{B}$. Докажите, что идеал J является максимальным в том и только в том случае, когда из к а ж д о й пары элементов α и $\bar{\alpha}$ один (и только один) принадлежит J.

б) Собственный идеал J называется *простым*, если из того, что α и β не принадлежат J следует, что J не принадлежит и их сумма $\alpha + \beta$. Докажите, что идеал является простым в том и только в том случае, если он является максимальным.

в) Докажите, что главный идеал J_α булевой алгебры $\mathbf{B}$ является максимальным (а значит, и простым) в том и только в том случае, если α — атом.

г) Докажите, что фактор-структура $\mathbf{B}/J$ в том и только в том случае является булевой структурой из двух элементов, если идеал J является максимальным.

9.9. Пусть $\mathbf{B}$ — структура всевозможных подмножеств бесконечного множества I; докажите, что множество всех конечных подмножеств I образует идеал этой булевой структуры.

9.10. *Гомоморфным* отображением (гомоморфизмом) булевой структуры $\mathbf{B}_1 = <\mathscr{B}_1; +, \cdot, ^-, \supset>$ на булеву структуру $\mathbf{B}_2 = <\mathscr{B}_2; +, \cdot, ^-, \supset>$ называется отображение $\varphi: \mathscr{B}_1 \to \mathscr{B}_2$, при котором, скажем, из $\alpha_1 + \beta_1 = \gamma_1$, $\alpha_1, \beta_1, \gamma_1 \in \mathscr{B}_1$ и $\varphi(\alpha_1) = \alpha_2$, $\varphi(\beta_1) = \beta_2$, $\varphi(\gamma_1) = \gamma_2$ следует $\alpha_2 + \beta_2 = \gamma_2$ (где сложение понимается уже в смысле структуры $\mathbf{B}_2$) и в аналогичном смысле φ переносит с $\mathscr{B}_1$ на $\mathscr{B}_2$ операции $\cdot$, $^-$ и отношение $\supset$. [Примером — и притом в определенном смысле чуть ли не единственным (см ниже упр. б) — гомоморфного отображения булевой структуры $\mathbf{B} = <\mathscr{B}; +, \cdot, ^-, \supset>$ в фактор-структуру $\mathbf{B}/J$ может служить естественное отображение $\mathbf{B} \to \mathbf{B}/J$, переводящее каждый элемент $\alpha \in \mathscr{B}$ в элемент $[\alpha] \in \mathscr{B}/J$ — см. с. 88.] Докажите, что

а) $\varphi(o_1) = o_2$ и $\varphi(\iota_1) = \iota_2$, где o_1 и ι_1 — соответственно нулевой и единичный элементы структур $\mathbf{B}_1$ и $\mathbf{B}_2$.

б) Ядро J гомоморфизма, т. е. множество $\{\alpha_1 \mid \alpha_1 \in \mathscr{B}_1 \text{ и } \varphi(\alpha_1) = o_2\}$ является некоторым идеалом J структуры $\mathbf{B}_1$ и $\mathbf{B}_2$ изоморфно $\mathbf{B}_1/J$

9.11 (теорема Стоуна). Пусть $\mathbf{B} = <\mathscr{B}; +, \cdot, ^-, \supset>$ — произвольная булева структура и $I = \{J\}$ — множество всех ее максимальных идеалов. Сопоставим каждому элементу $\alpha \in \mathscr{B}$ подмножество $A_\alpha \subset I$, состоящее из всех максимальных идеалов, не содержащих элемента α:

$$\alpha \in \mathscr{B} \longleftrightarrow A_\alpha = \{J \mid J \in I \text{ и } J \not\ni \alpha\}. \qquad (*)$$

Докажите, что отображение (*) устанавливает изоморфизм структуры $\mathbf{B}$ и структуры подмножеств A_α множества I, понимаемой в смысле гл. 1. [Разумеется, совокупность подмножеств A_α, вообще говоря, не будет совпадать с совокупностью всех без исключения подмножеств I; впрочем, если множество $\mathscr{B}$ конечно, то последнее утверждение справедливо.]

Глава 3

МОДЕЛИ БУЛЕВЫХ СТРУКТУР

10. ПЕРВЫЕ МОДЕЛИ

До сих пор мы имели единственную модель булевой структуры доказывающую непротиворечивость соответствующей аксиоматики, — реализацию булевой структуры

$$\mathbf{B} = <\mathscr{B}; +, \cdot, ^-, \supset> \qquad (10.1)$$

в виде системы подмножеств $\{A, B, C, \ldots\}$ некоторого универсального множества I, где сложение и умножение множеств определяется как их *объединение* и *пересечение*, операция «черта» вводится как образование *дополнения* множества, а отношение $\supset$ имеет смысл *включения* множеств. Эта модель имеет универсальный характер в том смысле, что любая булева структура (где выражение «любая» подчеркивает неполноту аксиоматики, т. е. наличие ряда неизоморфных булевых структур) может быть представлена в виде «алгебры множеств» (ср. с. 78), — но она, разумеется, отнюдь не является единственно возможной. В этой главе мы укажем ряд других реализаций булевых структур, причем богатство и разнообразие, а также важность рассматриваемых моделей (см., в частности, § 11 и 12) вполне оправдывают большое внимание, уделяемое сегодня этому своеобразному типу математических структур.

1. *Булева арифметика двух чисел.* Мы уже неоднократно встречались выше с простейшей нетривиальной (содержащей больше одного элемента) булевой структурой — структурой, задаваемой на множестве из двух элементов: нулевого элемента о и единичного элемента ι. При рассмотрении этой «арифметики двух чисел» обычно обозначают нулевой элемент цифрой 0, а единичный — цифрой 1 (помня, разумеется, что эти символы имеют здесь смысл, несколько отличный от того, который придается им в школе и в обыденной жизни). Итак, мы имеем структуру

$$\mathbf{B} = <\{0, 1\};\ +, \cdot, \bar{\ }, \supset>, \qquad (10.1')$$

где сложение и умножение чисел задаются следующими «таблицей сложения» и «таблицей умножения»:

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

Если еще положить

$\bar{0} = 1,\ \bar{1} = 0$

и определить отношение $\supset$ при помощи следующей таблицы:

$0 \supset 0,\ 1 \supset 0,\ 1 \supset 1,$

то мы получим (простейший и притом — очень важный!) пример булевой структуры.

2. *Булева арифметика четырех чисел.* Из доказанного в § 8 следует, что простейшая после рассмотренной выше булева структура будет содержать четыре элемента. Итак, рассмотрим множество из четырех элементов («чисел») 0, 1, a, b и структуру

$$<\{0, 1, a, b\};\ +, \cdot, \bar{\ }, \supset>, \qquad (10.1'')$$

где действия сложения и умножения определяются следующими таблицами:

+	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

Операция $^{-}$ определяется в этой «арифметике» следующим образом:

$$\bar{0} = 1, \ \bar{a} = b, \ \bar{b} = a, \ \bar{1} = 0,$$

а отношение $\supset$ задается выписанной ниже таблицей, в которой звездочкой отмечены пары элементов (первый из них указывается строкой таблицы, а второй — столбцом), связанные отношением $\supset$:

$\supset$	0	a	b	1
0	*			
a	*	*		
b	*		*	
1	*	*	*	*

(так, например, из таблицы следует, что $1 \supset b$, но что отношение $a \supset b$ места не имеет, ибо на месте, отвечающем строке 1 и столбцу b, стоит звездочка, а на строке a в том же столбце звездочки нет). Роль элементов о и ι этой булевой структуры по-прежнему играют «числа» 0 и 1.

3. *Арифметика наибольших кратных и наименьших делителей.* В качестве следующего примера рассмотрим множество всевозможных делителей некоторого «свободного от квадратов» (немецкое quadratenfrei) натурального числа N, т. е. такого числа, которое представляет собой произведение ряда р а з л и ч н ы х простых множителей. Так, при $N = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ рассматриваемое множество состоит из чисел

1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 и 210.

«Сложение» и «умножение» этих чисел определим отличным от привычного образом; для того чтобы подчеркнуть это различие, будем обозначать «булеву сумму» чисел a и b через $a \oplus b$, а их «булево произведение» через $a \otimes b$. А именно, под «суммой»

$$a \oplus b = \text{НОК}\,(a, b) = [a, b] \tag{10.2а}$$

двух чисел a и b нашей системы мы будем понимать их *наименьшее общее кратное*, а под «произведением»

$$a \otimes b = \text{НОД}\,(a, b) = (a, b) \tag{10.2б}$$

— *наибольший общий делитель* этих чисел (обозначения $[a, b]$ для наименьшего кратного и (a, b) для наибольшего делителя употребляются иногда в арифметике и в теории чисел). Например,

$$10 \oplus 15 = [10, 15] = 30; \quad 10 \otimes 15 = (10, 15) = 5.$$

Определенные таким образом «сложение» и «умножение» чисел нашей системы коммутативны. Они также и ассоциативны, ибо

$$[[a, b], c] = [a, [b, c]] = [a, b, c] \text{ и } ((a, b), c) = (a, (b, c)) = (a, b, c),$$

где через $[a, b, c]$ и (a, b, c) обозначены наименьшее кратное и наибольший делитель т р е х чисел a, b и c. Выполняются в нашей «арифметике» и идемпотентные законы (VI):

$$a \oplus a = [a, a] = a \text{ и } a \otimes a = (a, a) = a,$$

а также законы поглощения (VII) (почему?). Далее ясно, что при сделанных соглашениях

$$a \oplus 1 = [a, 1] = a \text{ и } a \otimes N = (a, N) = a,$$

$$a \oplus N = [a, N] = N \text{ и } a \otimes 1 = (a, 1) = 1$$

(напоминаем, что все рассматриваемые числа являются делителями числа N) Таким образом, роль элементов ι и o здесь играют числа N и 1.

Несколько сложнее доказываются дистрибутивные законы (III). Выражение

$$(a \oplus b) \otimes c = ([a, b], c) \tag{10.3}$$

представляет собой НОД c и числа НОК(a, b); оно содержит те и только те простые множители, которые входят в состав c и одновременно в состав х о т я б ы о д н о г о из чисел a и b. Но ясно, что все эти (и только эти!) простые множители входят также и в состав числа

$$[(a, c), (b, c)] = (a \otimes c) \oplus (b \otimes c), \tag{10.3$'$}$$

что и доказывает равенство выражений (3) и (3′). Аналогично проверяется, что

$$(a \otimes b) \oplus c = (a \oplus c) \otimes (b \oplus c), \quad \text{т. е.}$$

$$[(a, b), c] = ([a, c], [b, c]).$$

Условимся теперь считать, что

$$a \supset b, \text{ если } b \text{ есть } \textit{делитель} \text{ числа } a. \tag{10.4}$$

При этом очевидным образом будут выполняться правила (XII), (XIII), (XIV), а также правила (XV) ($N \supset a \supset 1$), (XVI) ($[a, b] \supset \supset a \supset (a, b)$) и (XVII) (если a делится на b, то $[a, b] = a$, $(a, b) = b$). Правило (XVIII) есть прямое следствие определения (4) и того, что $a \oplus b$ — это н а и м е н ь ш е е общее кратное a и b, а $a \otimes b$ — н а и б о л ь ш и й общий делитель.

Из этих определений вытекают и очень близкие к (XVIII) правила (XIX) (если a делится как на b, так и на c, то a делится на $[a, c]$, если как a, так и b делятся на c, то и (a, b) делится на c), а также (XX) (почему?).

Наконец, положим

$$\bar{a} = N/a, \tag{10.5}$$

откуда сразу вытекает, что в соответствии с законами (IX), (X), (VIII) и (XXI)

$$\bar{\bar{a}} = a;\ \bar{1} = N;\ \bar{N} = 1;\ [a, N/a] = N;\ (a, N/a) = 1$$

(ведь N — число, «свободное от квадратов», и потому a и N/a — взаимно простые числа) и что если $a \supset b$, то $\bar{b} \supset \bar{a}$ (т. е. если a делится на b, то N/b делится на N/a). Несложно проверяются также правила де Моргана (XI):

$$\overline{a \oplus b} = \bar{a} \otimes \bar{b} \quad (\text{т. е. } N/[a, b] = (N/a,\ N/b))$$

и

$$\overline{a \otimes b} = \bar{a} \oplus \bar{b} \quad (N/(a, b) = [N/a,\ N/b])$$

Таким образом, наша система чисел относительно определенных выше операций «сложение» и «умножение», «черта» и отношения $\supset$ представляет собой булеву структуру.

Построенная в этом примере «алгебра делителей числа N» играет заметную роль в теории чисел.

Заметим в заключение, что установить выполнимость всех аксиом булевой структуры здесь можно и не прибегая к непосредственной их проверке. В силу условия о том, что число N разлагается в произведение ряда р а з л и ч н ы х простых чисел $p_1, p_2, p_3, \ldots, p_k$, каждый делитель a числа N характеризуется каким-то набором простых делителей $p_{i_1}, p_{i_2}, \ldots, p_{i_m}$ из числа исходных k простых чисел.

$$a = p_{i_1} p_{i_2} \ldots p_{i_m}.$$

Множество $\{p_{i_1}, p_{i_2}, \ldots, p_{i_m}\}$ простых делителей числа a обозначим через A, а множество $\{p_{j_1}, p_{j_2}, \ldots, p_{j_l}\}$ простых делителей числа b — через B. В таком случае числа $a \oplus b = [a, b]$ и $a \otimes b = (a, b)$ характеризуются множествами $A + B$ и AB простых делителей, где $A + B$ и AB — *объединение* и *пересечение* множеств A и B простых чисел. Далее, число a делится на число b, если $A \supset B$ (т. е. A содержит B); число N/a характеризуется множеством $\bar{A}$ простых делителей — *дополнением* множества A делителей a, где $I = \{p_1, p_2, \ldots, p_k\}$ — множество в с е х делителей числа N. Сказанное позволяет свести рассмотренную здесь структуру Буля к уже изученной алгебре подмножеств универсального множества I.

Более того, сведение нашей арифметики делителей свободного от квадратов числа N к алгебре подмножеств k-элементного множества $I = \{p_1, p_2, \ldots, p_k\}$ доказывает универсальный характер этой модели булевой структуры, пригодной для описания л ю б о й конечной структуры: для того чтобы прийти к конечной булевой структуре ранга k, достаточно предположить, что число N разлагается в произведение k различных простых множителей. «Обратим» теперь нашу модель по принципу двойственности, назвав НОК $(a, b) = [a, b]$ «булевым произведением» чисел a и b, а НОД $(a, b) = (a, b)$ — «булевой суммой» этих чисел; тогда придется считать, что число 1 играет роль «единицы» булевой структуры, а число N — роль ее «нуля» и что отношение $a \supset b$ имеет смысл «a является делителем b» (в теории чисел это отношение записывается как $a|b$, где вертикальную черту, разумеется, не следует путать с символом операции Шеффера). При этом простые делители $p_1, p_2, \ldots, p_k$ числа N будут играть роль (мультипликативно) простых элементов булевой структуры и сформулированная на с. 79 теорема об однозначности разложения на простые множители обратится в «основную теорему арифметики» (ср. [6]) (разумеется, эта теорема применяется здесь к делителям числа N).

Ясно, что в рамках модели 3 могут быть определены все понятия, имеющие смысл для общих булевых структур. Так, например, «разность» $a \setminus b$ чисел a и b вводится так:

$$a \setminus b = a/(a, b); \tag{10.6}$$

это число представляет собой, так сказать, «наибольшую взаимно простую с b часть a» — оно является произведением всех тех делителей a, которые **не являются** делителями b. «Симметрическая разность»

$$a * b = (a,\ N/b) \cdot (N/a,\ b) \tag{10.6$'$}$$

чисел a и b представляет собой произведение наибольших общих делителей чисел a N/b, и чисел, N/a; b так, например, считая по-прежнему, что $N = 210$, будем иметь

$$10 \setminus 15 = 2; \quad 10 * 15 = (10, 14) \cdot (21, 15) = 2 \cdot 3 = 6.$$

При этом как нетрудно проверить (см упр. 2)

$$\text{а) } a \setminus a = 1; \quad \text{б) } a \setminus 1 = a; \quad \text{в) } N \setminus a = \bar{a}; \quad \text{г) } 1 \setminus a = 1;$$
$$\text{д) } (a \setminus b) \setminus c = (a \setminus c) \setminus b; \quad \text{е) } (a \setminus b, c) = (a, c) \setminus (b, c), \tag{10.7}$$

а также

а) $a * a = 1$, причем $a * b = 1$, лишь если $b = a$;

б) $a * 1 = a$, причем $a * b = a$, лишь если $b = 1$;

в) $N * a = \bar{a}$; г) $a * \bar{a} = 1$; д) $a * b = b * a$; е) если $a * c = b * c$, то $a = b$;

ж) если $a * b = c$, то $a * c = b$; з) $(a * b) * c = a * (b * c)$;

$$\text{и) } ((a\ \ b), c) = (a, c)\ \ (b, c). \tag{10.8}$$

Операция Шеффера | (см. с. 61) определяется для двух чисел a и b нашей системы следующим образом:

$$a \mid b = (N/a,\ N/b); \tag{10.9а}$$

другими словами, число $a|b$ содержит те и только те простые множители (из множителей числа N), которые не являются делителями ни a, ни b. Аналогично определяется и двойственная (9а) операция $\downarrow$:

$$a \downarrow b = [N/a,\ N/b]. \tag{10.9б}$$

Так если $N = 210$, то

$$10 \mid 15 = (21, 14) = 7 \quad \text{и} \quad 10 \downarrow 15 = [21, 14] = 42.$$

При этом, как легко убедиться,

а) $(a \mid b) \mid (a \mid b) = [a, b]$, б) $(a \mid a) \mid (b \mid b) = (a, b)$, в) $a \mid a = N/a$, (10.11)

или (ср равенства Ш$'_{1-2}$ на с. 63)

г) $(a \mid a) \mid (a \mid a) = a$, д) $a \mid [b \mid (b \mid b)] = a \mid a$. (10.11)

Аналогично

а) $(a \downarrow a) \downarrow (b \downarrow b) = [a, b]$, б) $(a \downarrow b) \downarrow (a \downarrow b) = (a, b)$, в) $a \downarrow a = N/a$. (10.11′)

Тернарная операция $\{a, b, c\}$ (см. с. 63) для чисел a, b и c определяется так:

$\{a, b, c\} = [(a, b), (b, c), (c, a)] = ([a, b], [b, c], [c, a])$

Другими словами, число $\{a, b, c\}$ содержит те и лишь те простые множители, которые входят в состав по крайней мере двух из чисел a, b и c. Так, например,

$\{15, 30, 70\} = 30$.

Наименьшее общее кратное $[a, b]$ и наибольший общий делитель (a, b) двух чисел a и b нашей системы определяются посредством тернарной операции $\{a, b, c\}$ следующим образом:

$[a, b] = \{a, b, N\}$; $(a, b) = \{a, b, 1\}$.

Интересно отметить, что условие о том, что исходное число N «свободно от квадратов», оказывается существенным лишь при проверке правил (VIII)

$$a \oplus \bar{a} = N, \quad a \otimes \bar{a} = 1. \tag{10.12}$$

В самом деле, примем за N совершенно произвольное натуральное число $N = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ (например, число $720 = 2^4 \cdot 3^2 \cdot 5$); далее для любых двух делителей $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ и $b = p_1^{\beta_1} p_2^{\beta_2} \ldots$ $\ldots p_k^{\beta_k}$ этого числа (где $0 \leqslant \alpha_1 \leqslant n_1$, $0 \leqslant \alpha_2 \leqslant n_2$, ..., $0 \leqslant \alpha_k \leqslant n_k$; $0 \leqslant \beta_1 \leqslant n_1$, $0 \leqslant \beta_2 \leqslant n_2$, ..., $0 \leqslant \beta_k \leqslant n_k$) положим

$$a \oplus b = [a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_k^{\max(\alpha_k, \beta_k)} \tag{10.13а}$$

и

$$a \otimes b = (a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \ldots p_k^{\min(\alpha_k, \beta_k)}. \tag{10.13б}$$

[Так, если $a = 12 = 2^2 \cdot 3$, а $b = 80 = 2^4 \cdot 5$, то $a \oplus b = [12, 80] = 2^4 \cdot 3 \cdot 5 = 240$, а $a \otimes b = (12, 80) = 2^2 = 4$.] Кроме того, обозначим

$$\bar{a} = N/a = p_1^{n_1 - \alpha_1} p_2^{n_2 - \alpha_2} \ldots p_k^{n_k - \alpha_k} \tag{10.13в}$$

и условимся обозначать символом $a \supset b$ то обстоятельство, что a делится на b (т. е. что $\alpha_1 \geqslant \beta_1$, $\alpha_2 \geqslant \beta_2$, ..., $\alpha_k \geqslant \beta_k$). Для определенной таким образом алгебраической системы сохраняют силу все отвечающие аксиомам (I) — (XXI) § 5 правила, за исключением одних лишь правил (VIII) (ибо здесь, например, при $N = 720$ имеем

$$36 \oplus \overline{36} = [36, 20] = 180 \neq N, \quad 36 \otimes \overline{36} = (36, 20) = 4 \neq 1$$

— ср. упр. 5).

Алгебраическая система (1), для которой имеют место все аксиомы (I)—(XXI) булевой структуры, кроме аксиом (VIII) (35 из 37 аксиом!), очень близка к булевой структуре, но все же, строго говоря, ею не является. Подобная структура является *дистрибутивной решеткой с нулем и единицей* (см. § 8), но она даже еще ближе того к булевой структуре, поскольку в ней имеются «почти дополнения» элементов структуры — каждому элементу $a \in \mathcal{B}$ отвечает элемент $\overline{a}$ (в решетке определена унарная операция «черта»), не обладающий свойствами (VIII), но обладающий всеми остальными свойствами (IX)—(XI) и (XXI) булевой операции $^{-}$. Иногда системы такого рода включают в теорию булевых структур (алгебр Буля), отбрасывая в списке определяющих булеву структуру аксиом соотношения (VIII); в таком случае аксиомы (VIII) считаются «дополнительными», выделяющими некоторый специальный класс булевых структур («полные» булевы структуры). В других случаях принимают, что алгебраическая система (1), в которой выполняются аксиомы (I)—(VII) и (IX)—(XXI), но не обязательно выполняются аксиомы (VIII) («неполная» булева структура), представляет собой образование, родственное булевой структуре, но все же отличное от нее.

Мы также чаще будем стоять на этой последней точке зрения.

4. *Арифметика максимумов и минимумов.* Модель, очень близкую к рассмотренной выше, можно также получить следующим образом. Рассмотрим некоторое множество $\mathcal{B}$ (вещественных!) чисел a; в дальнейшем для простоты будем считать, что числа a — это всевозможные числа, заключенные между нулем и единицей: $0 \leqslant a \leqslant 1$, так что их можно изображать точками единичного отрезка числовой оси. Далее положим

$$\text{а) } a \oplus b = \max(a, b), \quad \text{б) } a \otimes b = \min(a, b), \quad \text{в) } \overline{a} = 1 - a \qquad (10.14)$$

(число $\overline{a}$ изображается точкой, симметричной точке a относительно середины 1/2 отрезка [0, 1]; рис. 33 и 34) и условимся писать $a \supset b$, если $a \geqslant b$.

Определенные таким образом «сложение» и «умножение» вещественных чисел коммутативны и ассоциативны (ибо

$$\max[\max(a, b), c] = \max[a, \max(b, c)] = \max(a, b, c) \text{ и}$$

$$\min[\min(a, b), c] = \min[a, \min(b, c)] = \min(a, b, c));$$

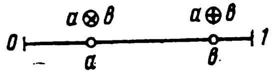


Рис. 33

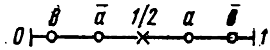


Рис. 34

совершенно очевидны также оба идемпотентных закона (ибо $\max(a, a) = a$, $\min(a, a) = a$) и законы поглощения (ибо, например, $a \oplus [a \otimes b] = \max[a, \min(a, b)] = a$). Далее имеют место также и оба дистрибутивных закона. Например, число

$$(a \oplus b) \otimes c = \min[\max(a, b), c]$$

равно c, если хоть одно из чисел a, b больше c, и равно наибольшему из чисел a, b, если оба они меньше c; но этому же равно и число

$$(a \otimes c) \oplus (b \otimes c) = \max[\min(a, c), \min(b, c)]$$

(рис. 35, *а*, *б*). Кроме того, очевидно,

$$a \oplus 0 = \max(a, 0) = a \text{ и } a \otimes 1 = \min(a, 1) = a;$$

$$a \oplus 1 = \max(a, 1) = 1 \text{ и } a \otimes 0 = \min(a, 0) = 0,$$

так что роль элементов о и ι играют числа 0 и 1.

Из определения операции $^{-}$ (рис. 34) и отношения $\supset$ сразу вытекает, что

$$\bar{\bar{a}} = a, \ \bar{1} = 0, \quad \bar{0} = 1;$$

$$a \supset a;$$

если $a \supset b$ и $b \supset c$, то $a \supset c$;

если $a \supset b$ и $b \supset a$, то $a = b$;

$$1 \supset a \supset 0 \text{ и } a \oplus b = \max(a, b) \supset a \supset$$

$$\supset \min(a, b) = a \otimes b,$$

а также, что

если $a \supset b$, то $a \oplus b = \max(a, b) = a$, $a \otimes b = \min(a, b) = b$,

$a \oplus c = \max(a, c) \supset \max(b, c) = b \oplus c$ и $a \otimes c \supset b \otimes c$;

если $a \supset b$ и $a \supset c$, то $a \supset \max(b, c) = b \oplus c$;

если $b \supset a$ и $c \supset a$, то $b \otimes c = \min(b, c) \supset a$.

[Заметим, что правила (XVIII) в силу нашего определения отношения $\supset$ просто совпадают с определениями (14).] Наконец, очевидно,

если $a \supset b$, то $\bar{b} \supset \bar{a}$

(см. рис. 34).

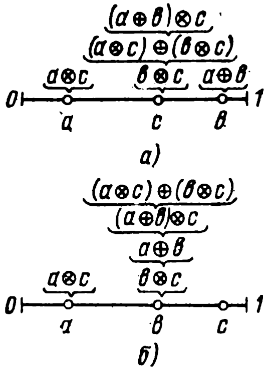


Рис. 35

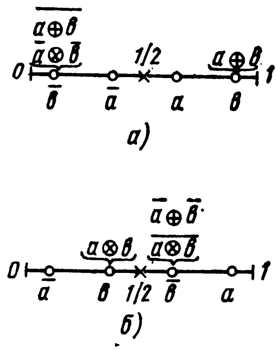


Рис. 36

Почти так же просто проверяются и правила де Моргана (XI):

$$\overline{a \oplus b} = 1 - \max(a, b) = \min(1 - a, 1 - b) = \bar{a} \otimes \bar{b},$$

$$\overline{a \otimes b} = 1 - \min(a, b) = \max(1 - a, 1 - b) = \bar{a} \oplus \bar{b}$$

(см. рис. 36, *а*, *б*). Таким образом, для нашей алгебраической системы выполняются все аксиомы булевой структуры, кроме аксиом (VIII) (ясно, что, вообще говоря, $a \oplus \bar{a} = \max(a, 1 - a) \neq 1$, $a \otimes \bar{a} = \min(a, 1 - a) \neq 0$). Другими словами, здесь мы снова встречаемся с «неполной» булевой структурой. [Большое сходство этой алгебраической системы с предыдущей объясняется глубокой аналогией определений (14) и (13).]

5. Еще более далекий от «полных» булевых структур пример, сохраняющий при всем том целый ряд присущих булевым структурам черт, доставляет нам *связка* $\mathfrak{S}$ *прямых и плоскостей* (обыкновенного или трехмерного) *пространства*, т. е. совокупность всех проходящих через фиксированную точку O прямых и плоскостей; к элементам $\mathfrak{S}$ мы условимся присоединять также точку O (*центр* связки) и все пространство R. Под «суммой» $a + b$ двух прямых a и b мы будем понимать содержащую их плоскость (рис. 37, *а*), если эти прямые различны, и каждую из этих прямых, если они одинаковы; под «суммой» $a + \alpha$ прямой a и плоскости α — все пространство R, если a не принадлежит α, и плоскость α в противном случае; под «суммой» $\alpha + \beta$ двух плоскостей α и β — все пространство R, если α и β различны, и плоскость $\alpha = \beta$, если они одинаковы; наконец, положим

$$z + O = O + z = z, \quad z + R = R + z = R, \tag{10.15a}$$

каков бы ни был элемент z связки.

Под «произведением» ab двух прямых a и b мы будем понимать точку O, если эти прямые различны, и каждую из этих прямых, если они совпадают; под произведением $a\alpha$ прямой a и плоскости α — точку O, если прямая a не принадлежит α, и саму прямую a в противном случае; под произведением $\alpha\beta$ двух плоскостей α и β — прямую их пересечения, если они не совпадают (рис. 37, *б*), и каждую из этих плоскостей в противном случае; наконец, условимся считать, что для каждого элемента z связки $\mathcal{S}$

$$zO = Oz = O,\ zR = Rz = z. \tag{10.15б}$$

Ясно, что определенные таким образом «сложение» и «умножение» элементов связки коммутативны, ассоциативны и удовлетворяют идемпотентным законам (VI); выполняются для них и законы поглощения (VII) (см. упр. 8а)). Роль «нулевого элемента» о и «единичного элемента» ι нашей системы играют, очевидно, точка O и все пространство R (ср. определения (15 а, б) с правилами (IV)—(V)).

Условимся далее считать, что $z \supset t$, если элемент z связки $\mathcal{S}$ с о д е р ж и т элемент t; при этом, очевидно, будут выполняться правила (XII)—(XV), а также правила (XVI) и (XVII). Несколько бо́льших усилий требует проверка правил (XVIII)—(XX) (выполните ее!), — но и они имеют здесь место. Наконец, если a есть прямая, то через $\bar{a}$ мы обозначим перпендикулярную a плоскость α; напротив, для плоскости α за $\bar{\alpha}$ примем перпендикулярную α прямую a (рис. 38); кроме того, положим

$$\bar{O} = R,\ \bar{R} = O. \tag{10.16}$$

Ясно, что при этом окажутся выполненными как правила (VIII), так и законы (IX), (X) (ср. (16)) и (XXI).

Менее очевидна — но все еще устанавливается без особого труда — выполнимость законов де Моргана (XI). Так, например, если a и b — две различные прямые, то их сумма $a + b$ есть «натянутая» на a и b плоскость α, а произведение ab — точка O (рис. 37,*а*). Но произведение $\bar{a}\bar{b}$ перпендикулярных a и b плоскостей $\bar{a}$ и $\bar{b}$ соответственно совпадает с перпендикуляром к плоскости α, а сумма $\bar{a} + \bar{b}$ совпадает со всем пространством R, так что здесь $\bar{a}\bar{b} = \overline{a + b}$, $\bar{a} + \bar{b} = \overline{ab}$. Аналогично, если α и β — пересекающиеся по прямой a плоскости, то $\alpha + \beta$ есть все пространство R, а $\alpha\beta = a$ (рис. 37, *б*); но так как пер-

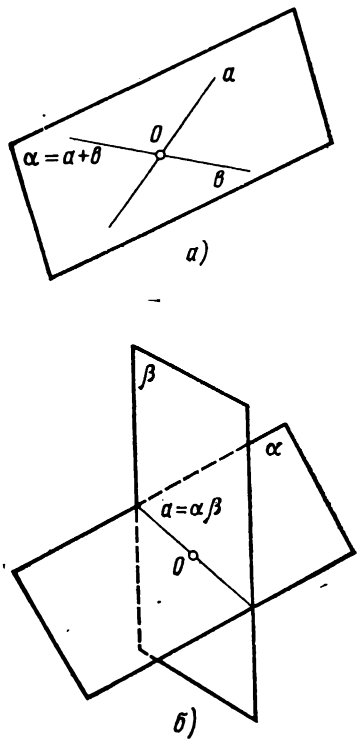


Рис. 37

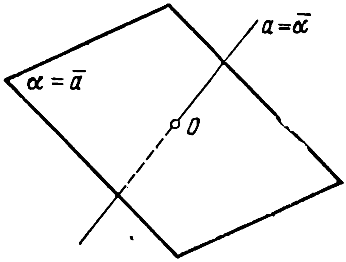


Рис. 38

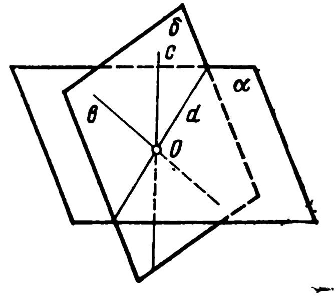


Рис. 39

пендикулярные к α и β прямые $\bar{\alpha}$ и $\bar{\beta}$ обе перпендикулярны a, то $\bar{\alpha} + \bar{\beta} = \bar{a}$ (а $\bar{\alpha}\bar{\beta} = O$), так что $\bar{\alpha} + \bar{\beta} = \overline{\alpha\beta}$, $\bar{\alpha}\bar{\beta} = \overline{\alpha + \beta}$ (ср. упр. 8в)). Однако дистрибутивные законы (III) для нашей системы места не имеют: так, например, если α есть некоторая плоскость, а b и c — две разные не принадлежащие α прямые, «порождающие» плоскость δ, пересекающую α по прямой d (рис. 39), то

$$b + c = \delta \text{ и } \alpha(b + c) = \alpha\delta = d,$$

а

$$\alpha b = \alpha c = O \text{ и } \alpha b + \alpha c = O + O = O,$$

так что

$$\alpha(b + c) \neq \alpha b + \alpha c.$$

[Впрочем, о невыполнении в нашей структуре

$$\mathbf{S} = <\mathcal{S};\ +,\ \cdot,\ ^{-},\ \supset> \tag{10.17}$$

дистрибутивных законов (III) (другими словами, о «небулевом» характере S) можно судить и из косвенных соображений: ведь в булевой структуре «дополнение» $\bar{\alpha}$ элемента α, определяемое условиями (VIII), всегда единственно (ср. с. 42), в то время как в связке $\mathcal{S}$ условиям

$$a + \alpha = R,\ a\alpha = O \tag{10.18}$$

удовлетворяет любая пара из плоскости α и не принадлежащей ей прямой a, так что за $\bar{\alpha}$ можно принять каждую не лежащую в α прямую, а за $\bar{a}$ — любую не содержащую a плоскость.] Таким образом, для структуры (17) выполняются все законы (I)—(II) и (IV)—(XXI) (т. е. 35 законов из 37), но не законы (III): S (при нашем определении операций $+$, $\cdot$, $^{-}$ и отношения $\supset$) представляет собой *решетку с дополнениями* (и даже алгебраическую структуру, несколько более близкую к булевой структуре, чем просто решетка с дополнениями — см. ниже упр. 9), но не дистрибутивную решетку с дополнениями, т. е. не булеву структуру. Ясно, что для структуры S выполняются все базирующиеся на аксиомах (I)—(II) и (IV)—(XXI) свойства булевых структур, но не свойства, существенно апеллирующие к дистрибутивности (III).

Этот пример может быть еще несколько обобщен. Нетрудно понять, что ограничение одними лишь трехмерными (векторными) пространствами вовсе не является здесь принципиальным. А именно, пусть R — произвольное (конечномерное) векторное пространство (см., например, [7] или [II, с. 88]); через $\mathcal{S}$ обозначим совокупность («связку») всех (линейных) подпространств векторного пространства R, включая сюда и «нульмерное подпространство» — нулевой вектор 0 или точку O, и все пространство R. Под *суммой* $U + V$ двух пространств U и V будем понимать их «векторную сумму»:

$$U + V = \{\mathbf{a} \mid \mathbf{a} \in R \text{ и } \mathbf{a} = \mathbf{a}_1 + \mathbf{a}_2, \text{ где } \mathbf{a}_1 \in U \text{ и } \mathbf{a}_2 \in V\}, \tag{10.19а}$$

а под *произведением* UV — пересечение пространств:

$$UV = \{\mathbf{a} \mid \mathbf{a} \in U \text{ и } \mathbf{a} \in V\}. \tag{10.19б}$$

Отношение $U \subset V$ определим как *принадлежность* подпространства U подпространству V. Далее, выбрав произвольным образом базис $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k$ пространства R, где k — размерность R, а значит, и отвечающие этому базису координаты:

$$\text{если } \mathbf{a} = \mathbf{a}(x_1, x_2, \ldots, x_k), \text{ то } \mathbf{a} = x_1\mathbf{e}_1 + x\,\mathbf{e}_2 + \ldots + x_k\mathbf{e}_k, \tag{10.20}$$

введем в R (евклидово) *скалярное произведение*:

$$\mathbf{ab} = x_1y_1 + x_2y_2 + \ldots + x_ky_k, \tag{10.21}$$

где $\mathbf{a} = \mathbf{a}(x_1, x_2, \ldots, x_k)$ и $\mathbf{b} = \mathbf{b}(y_1, y_2, \ldots, y_k)$. Теперь мы можем определить отношение *перпендикулярности* (или *ортогональности*) векторов:

$$\mathbf{a} \perp \mathbf{b} \text{ означает, что } \mathbf{ab} = 0, \tag{10.22}$$

и ввести $\overline{U}$ как «ортогональное дополнение» $U^{\perp}$ подпространства U:

$$\overline{U} = U^{\perp} = \{\mathbf{a} \mid \text{если } \mathbf{b} \in U, \text{ то } \mathbf{a} \perp \mathbf{b}\}. \tag{10.23}$$

Нетрудно видеть, что при таких определениях сложения и умножения подпространств, отношения $\supset$ между подпространствами и «дополнения» $\overline{U}$ подпространства U, множество $\mathcal{S}$ всех подпространств векторного пространства R образует (не дистрибутивную!) решетку с дополнениями, для которой выполняются все аксиомы (I)—(II) и (IV)—(XXI) булевой структуры, но не свойства (III) (см. упр. 9).

6. Итак, связка $\mathcal{S}$ векторных подпространств векторного пространства R порождает весьма близкую к булевой алгебраическую структуру, но не собственно булеву структуру. Однако исходя из концепции векторного пространства можно прийти и к содержательной и нетривиальной модели булевой структуры, в определенном смысле вложенной в решетку $\mathcal{S}$ линейных подпространств векторного пространства.

Назовем *n-угольником* (обыкновенной плоскости, трехмерного пространства или k-мерного векторного пространства[1]) просто последовательность

[1] Рассматриваемое векторное пространство можно считать *евклидовым*, хотя во всех связанных с учением о n-угольниках построениях используются лишь чисто *аффинные* конструкции. Это пространство можно также считать *точечно-векторным*; впрочем, начиная с задания n-угольника последовательностью векторов мы полностью отказываемся от использования точек, так что здесь допустимо ограничиться «чистой» концепцией векторного пространства. Основное поле F, над которым строится векторное пространство, может быть «почти любым» ([3]; ср. [8]); мы, однако, здесь будем все время иметь в виду в е щ е с т в е н н о е векторное пространство.

$<A, A_2, \ldots, A_n>$ n точек; зафиксировав произвольное начало отсчета векторов O, мы можем заменить точки их радиусами-векторами $<\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_n>$ (точке O, естественно, отвечает нулевой вектор 0). Алгебраическая структура векторного пространства позволяет определить также *сложение* n-угольников и *умножение* n-угольника *на число*:

$$\langle \mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_n\rangle + \langle \mathrm{b}_1, \mathrm{b}_2, \ldots, \mathrm{b}_n\rangle = \langle \mathrm{a}_1+\mathrm{b}_1, \mathrm{a}_2+\mathrm{b}_2, \ldots, \mathrm{a}_n+\mathrm{b}_n\rangle, \qquad (10.24а)$$

$$\lambda \langle \mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_n\rangle = \langle \lambda\mathrm{a}_1, \lambda\mathrm{a}_2, \ldots, \lambda\mathrm{a}_n\rangle, \qquad (10.24б)$$

что обращает само множество $\mathcal{M}_n$ n-угольников в векторное пространство (kn-мерное, если рассматриваются n-угольники k-мерного векторного пространства, в частности, $2n$-мерное для плоских n-угольников и $3n$-мерное для n-угольников обычного пространства). Так как, однако, «геометрическая» теория многоугольников никогда не фиксирует начальной вершины A_1, то пространство $\mathcal{M}_n$ n-угольников естественно еще «профакторизовать» по отношению $\underset{\text{ц}}{\sim}$ «циклической эквивалентности» (или просто $\sim$, как мы будем обозначать это отношение ниже), определяемому условием

$$\langle \mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{n-1}, \mathrm{a}_n\rangle \sim \langle \mathrm{a}_2, \mathrm{a}_3, \ldots, \mathrm{a}_n, \mathrm{a}_1\rangle \qquad (10.25)$$

(и естественными требованиями рефлексивности, симметричности и транзитивности этого отношения; ср. [11], с. 54). Другими словами, мы «склеиваем между собой», т. е. считаем одним объектом (*циклической последовательностью* n-угольников или *геометрическим n-угольником*[1]) цепочку

$$\langle \mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{n-1}, \mathrm{a}_n\rangle, \langle \mathrm{a}_2, \mathrm{a}_3, \ldots, \mathrm{a}_n, \mathrm{a}_1\rangle, \langle \mathrm{a}_3, \mathrm{a}_4, \ldots, \mathrm{a}_1, \mathrm{a}_2\rangle, \ldots$$
$$\ldots, \langle \mathrm{a}_n, \mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_{n-1}\rangle \qquad (10.26)$$

n-угольников, получаемых один из другого конечным числом «циклических подстановок»

$$\mathrm{a}_1' = \mathrm{a}_2, \ldots, \qquad (10.25')$$

где многоточие в конце указывает, что первое уравнение должно быть «циклически продолжено» с помощью подстановки $\begin{pmatrix}1 & 2 & \ldots & n-1 & n\\ 2 & 3 & \ldots & n & 1\end{pmatrix}$, т. е. дополнено до системы

$$\mathrm{a}_1' = \mathrm{a}_2, \mathrm{a}_2' = \mathrm{a}_3, \ldots, \mathrm{a}_{n-1}' = \mathrm{a}_n, \mathrm{a}_n' = \mathrm{a}_1; \qquad (10.25'')$$

имеющее подобный смысл многоточие после первого равенства мы будем употреблять и ниже. Таким образом, реальным объектом изучения в теории n-угольников служат циклические последовательности (26), так что интересует нас собственно не пространство $\mathcal{M}$ n-угольников, а фактор-пространство $\mathcal{M}/_{\sim}$.

Выделим теперь с помощью уравнения

$$\lambda_1 \mathrm{a}_1 + \lambda_2 \mathrm{a}_2 + \ldots + \lambda_n \mathrm{a}_n = 0, \ldots \qquad (10.27)$$

некоторое подпространство векторного пространства $\mathcal{M}_n$. Для того чтобы гарантировать согласованность этого подпространства с отношением циклической эквивалентности $\sim$ (т. е. гарантировать, что попадание одного n-угольника $<\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_n>$ в это подпространство автоматически влечет попадание в него и всех элементов цепочки (26)), мы продолжим уравнение (27) до «циклической системы» (на что указывает многоточие в конце равенства (27)), дополнив первое

[1] Таким образом, под «геометрическим n-угольником» мы понимаем здесь столь часто фигурирующие в геометрических рассмотрениях (см., например, [9]) ориентированные n-угольники, поскольку, скажем, многоугольники $<A_1, A_2, \ldots, A_{n-1}, A_n>$ и $<A_n, A_{n-1}, \ldots, A_2, A_1>$ нам удобнее не отождествлять.

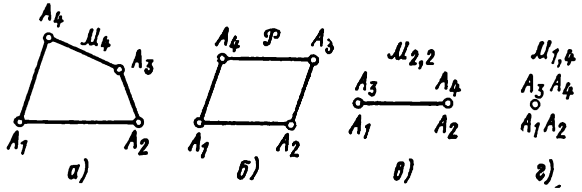


Рис. 40

уравнение (27) с коэффициентами $<\lambda_1, \lambda_2, ..., \lambda_{n-1}, \lambda_n>$ (или «уравнение $<\lambda_1, \lambda_2, ..., \lambda_{n-1}, \lambda_n>$», как мы будем говорить далее) уравнениями $<\lambda_2, \lambda_3, ..., \lambda_n, \lambda_1>$, $<\lambda_3, \lambda_4, ..., \lambda_1, \lambda_2>$, ..., наконец, $<\lambda_n, \lambda_1, \lambda_2, ..., \lambda_{n-1}>$ (система n линейных однородных уравнений с n «векторными переменными» $\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n$). Множество $\mathcal{L}$ n-угольников, удовлетворяющих некоторой системе (27), мы назовем (задаваемым системой (27)) *«циклическим классом»* n-угольников (разумеется, реально нас интересует не множество $\mathcal{L} \in \mathcal{M}_n$, а фактор-множество $\mathcal{L}/_\sim \subset \mathcal{M}_n/_\sim$). Ясно, что каждой системе (27) отвечает свой циклический класс n-угольников, однако одному и тому же циклическому классу могут, разумеется, соответствовать разные системы уравнений — хотя бы уже потому, что уравнения $<\lambda_1, \lambda_2, ..., \lambda_n>$ и $<\alpha\lambda_1, \alpha\lambda_2, ..., \alpha\lambda_n>$ (где $\alpha \neq 0$ произвольно), конечно, порождают эквивалентные системы и, следовательно, один и тот же циклический класс. Вообще, несмотря на то, что разных систем (27) существует бесконечно много, для каждого n имеется лишь к о н е ч н ы й набор циклических классов n-угольников. Вот, например, все возможные классы 4-угольников:

1) полный класс $\mathcal{I}$ или $\mathcal{M}_4$ (рис. 40, *а*; он порождается, скажем, уравнением $<0,0,0,0>$);

2) класс $\mathcal{P}$ *параллелограммов* (порождаемый уравнением $<1, -1, 1, -1>$: $\mathbf{a}_1 - \mathbf{a}_2 + \mathbf{a}_3 - \mathbf{a}_4 = 0$; см. рис. 40,*б*);

3) класс $\mathcal{M}_{2,2}$ *дважды проходимых отрезков* $<\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_1, \mathbf{a}_2>$ (рис. 40,*в*; этот класс можно задать уравнением $<1,0-1,0>$, т. е. $\mathbf{a}_1 - \mathbf{a}_3 = 0$);

4) класс $\mathcal{M}_{1,4}$ четырежды взятых точек $<\mathbf{a}_1, \mathbf{a}_1, \mathbf{a}_1, \mathbf{a}_1>$ (рис. 40,*г*; этот класс задается уравнением $<1-1, 0, 0>$ или $\mathbf{a}_1 - \mathbf{a}_2 = 0$);

5)—8) классы $\mathcal{M}_4^0, \mathcal{P}^0, \mathcal{M}_{2,2}^0, \mathcal{M}_{1,4}^0 = O$, выделяющие те из многоугольников предыдущих четырех классов, *центр тяжести* (или *центроид*) $\frac{1}{4}$ $(\mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 + \mathbf{a}_4)$ которых совпадает с «нулевой точкой» O (с нулевым вектором 0). Классы 5)—8) задаются соответственно системами (27), порождаемыми уравнениями:

$\mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 + \mathbf{a}_4 = 0$, или $<1, 1, 1, 1>$; $\mathbf{a}_1 + \mathbf{a}_3 = 0$, или $<1, 0, 1, 0>$; $\mathbf{a}_1 + \mathbf{a}_2 = 0$, или $<1, 1, 0, 0>$; $\mathbf{a}_1 = 0$, или $<1, 0, 0, 0>$

Нетрудно проверить, что (конечное!) множество линейных подпространств векторного пространства $\mathcal{M}_n$, отвечающих циклическим классам n-угольников, замкнуто относительно положенных в основу модели 5 (решетки линейных подпространств векторного пространства) операций $+$ (векторного) сложения и $\cdot$ пересечения подпространств. Эта «подрешетка» решетки всех вообще подпространств пространства $\mathcal{M}_n$ обладает единицей (класс $\mathcal{M}_n$ всех n-угольников) и нулем (нулевой класс $\mathcal{M}_{1,n}^0$, образованный единственным «нулевым» n-угольником $<O, O, ..., O>$, или $<0, 0, ..., 0>$). Но, более того, по отношению к операциям $+$ и $\cdot$ решетка циклических классов n-угольников представляет собой дистрибутивную решетку с дополнениями, т. е. *булеву структуру*. Так, на рис. 41 изображена диаграмма Гессе циклических классов 4-угольников, из которой следует, что, скажем, $\mathcal{P} + \mathcal{M}_{2,2} = \mathcal{M}_4$; $\mathcal{P} \cdot \mathcal{M}_{2,2} = \mathcal{M}_{1,4}$; $\overline{\mathcal{P}} = \mathcal{M}_{2,2}^0$; $\mathcal{M}_4^0 \supset \mathcal{M}_{2,2}^0$; $\mathcal{P}^0$, $\mathcal{M}_{2,2}^0$ и $\mathcal{M}_{1,4}$ — атомы структуры и т. д.

По поводу доказательства основной теоремы о булевой структуре циклических классов n-угольников см. [8]. В книге [8] освещается глубокая связь рассматриваемой структуры с полностью аналогичной нашей модели 3 булевой структурой делителей «многочлена деления круга» $x^n - 1$ (этот многочлен при любом n «свободен от квадратов»; при $n = 4$ элементами «структуры делителей $x^n - 1$» являются многочлены $x^4 - 1$, $x^3 + x^2 + x + 1$, $x^3 - x^2 + x - 1$, $x^2 + 1$, $x^2 - 1$, $x + 1$, $x - 1$ и 1, где сумма и произведение двух многочленов определяются как их НОК и НОД). В той же книге раскрывается роль в развиваемой теории так называемых *циклических отображений* n-угольников, подобных отображению, задаваемому уравнениями (25′) (впрочем, самоотображение (25′), разумеется, «тривиально» — оно переводит каждый n-угольник в себя). Так, отображение $\overset{\bullet}{a}_1 = \frac{1}{2}(a_1 + a_2), \ldots$ переводит «полный класс» $\mathcal{M}_4$ в класс $\mathcal{P}$ параллелограммов; отображение $\overset{\bullet\bullet}{a}_1 = \frac{1}{2}(a_1 + a_3), \ldots$ — в класс $\mathcal{M}_{2,2}$ дважды взятых отрезков и отображение $a_1^* = \frac{1}{4}(a_1 + a_2 + a_3 + a_4), \ldots$ — в класс $\mathcal{M}_{1,4}$ четырехкратных точек.

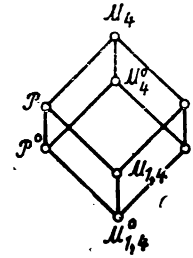


Рис. 41

Упражнения. **10.1.** Составьте таблицы, описывающие операции $\setminus$ и $*$; $|$ и $\downarrow$ (см. с. 47 и 61—62)

а) «в арифметике двух чисел»; б) в «арифметике четырех чисел».

10.2. Обозначив подходящим образом элементы булевой структуры

а) порядка 8; б) порядка 16,

составьте для этих структур «таблицу сложения»; «таблицу умножения»; «таблицу дополнения», описывающую действие операции «черта»; таблицу отношения $\supset$ (ср. с. 92)

10.3. а) Не обращаясь к общим свойствам булевых структур, докажите формулы (7); (8); (10); (11) «арифметики делителей свободного от квадратов числа N».

б) Какие из перечисленных в упр. а) результатов сохраняют силу для арифметики делителей произвольного (не обязательно свободного от квадратов) натурального числа?

10.4. а) Нарисуйте диаграмму Гессе для решетки делителей числа $180 = 2^2 \cdot 3^2 \cdot 5$.

б) Сколько элементов содержит решетка делителей числа $N = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$?

10.5. Докажите, что соотношения (VIII) заменяются в общей «арифметике наибольших кратных и наименьших делителей» (и в «арифметике максимумов и минимумов») следующими (более слабыми, чем (12)) равенствами: $a \oplus \bar{a} = \overline{a \otimes \bar{a}}$; $a \otimes \bar{a} = \overline{a \oplus \bar{a}}$. Как выводятся эти равенства из аксиом (I)—(VII) и (IX)—(XXI) «неполной» булевой структуры?

10.6. Докажите, что в (действующей на отрезке [0, 1]) «арифметике максимумов и минимумов» операцию «черта» можно задать любым инволютивным и монотонно убывающим отображением $\varphi: a \to \bar{a}$ отрезка I на себя (т. е. таким, что $\varphi(\varphi(a)) = a$ для каждого a, где $0 < a \leqslant 1$, и что из $a < b$ следует $\varphi(a) > \varphi(b)$). Так, например, вместо (14 в) можно положить $\bar{a} = 1 - 2a$, где $0 < a < 1/3$ и $\bar{\bar{a}} = a$.

10.7. Исследуйте «на независимость» аксиомы (I)—(VII) и (IX)—(XXI) неполной булевой структуры.

10.8. Не ссылаясь на общие свойства решеток, проверьте выполнимость а) правил поглощения (VII); б) законов (XVIII)—(XXI); в) правил де Моргана (XI)

1) для решетки прямых и плоскостей обыкновенного трехмерного пространства;

2) для совокупности линейных подпространств n-мерного векторного пространства.

10.9. Докажите, что совокупность линейных подпространств конечномерного векторного пространства при введенных выше определениях операций $+$, $\cdot$, $^-$ и отношения $\supset$ представляет собой модулярную решетку с дополнениями.

11. АЛГЕБРА ВЫСКАЗЫВАНИЙ И «ЗАКОНЫ МЫСЛИ»

Перейдем теперь к самому важному примеру структуры Буля, изучение которого послужило первым стимулом к введению самого этого понятия. Этот пример доставляет нам так называемая *алгебра высказываний*, представляющая собой раздел математической логики, правда, весьма элементарный и в значительной мере технический. Основными элементами алгебры высказываний служат так называемые *простые высказывания*, например высказывания: *сегодня вторник, Петя — студент, слон — насекомое*, и т. д. (мы их будем обозначать малыми буквами латинского алфавита p, q, r, ...). Потребуем, чтобы для каждого высказывания имел точный смысл вопрос о том, истинно ли оно или ложно; поэтому, скажем, фразы *два часа — это большой промежуток времени* или *Николай — умный человек*, имеющие чисто субъективный характер, для нас высказываниями не являются (ср., впрочем, ниже с. 177).

Два высказывания p и q мы будем считать *одинаковыми* (*эквивалентными*), если истинность любого из них одновременно означает и истинность другого; такие высказывания мы условимся соединять знаком равенства: $p = q$. Так, например, одинаковы высказывания: p — *сегодня воскресенье*, q — *вчера была суббота* и r — *завтра будет понедельник*. Употребление знака равенства в применении к высказываниям оправдывается тем, что определенное нами «равенство высказываний» обладает теми тремя свойствами, выполнимость которых характеризует каждое «равенство», а именно, *рефлексивностью* ($p = p$ для всех p); *симметричностью* (если $p = q$, то $q = p$) и *транзитивностью* (если $p = q$ и $q = r$, то $p = r$).

Под *суммой* $p + q$ высказываний p и q мы будем понимать новое высказывание, которое получается, если соединить высказывания p и q при помощи союза «или»; так, если p имеет смысл *Петя — студент*, а q: *слон — насекомое*, то $p + q$ есть высказывание: *Петя является студентом или слон — это насекомое*. При этом частицу «или» мы условимся понимать в неисключающем смысле — утверждение «p или q» всегда будет иметь следующий смысл: имеет место или p, или q, или, быть может, и p и q (т. е. справедливо по крайней мере одно из двух высказываний p и q). В математической логике сумма высказываний p и q называется их *дизъюнкцией* и обозначается через $p \vee q$[1].

Под *произведением* pq двух высказываний p и q мы будем понимать высказывание, получаемое, если соединить высказывания p и q с помощью союза «и»; так, при тех же высказываниях p и q, что и выше, высказывание pq гласит: *Петя является студентом и слон — это насекомое.* Таким образом, высказывание pq означает, что справедливы оба высказывания p и q. В математической логике вместо произведения двух высказываний p и q говорят об их *конъюнкции*, которую обозначают через $p \wedge q$[1].

Ясно, что определенные выше сложение (дизъюнкция) и умножение (конъюнкция) высказываний коммутативны и ассоциативны:

$$\text{а) } p + q = q + p \text{ и б) } pq = qp, \tag{I}$$

$$\text{а) } (p + q) + r = p + (q + r) \text{ и б) } (pq)r = p\,(qr); \tag{II}$$

они удовлетворяют также и идемпотентным законам:

$$\text{а) } p + p = p \text{ и б) } pp = p. \tag{VI}$$

Несколько сложнее проверяются дистрибутивные законы. Пусть p означает высказывание *сегодня ветрено*, q — *сегодня стоит ясная погода* и r — *сегодня воскресенье*. В таком случае высказывание $(p + q)r$ имет следующий смысл: *сегодня ветрено или ясно и, кроме того, сегодня воскресенье*. Высказывание же $pr + qr$ означает: *сегодня ветрено и при этом сегодня воскресенье или же сегодня стоит ясная погода и сегодня воскресенье.* Но ясно, что последние два высказывания эквивалентны:

$$(p + q)r = pr + qr. \tag{IIIа}$$

Аналогично высказывание $pq + r$ в нашем случае имеет смысл: *сегодня ветрено и ясно или сегодня воскресенье*, а комбинация $(p + r)\,(q + r)$ наших высказываний p, q, r имеет смысл: *сегодня ветрено или сегодня воскресенье, а также сегодня стоит ясная погода или сегодня воскресенье*. Но нетрудно понять, что последнее высказывание по существу совпадает с первым: ведь, если день, о котором идет речь, не является воскресеньем, то он наверное является и ясным и ветреным. Таким образом, всегда

$$pq + r = (p + r)\,(q + r). \tag{IIIб}$$

Той же схеме следует и проверка законов поглощения (VII). При прежних высказываниях p и q высказывание pq означает: *сегодня ветрено и ясно*, а высказывание $p + pq$: *сегодня ветрено или и ветрено и ясно*, откуда следует, что сегодня, во всяком случае, ветрено (но может

[1] Наряду с указанными в этой книге в литературе встречается еще ряд других символов для дизъюнкции, конъюнкции и отрицания.

быть и ясно и пасмурно — этот пример хорошо поясняет, почему здесь говорят о поглощении слагаемого pq первым членом p). Поэтому

$$p + pq = p. \tag{VIIa}$$

Так же устанавливается и равенство

$$p(p + q) = p \tag{VIIб}$$

(проверьте его!).

Условимся теперь обозначать буквой i высказывание, которое всегда является истинным (например, $2 \times 2 = 4$); под o будем понимать высказывание, которое всегда ложно (скажем *слон — это насекомое*) Ясно, что в таком случае

$$\text{а) } p + o = p \text{ и б) } pi = p; \tag{IV}$$

$$\text{а) } p + i = i \text{ и б) } po = o. \tag{V}$$

Таким образом, роль элементов i и o нашей булевой структуры играют *тождественно истинное высказывание* i и *тождественно ложное высказывание* o.

Рассмотрим еще одну чрезвычайно важную операцию «алгебры высказываний», сопоставляющую каждому высказыванию p новое высказывание $\bar{p}$ — *отрицание* p. Грамматически $\bar{p}$ получается из p при помощи частицы «не»; так, например, отрицанием высказывания *сегодня воскресенье* служит высказывание *сегодня не воскресенье.* При этом ясно, что

$$\text{а) } \bar{i} = o \text{ и б) } \bar{o} = i \tag{X}$$

— отрицание тождественно истинного высказывания (например, утверждение $2 \times 2 \neq 4$) всегда ложно, а отрицание ложного высказывания (*слон не насекомое*) всегда истинно.

Основные свойства отрицания играют в логике очень большую роль; эти свойства (их знали еще древние греки) получили даже специальные названия. Вот эти свойства:

1. Закон двойного отрицания:

$$\bar{\bar{p}} = p \tag{IX}$$

— *отрицание отрицания какого-либо высказывания равносильно первоначальному высказыванию.* Так, например, отрицанием высказывания *сегодня рабочий день* является утверждение о том, что *сегодня нерабочий день* (суббота, воскресенье или праздник); отрицание же $\bar{\bar{p}}$ утверждения $\bar{p}$ снова возвращает нас к первоначальной ситуации: *сегодняшний день не нерабочий*, т. е. *сегодня рабочий день.*

2. Закон исключенного третьего:

$$p + \bar{p} = i \tag{VIIIa}$$

— *для любого p высказывание p или не p* (т. е. p или $\bar{p}$) *всегда верно*: сегодня или рабочий день (p) или нерабочий ($\bar{p}$). [Более обычная формулировка: хоть одно из высказываний p или $\bar{p}$ всегда истинно, третьего не дано.]

3. Закон противоречия:

$$p\bar{p} = o \tag{VIIIб}$$

— *высказывание p и его отрицание $\bar{p}$ одновременно никогда не выполняются*: утверждение *сегодня и рабочий и нерабочий день* наверняка ложно, в этом можно быть уверенным и не заглядывая в календарь.

Остановимся еще на правилах де Моргана:

$$\text{а) } \overline{p+q} = \bar{p}\bar{q} \quad \text{и} \quad \text{б) } \overline{pq} = \bar{p} + \bar{q}. \tag{XI}$$

Пусть, например, p означает *Петя умеет играть в шахматы*, а q — *Петя умеет играть в шашки*. В таком случае сложное высказывание $\overline{p+q}$ — это отрицание того, что *Петя умеет играть в шахматы или в шашки*, т. е. утверждение, что *Петя не умеет играть ни в шахматы, ни в шашки*, другими словами, высказывание $\bar{p}\bar{q}$. Аналогично этому отрицание $\overline{pq}$ утверждения pq: *Петя умеет играть в шахматы и в шашки* означает, что *или Петя не умеет играть в шахматы или он не умеет играть в шашки*; но это и есть высказывание $\bar{p} + \bar{q}$.

Условимся теперь говорить, что высказывание p *следует* из высказывания q и писать $p \supset q$, если из справедливости высказывания q автоматически следует справедливость высказывания p. Так, например, если p есть высказывание *сегодня нерабочий день*, а q — высказывание *сегодня воскресенье*, то $p \supset q$ (но отношение $q \supset p$ не имеет места, ибо, кроме воскресений, нерабочими днями являются еще и праздники). Очевидно, что

$$p \supset p; \tag{XII}$$

$$\text{если } p \supset q \text{ и } q \supset r, \text{ то } p \supset r; \tag{XIII}$$

$$\text{если } p \supset q \text{ и } q \supset p, \text{ то } p = q; \tag{XIV}$$

а также

$$\text{а) } p + q \supset p, \text{ б) } p \supset pq. \tag{XVI}$$

Наконец, естественно считать, что при каждом высказывании p

$$i \supset p \tag{XVа}$$

— так как высказывание i имеет место всегда, то можно считать, что оно следует из любого высказывания p (если справедливо p, то справедливо i, поскольку i справедливо во всех случаях). Далее можно положить, что для всех p

$$p \supset o \tag{XVб}$$

— поскольку высказывание o не имеет места н и к о г д а, то в условиях, когда истинно o, можно предполагать все, что угодно (*если* $2 \times 2 = 5$, *то существуют ведьмы*): ведь сами эти условия никогда не выполняются.

Из определения отношения следствия вытекает, что

$$\text{если } p \supset q, \text{ то а) } p + q = p \text{ и б) } pq = q. \qquad \text{(XVII)}$$

В самом деле, если p следует из q, то справедливость q уже влечет за собой справедливость p; поэтому для того чтобы имело место p *или* q (т. е. высказывание $p + q$), необходимо, чтобы выполнялось p (иначе не может быть истинным н и о д н о из этих высказываний). Аналогично, для того чтобы были справедливы оба высказывания p и q (т. е. высказывание pq), достаточно, чтобы имело место q (тогда и p будет истинным). Ясно также, что если $p \supset q$ (высказывание p следует из q) и $p \supset r$ (высказывание p следует из r), то также и высказывание $q + r$ (т. е. или q, или r, или и q и r) влечет за собой p; если, напротив, $q \supset p$ и $r \supset p$ (из p следуют и q и r), то $qr \supset p$ (собственно, это мы только что и сформулировали!):

$$\left.\begin{array}{l}\text{а) если } p \supset q \text{ и } p \supset r, \text{ то } p \supset q + r;\\ \text{б) если } q \supset p \text{ и } r \supset p, \text{ то } qr \supset p.\end{array}\right\} \qquad \text{(XIX)}$$

Не сложнее доказываются и предположения:

$$\text{если } p \supset q, \text{ то а) } p + r \supset q + r \text{ и б) } pr \supset qr. \qquad \text{(XX)}$$

[Соотношения (XX) читаются так: в том случае, когда из q следует p, мы, зная, что верно высказывание q или r (т. е. $q + r$) или и q и r (т. е. qr), можем с уверенностью утверждать, что верно также высказывание p или r, и p и r соответственно.] Наконец, легко понять, что (XIXа) и (XVIа), а также соответственно (XIXб) и (XVIб) можно записать еще и так:

$$\text{а) } p + q = \max[p, q], \text{ б) } pq = \min[p, q], \qquad \text{(XVIII)}$$

где под $\max[p, q]$ понимается такое высказывание u, что, во-первых,

$$u \supset p \text{ и } u \supset q,$$

и, во-вторых, каждое такое высказывание U, что $U \supset p$ и $U \supset q$, удовлетворяет условию $U \supset u$ (разумеется, U может и совпадать с u). [Равенство (XVIIIб) аналогично выводится из (XVIб) и (XIXб); точное определение понятия $\min[p, q]$ мы предоставляем читателю.]

Наконец, также ясно, что

$$\text{если } p \supset q, \text{ то } \bar{q} \supset \bar{p}. \qquad \text{(XXI)}$$

В самом деле, отношение $p \supset q$ означает, что если имеет место q, то, наверное, справедливо и высказывание p. Но тогда из того, что p не имеет места, можно с определенностью заключить, что и высказывание q является ложным: ведь если бы q было истинным, то должно было бы быть истинным и высказывание p. Таким образом, из высказывания $\bar{p}$ следует в этом случае высказывание $\bar{q}$. Так, например, если все умеющие играть в шахматы студенты определенной студенческой группы — мужчины (из p следует q, где p — высказывание *он умеет играть в шахматы*, а q — *он мужчина*), то если данный учащийся группы — женщина, то она наверняка в шахматы не играет (из $\bar{q}$ следует $\bar{p}$).

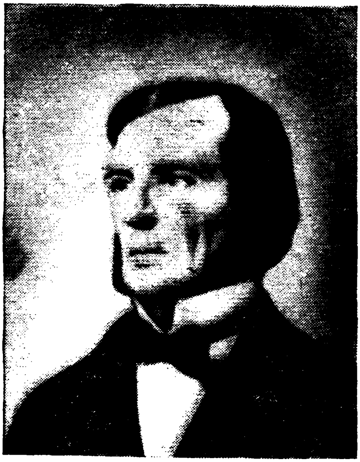
Итак, мы убедились, что *множество высказываний при определенных нами операциях сложения и умножения* (дизъюнкции и конъюнкции высказываний), *операции* $^{-}$ (отрицание) и *отношении* $\supset$ (отношение следствия) удовлетворяет аксиомам (I)—(XXI) § 5 и, следовательно, образует *булеву структуру*. Именно этот пример был подробно проанализирован в основополагающем сочинении Джорджа Буля «Исследование законов мысли» (An Investigation of the Laws of Thought), положившем начало учению об булевых структурах.

Джордж Буль (1815—1864) родился в Линкольне (Англия) в семье мелкого торговца. Материальное положение его родителей было очень затруднительным; поэтому, несмотря на явно выраженную тягу молодого Джорджа к знаниям, они не смогли дать ему систематического образования и, кроме начальных классов школы для детей бедняков, Буль не учился ни в одном учебном заведении. Впрочем, может быть, частично этим обстоятельством объясняется поражающая оригинальность Буля и свежесть его мысли, никогда не ищущей проторенных путей: ведь он не ощущал давления традиций, воплощенных в налаженной системе массового образования. Нешаблонность научного творчества Буля и всего его научного облика задержала и истинное признание заслуг Буля, которое пришло лишь тогда, когда самого Буля уже давно не было в живых

Стремление Буля к образованию радовало его родителей; однако они не имели возможности отдать его в хорошую школу и не могли помогать ему в занятиях консультациями или советами. Мальчиком Буль самостоятельно изучил латынь и греческий, которые проходились в те годы во всех аристократических школах, — и это несмотря на то, что большим затруднением явилось отсутствие в окружении Буля лиц, знавших эти языки В 12 лет он уже печатал в местных изданиях свои переводы из Горация, — но это не приносило денег, а семья крайне нуждалась

С ранних лет начался трудовой путь Буля, похожий на путь многих героев Диккенса: Буль долго искал работу, дающую какой-то заработок и в то же время оставляющую возможности для дальнейшего самообразования. Лишь после долгих мучительных поисков и многих неудачных попыток устроиться Булю удалось открыть маленькую элементарную школу, в которой он преподавал сам; денег это давало мало, но оставляло некоторый досуг. В процессе занятий с учащимися Буль впервые обратился к математике — и школьные учебники привели его в ужас своей нестрогостью и нелогичностью. Стремясь понять, что же на самом деле представляет собой математика, Буль обратился к сочинениям классиков науки и самостоятельно проштудировал обширные труды Лапласа и Лагранжа. В связи с этими занятиями у него появились первые самостоятельные идеи — и, к его счастью, Д. Грегори, основавший незадолго до того «Кембриджский математический журнал», сразу же оценил глубину мысли и оригинальность стиля провинциального учителя, присылавшего ему свои статьи; зародившаяся в эти годы дружба Грегори и Буля сыграла большую роль в жизни последнего.

Вторым человеком, поддержка которого оказалась драгоценной для Буля, был уже упоминавшийся выше (с. 20) кембриджский математик, профессор уни-



Дж. Буль

верситета Аугустус де Морган. Интересный, хоть и не всегда бесспорный ученый (его труды по расходящимся рядам Х. Х Харди (1877—1947) характеризовал как поражающий сплав глубоких мыслей и грубых ошибок), А. де Морган сам интересовался вопросами логического обоснования математики, которые вскоре стали краеугольным камнем всех размышлений Буля; первые публикации Буля заинтересовали де Моргана, а краткая брошюра «Математический анализ логики, сопровождаемый наброском исчисления дедуктивных рассуждений» (1847) привела его в восторг. [Заметим, что в том же 1847 г., несколькими месяцами позже «Математического анализа логики» вышло в свет сочинение самого де Моргана на ту же тему: «Формальная логика, или исчисление выводов, необходимых и возможных», где, в частности содержались те логические законы, которые ныне называют «правилами де Моргана»; это обстоятельство делало его высокую оценку работы Буля особенно весомой.] Усилиями де Моргана, Грегори и других друзей и поклонников самоучка Буль стал в 1849 г. профессором математики вновь открытого католического колледжа в г. Корк (Ирландия); здесь он провел последние 15 лет своей жизни, наконец-то получив возможность не только обеспечить старость родителей, но и спокойно, без мыслей о хлебе насущном, заниматься наукой. Здесь же он женился на Мери Эверест — дочери профессора греческого языка в том же колледже и родственнице бывшего генерала-губернатора Индии, по имени которого высочайшая вершина мира долго именовалась «гора Эверест»; эта женитьба способствовала укреплению материального благосостояния Буля и его социального статуса. Мери Буль-Эверест много помогала Булю в работе, а после его смерти оставила интересные воспоминания о своем муже и его научном творчестве; она стала матерью четырех дочерей Буля, которые все оказались замечательными людьми (в нашей стране из них наиболее известна Этель Лилиан Буль в замужестве Войнич[1], автор романа «Овод»).

В 1854 г. вышло в свет основное произведение Буля «Исследование законов мысли, на которых основаны математические теории логики и вероятностей». Эта обстоятельная книга ныне причисляется к математической классике; в ней подробно исследуется та алгебраическая система, которую сегодня называют «алгеброй высказываний». Правда, строго говоря, система Буля несколько отличалась от разобранной в настоящей книге: так. в качестве основных операций «алгебры логики» Буль рассматривает операции *и* (конъюнкция), *не* (отрицание) и «исключающее *или*» («исключающая дизъюнкция» или *симметрическая разность* — у Буля выражение «*p или q*» всегда имеет смысл «*или p или q, но не то и другое вместе*» — ср. ниже с. 127). Однако та отчетливость, с которой подошел Буль к задаче «алгебраизации логики», и то глубокое понимание природы математики и смысла абстрактных математических структур, которые он при этом обнаружил, не только вполне оправдывают общепринятый термин «структура (или алгебра) Буля», но и сделали возможной крылатую фразу Б. Рассела [2]: «Чистую математику открыл Буль в сочинении, которое называлось «Законы мысли»

[1] Мужем Этель Буль был польский революционер М. Войнич.

[2] Бертран Рассел (1872—1970) — выдающийся английский математик и философ, один из классиков математической логики, лауреат Нобелев-

Разумеется, фразу Рассела никак не следует понимать буквально: так, не говоря уже о гениальном Готфриде Вильгельме Лейбнице (1646—1716) или о древних греках, на европейском континенте не уступающую Булю глубину понимания абстрактной природы («чистой») математики демонстрировал в те же годы еще один самоучка (еще один школьный учитель, так же как и Буль, по достоинству оцененный лишь после смерти), немец Герман Грассман (1809—1877) [1]. Однако бесспорно, что данная Дж. Булем в «Законах мысли» характеристика (любого!) математического исчисления как «метода, базирующегося на употреблении символов, законы комбинации которых нам известны», или фраза «действенность анализа зависит не от истолкования символов, а исключительно от законов их комбинации» свидетельствуют об исключительной глубине проникновения в суть математики. И, конечно, нельзя забыть, что серьезная попытка формализованного изложения той логической системы, которая лежит в основе всех математических умозаключений,— так сказать, попытка строгого описания тех «правил игры», которым подчиняется математика (ср. [11], § 1), — принадлежит именно Дж. Булю.

Мы видим, что соотношения, выполняющиеся в абстрактных структурах Буля, имеют важный конкретный смысл: они совпадают с правилами алгебры высказываний, т. е. с теми логическими законами, которые играют основную роль в процессе нашего мышления. Любое дедуктивное рассуждение, заключающееся в том, что мы из каких-то известных заранее предпосылок делаем те или иные выводы, по существу сводится к преобразованию исходных данных по правилам алгебры высказываний; рассуждение считают «правильным» (или «точным»), если оно целиком построено на использовании перечисленных в § 5 аксиом булевой структуры (или некоторой части этих аксиом). При этом человек в процессе мышления инстинктивно следует правилам формальной логики, не формулируя каждый раз те математические законы, которыми он руководствуется в своих умозаключениях. В настоящее время, однако, мы стремимся перепоручить весьма многие функции интеллектуальной деятельности человека электронным вычислительным машинам. При этом оказалось необходимым тщательно

ской премии по литературе (на русский язык переведена обстоятельная «История западной философии» Б. Рассела (М., ИЛ., 1959) и некоторые другие его философские и литературно-философские произведения, а также научно-фантастические рассказы). Опубликованные в 1910—1913 гг. двухтомные «Основания математики» Б. Рассела и Альфреда Норта Уайтхеда (1861—1947) содержат одну из наиболее известных и продуманных систем логического обоснования математики, оказавшую большое влияние на Давида Гильберта (1862—1947) и на всех последующих ученых, занимавшихся основаниями математики и математической логикой.

[1] Ср. принадлежащие Булю и Грассману краткие формулировки сути математики [11, с. 43]. [Грассман оказал большое влияние на Рихарда Дедекинда (1831—1916), превосходно написанная и некогда весьма знаменитая (а ныне — почти забытая) брошюра которого «Что суть и что должны числа» (Was sind und was sollen die Zahlen — в русском переводе «Что такое числа и для чего они служат» (Казань, изд. Университета, 1909)) содержит развернутую трактовку грассмановских взглядов на числа и на математику в целом.]

разобраться в существе правил логики с тем, чтобы затем заложить эти правила в электронную память машины, заставив ее строго их соблюдать. С этим обстоятельством и связан, в первую очередь, тот интерес к проблемам математической логики, который характерен для наших дней.

Укажем еще, что связь булевой структуры с «законами мысли» является типичным примером использования математических методов и конструкций в (естественных и гуманитарных) науках, исследующих явления реальной жизни (см. об этом, например, [11, § 8]).

Алгебру высказываний мы рассматриваем здесь как одну из моделей абстрактного понятия *булевой структуры*, — но что представляет собой сама алгебра высказываний? Прямо связать ее можно, пожалуй, лишь с филологическими науками — это есть некоторый условный язык, позволяющий по отдельным фразам конструировать новые, более сложные: по высказываниям p, q и r построить, скажем, высказывание $p\bar{q} + \bar{p}r + pq\bar{r}$); но нас ведь интересуют не фразы, сами по себе, а смысл, который можно им придать (не семиотика или грамматика, а *семантика* «логического языка»). Выше мы сказали, что логические законы, записываемые в виде правил алгебры высказываний, играют в процессе человеческого мышления основную роль; однако слово «основную» здесь, возможно, является и некоторым преувеличением. Дж. Буль и другие логики второй половины XIX столетия (Аугустус де Морган, Готлоб Фреге, Бенджамин Пирс, Э. Шрёдер, П. С. Порецкий и др.) обработали в духе современной им алгебры так называемую «формальную» или «аристотелеву» логику, разработанную Аристотелем и его последователями специально в связи с проблемой точного описания математического доказательства, а по существу — далеко не достаточную даже и для этих ограниченных целей[1]. Разумеется, формальная (аристотелева) логика играет важную роль в процессе мышления, но она далеко не исчерпывает содержание этого необычно сложного процесса. Происхождение аристотелевой силлогистики ничем не отличается от происхождения любой другой «полуэмпирической» теории: она возникла на пути существенного огрубления реальных фактов, относящихся к высшей нервной деятельности человека, вычленения из процесса мышления «логической компоненты», легко поддающейся точному описанию и математической формализации. Таким образом, «алгебра высказываний» является не более чем достаточно неполной *моделью* «жизненной логики» человека, причем моделью, полученной в результате определенной идеализации, отсечения многих существенных, но трудно формализуемых моментов, без чего мы не пришли бы к схеме, укладывающейся в прокрустово ложе четко формулируемых законов. С подобной «идеализацией путем

---

[1] См., например, книги [10 и 11], специально посвященные вопросу о месте в математике интуиции и «полудоказательных» соображений и о специфической логике *прикладной* математики, весьма далекой от жестких аристотелевых схем.

огрубления» мы встречаемся каждый раз при попытке такой схематизации сложных жизненных явлений, которая делает возможным их математическое моделирование.

В этом отношении «алгебра высказываний» ничем не отличается от других абстрактных схем, вроде, например, ньютоновских «законов движения материальной точки» или идущей еще от голландца В. Снеллиуса (1581—1626) «геометрической оптики» — это есть схема, дающая первое приближение к реальному процессу, но вовсе не отображающая адекватно этот процесс. Именно за счет огрубления и упрощения фактического положения вещей подобные «идеализированные» схемы (ньютоновская или эйнштейнова механика, максвелловская теория электромагнитного поля, менделевская генетика и др.) допускают базирующееся на компактном списке аксиом математическое описание, не только облегчающее анализ и систематизацию известных фактов, но и дающее возможность предсказывать новые факты, которые затем удается подтвердить прямым наблюдением.

Разумеется, многие умозаключения людей не могут быть обоснованы с точки зрения строгой логики: зачастую они связаны с некоторыми полуинтуитивными представлениями, которые при настоящем положении психологии не могут быть даже охарактеризованы с той степенью полноты, которая необходима для их научного анализа. Можно сказать, что мышление человека представляет собой достаточно сложную смесь логики и интуиции; противоположную логике границу этого процесса составляют простейшие рефлексы, управляющие поведением животных. Интересно отметить, что как «формальная логика», так и изученные И. П. Павловым «условные рефлексы» легко моделируются на электронных вычислительных машинах; однако все сложное переплетение логических умозаключений, интуитивных представлений, эмоциональных возбудителей и т. д., в совокупности определяющее высшую нервную деятельность человека, не изучено еще с той степенью обстоятельности, при которой можно ставить задачу о математическом (а затем — о машинном) моделировании этого процесса. Так, перечисленные на с. 108—109 законы (VIII) и (IX) в определенной степени можно считать характерными для человеческой психики — но вовсе не «абсолютными». Ведь в жизни высказывание p человек может считать не только «верным» или «неверным» (т. е. высказывание $p + \bar{p}$ — наверняка истинным в соответствии с законом исключенного третьего (VIIIа)), но и «почти верным», «более или менее верным» или даже «вообще-то, конечно, верным, но все же для меня сомнительным» и т. д. (ср. с. 175). Также и *закон противоречия* (VIIIб) мы обычно считаем справедливым — но при этом нас ни капли не удивляет и прямо противоречащее этому закону известное двустишие римского поэта I в. до н. э. Катулла:

Да! ненавижу и вместе люблю.— Как возможно, ты спросишь?
Не объясню я. Но так чувствую, смертно томясь

(пер. А. Пиотровского), ибо мы легко можем представить себе и столь «нелогичное» (точнее, возможно, было бы сказать «неаристотелево») состояние нашей психики, имеющей гораздо более широкий спектр возможностей, чем это допускает «жесткая» аксиоматика (I)—(XXI).

Поскольку описываемая аксиомами (I)—(XXI) булевой структуры логическая система не отображает со всей полнотой процессы нашего мышления, то у нас нет никаких оснований считать ее «абсолютно истинной» — это есть всего лишь удобная математическая модель, внутренне непротиворечивая, но безупречная лишь как раздел математики, а не как психологическая реальность. «Истинной» в последней инстанции логической аксиоматики не может существовать, как не может существовать и «абсолютно истинных» аксиом механики или геометрии, рассматриваемых как свод законов, описывающих физическую реальность (в частности, то пространство, в котором мы живем) — и «аристотелева» (или «булева») логика, подобно ньютоновской механике или евклидовой геометрии, является лишь одной из ряда a priori допустимых «логик», «механик» или «геометрий» соответственно, к которым мы вынуждены прибегать, анализируя те или иные явления необозримо богатой реальности (ср. [II, с. 45]).

Близость законов алгебры высказываний к законам алгебры множеств определяется двойной связью между этими двумя алгебраическими системами. Каждое множество может быть описано либо при помощи прямого перечисления его элементов (явный, или *конструктивный*, метод задания множества), либо путем указания свойства, которому удовлетворяют все элементы данного множества и только эти элементы (неявный, или *дескриптивный*, способ задания множества). Так, можно говорить о множестве, состоящем из четырех студентов: Пети, Гали, Коли и Оли, или о *множестве отличников* данной студенческой группы, имея в виду в обоих случаях одно и то же множество.

Дескриптивный способ задания множеств связывает учение о множествах с учением о высказываниях, поскольку характеризующее элементы множества P свойство задается некоторым высказыванием p (например, *он отличник*). При этом, очевидно, что если множества P и Q описываются высказываниями (свойствами) p и q, то множества $P+Q$, PQ и $\overline{P}$ характеризуются высказываниями $p+q$, pq и $\overline{p}$. Так, например, если в некотором множестве I плоских фигур выделено подмножество P фигур единичной площади и подмножество Q треугольников, то множество $P+Q$ характеризуется высказыванием: *она (фигура) имеет площадь* 1 *или является треугольником* (рис. 42). Далее, если $P \supset Q$, то и $p \supset q$; так, если в рассмотренном выше примере все треугольники имеют единичную площадь (рис. 43), то $P \supset Q$ и одновременно с этим высказывание p — *она* (*фигура*) *имеет площадь* 1 — является следствием высказывания q — *она является треугольником*. Таким образом, задаваемое дескриптивными определениями мно-

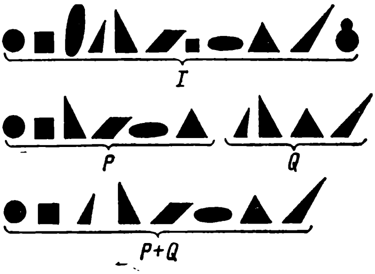


Рис. 42

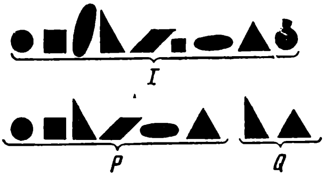


Рис. 43

жеств отображение множеств на высказывания переводит булеву структуру множеств в булеву структуру высказываний.

С другой стороны, выделив какой-то определенный круг высказываний, можно рассмотреть множество I всевозможных объектов, к которым эти высказывания относятся; так, если ограничиться лишь высказываниями о студентах определенной студенческой группы, то роль множества I будет играть множество всех учащихся этой группы. При этом каждому высказыванию p будет отвечать некоторое подмножество P множества I, а именно, множество тех элементов I, для которых *высказывание p является истинным*. Так, для высказывания p *он отличник* множество P может состоять из названных выше четырех студентов. Определенное таким образом множество P называется *множеством истинности* высказывания p. При этом, очевидно, если множества истинности высказываний p и q суть P и Q, то множества истинности высказываний $p+q$, pq и $\bar{p}$ суть $P+Q$, PQ и $\bar{P}$; так, например, в рассмотренном выше примере множество истинности высказывания $\bar{p}$: *он не отличник* состоит из всех студентов данной группы, к р о м е Пети, Гали, Коли и Оли, т. е. совпадает с множеством $\bar{P}$. Кроме того, если высказывание p следует из высказывания $q: p \supset q$, то, очевидно, множество истинности высказывания p (множество P) содержит множество истинности высказывания q (множество Q); так, если множество отличников состоит из студентов Пети, Гены, Семы и Олега, то высказывание p: *он юноша* следует из высказывания q: *он отличник* и одновременно множество юношей из данной группы содержит множество отлично учащихся студентов. Следовательно, понятие множества истинности данного высказывания отображает булеву структуру высказываний на булеву структуру множеств. При этом как первое, так и второе отображения устанавливают тождественность (изоморфизм) наших двух моделей структуры Буля: алгебры множеств и алгебры высказываний, что позволяет не проверять аксиомы (I)—(XXI) для одной из этих двух алгебраических систем, коль скоро они уже проверены для другой.

Правила алгебры высказываний могут быть использованы при решении логических задач, условия которых представляют собой совокупность высказываний, по которым требуется установить истинность или ложность других высказываний. Вот пример такого рода.

Предположим, что в санатории на берегу моря отдыхают отец O, мать M, сын C и две дочери $Д_1$ и $Д_2$. До завтрака члены семьи часто купаются в море, причем известно, что если отец утром отправляется купаться, то с ним обязательно идут мать и сын; если сын идет купаться, то его сестра $Д_1$ отправляется вместе с ним; вторая дочь $Д_2$ купается тогда и только тогда, когда купается мать, и каждое утро купается по крайней мере один из родителей. Если в воскресенье утром купалась в море лишь одна из дочерей, то кто из членов семьи в это утро ходил на море?

◀ Условимся обозначать высказывания *отец утром купался в море, мать купалась в море, 1-я дочь утром купалась в море* и т. д. символами O, M, $Д_1$, $Д_2$ и C; отрицания этих высказываний мы, как обычно, будем обозначать теми же символами, что и сами высказывания, но с черточкой наверху. В символической форме условия задачи записываются так:

$$\begin{aligned}
&1)\ OMC + \overline{O} = i,\\
&2)\ CД_1 + \overline{C} = i,\\
&3)\ MД_2 + \overline{M}\overline{Д}_2 = i,\\
&4)\ O + M = i,\\
&5)\ Д_1\overline{Д}_2 + \overline{Д}_1Д_2 = i,
\end{aligned} \tag{11.1}$$

где буквой i, как всегда, обозначено истинное высказывание. Перемножив все равенства (1), мы получим следующее соотношение:

$$(OMC + \overline{O})(CД_1 + \overline{C})(MД_2 + \overline{M}\overline{Д}_2)(O + M)(Д_1\overline{Д}_2 + \overline{Д}_1Д_2) = i, \tag{11.2}$$

равносильное системе (1) равенств (ибо истинность произведения высказываний означает, что истинны в с е высказывания).

Раскроем скобки в выражении, стоящем слева, опираясь на (первый) дистрибутивный закон (IIIa) и используя коммутативные законы (I) и ассоциативные законы (II), а также идемпотентные законы (VI), закон противоречия (VIIIб) и соотношения (Vб) и (IVa). При этом, для того чтобы несколько упростить преобразования, мы изменим порядок, в котором будем перемножать скобки:

$$\begin{aligned}
&(OMC + \overline{O})(O + M) = OMC + \overline{O}M,\\
&(OMC + \overline{O}M)(MД_2 + \overline{M}\overline{Д}_2) = OMCД_2 + \overline{O}MД_2,\\
&(OMCД_2 + \overline{O}MД_2)(Д_1\overline{Д}_2 + \overline{Д}_1Д_2) = OMC\overline{Д}_1Д_2 + \overline{O}M\overline{Д}_1Д_2,\\
&(OMC\overline{Д}_1Д_2 + \overline{O}M\overline{Д}_1Д_2)(CД_1 + \overline{C}) = \overline{O}M\overline{C}\overline{Д}_1Д_2.
\end{aligned}$$

Таким образом, окончательно получаем:

$$\bar{O}M\bar{C}\bar{Д}_1Д_2 = i, \tag{11.2'}$$

т. е. *в воскресенье утром купались в море лишь мать М и вторая дочь $Д_2$.* ▶

Основу этого решения задачи составляют те алгебраические преобразования, с помощью которых мы упростили довольно сложное выражение (2), приведя его к форме (2′). Внимательный читатель без труда поймет, что здесь мы использовали процедуру приведения стоящего в левой части (2) «булева многочлена» к *совершенной нормальной аддитивной форме*[1] (см. § 6). При этом ясно, что в случае равенства типа (2)

$$F\,(p,\ q,\ r,\ \ldots) = i, \tag{11.3}$$

где $F\,(p, q, r, \ldots)$ — какой-то булев многочлен, приведение левой части (3) к совершенной аддитивной форме, скажем, переход от (3) к

$$pq\bar{r} + p\bar{q}r + p\bar{q}\bar{r} = i, \tag{11.3'}$$

полностью проясняет ситуацию: равенство (3′) означает, что *либо p и q истинны, а r ложно*; *либо p и r истинны, а q ложно*; *либо, наконец, истинно лишь p, а q и r оба ложны.*

Впрочем, в некоторых случаях может оказаться удобнее приведение левой части (3) к *совершенной нормальной мультипликативной форме*[2]

$$\Pi\,(p' + q' + r' + \ldots) = i, \tag{11.3''}$$

где p' есть p или $\bar{p}$; аналогично расшифровываются записи q', r', ...; этот переход также проясняет условия выполнимости равенства (3).

Заметим еще, что если вместо систем типа (1) совокупность условий логической задачи записывается в виде ряда равенств, в правой части которых стоит *тождественно ложное* высказывание o, то эти равенства надо не перемножать, а складывать, и при этом мы придем к эквивалентному исходной системе равенству

$$G\,(p, q, r, \ldots) = o, \tag{11.4}$$

где $G\,(p, q, r, \ldots)$ — какой-то булев многочлен, зависящий от высказываний $p, q, r, \ldots$ (ср. упр. 1б)).

Совершенная нормальная форма высказывания может быть полезна для распознавания равных (или эквивалентных) высказываний: ведь ясно, что два зависящих от независимых[3] высказываний p, q,

---

[1] В математической логике ее чаще называют *совершенной нормальной дизъюнктивной формой.*

[2] В логике форма (3″) сложного высказывания называется *совершенной нормальной конъюнктивной формой.*

[3] Т. е. таких, что каждое из них может оказаться истинным или ложным, независимо от истинности или ложности остальных высказываний.

r, ... булева многочлена f_1 и f_2 равны в смысле нашей булевой структуры в том и только в том случае, если они имеют одинаковую совершенную нормальную аддитивную или мультипликативную форму. [При этом мы, разумеется, должны считать, что f_1 и f_2 зависят от о д н и х и т е х ж е «простых» высказываний p, q, r, ..., чего, впрочем, всегда можно добиться: ведь если, скажем, высказывание p входит в выражение для f_1, но не в выражение для f_2, то мы можем записать f_2 в виде $f_2\,(p+\bar{p})$, уже содержащем высказывание p — ср. выше, с. 51]. Но и, помимо этого, совершенная нормальная аддитивная форма сложного высказывания часто оказывается полезной.

Один пример подобного рода мы уже рассмотрели выше. Вот еще одна задача, близкая по своему математическому содержанию к рассмотренной нами «задаче об утреннем купании». Проанализируем упрощенный учебный план, где неделя включает всего три учебных дня — понедельник среду и пятницу, причем каждый день содержит не более трех пар учебных часов В течение недели учащиеся должны иметь три пары учебных часов по математике, две — по физике и по одной — по химии, истории и физкультуре. При этом:

1. Математик настаивает, чтобы его часы никогда не были последними и по крайней мере два раза — первыми

2. Физик желает чтобы его часы также не были последними; по крайней мере один раз он хочет иметь первую пару часов; в среду он должен быть свободен первые два часа, а в пятницу напротив того может работать лишь первые два часа.

3. Историк может преподавать лишь в понедельник в течение первых четырех часов или в среду в течение третьего и четвертого часов; кроме того, он не желает, чтобы его занятия непосредственно предшествовали физкультуре.

4. Химик настаивает, чтобы его занятия происходили не в пятницу и не в те дни, когда учащиеся занимаются физикой.

5. Занятия по физкультуре проводятся на стадионе, и поэтому естественно требовать, чтобы они были последними в свой день; кроме того, физкультурник в пятницу занят на другой работе.

6. Естественно требовать, чтобы в течение каждого учебного дня у учащихся было не больше двух часов занятий по одному и тому же предмету.

7. Свободные от занятий два часа в рамках учебной недели из $3\times3=9$ пар часов (из которых заняты лишь $3+2+1+1+1=8$ пар часов) должны приходиться на последнюю пару часов в пятницу или на первую пару часов в понедельник.

Как можно составить расписание с соблюдением всех поставленных условий?

◀ Перенумеруем 9 пар учебных часов цифрами от 1 до 9; в таком случае задача заключается в выяснении истинности или ложности 54 высказываний M_j, Φ_j, X_j, $И_j$, C_j, O_j, означающих, что j-я пара часов (где $j = 1, 2, \ldots$, или 9) посвящена Математике, или Физике, или Химии, или Истории, или Физкультуре (Спорту) или свободна от занятий (учащиеся Отдыхают). Условия задачи можно записать в виде следующей системы соотношений:

$$\begin{aligned}
&1)\ f_1=\overline{M}_3\,\overline{M}_6\,\overline{M}_9\,(M_1M_4+M_1M_7+M_4M_7)=i,\\
&2)\ f_2=\overline{\Phi}_3\,\overline{\Phi}_6\,\overline{\Phi}_9\,(\Phi_1+\Phi_4+\Phi_7)\,\overline{\Phi}_4\,\overline{\Phi}_8\,\overline{\Phi}_9=i\\
&3)\ f_3=(И_1+И_2+И_5)\,(\overline{И_1C_2+И_2C_3+И_4C_5+И_5C_6+И_7C_8+И_8C_9})=i,\\
&4)\ f_4=\overline{X}_7\,\overline{X}_8\,\overline{X}_9\,(\overline{\Phi_1X_2+\Phi_1X_3+\Phi_2X_1+\Phi_2X_3+\ldots+\Phi_9X_7+\Phi_9X_8})=i,\\
&5)\ f_5=(C_3+C_6+C_9+C_2O_3+C_5O_6+C_8O_9)\,\overline{C}_7\,\overline{C}_8\,\overline{C}_9=i,
\end{aligned}\qquad(11.5)$$

6) $f_6=(\overline{M_1 M_2+M_1 M_3+M_2 M_3+M_4 M_5+\ldots+M_8 M_9})\cdot$

$\cdot(\overline{\Phi_1 \Phi_2+\Phi_1 \Phi_3+\ldots+\Phi_8 \Phi_9})=i,$ **(11.5)**

7) $f_7=O_1+O_9=i.$

Система равенств (5) равносильна одному равенству

$$f=f_1 f_2 f_3 f_4 f_5 f_6 f_7=i. \qquad (11.5')$$

Совершенная нормальная аддитивная форма выражения f имеет вид:

$$f=M_1 И_2 X_3 M_4 \Phi_5 C_6 \Phi_7 M_8 O_9 \ldots+M_1 \Phi_2 C_3 M_4 И_5 X_6 \Phi_7 M_8 O_9 \ldots, \qquad (11.5'')$$

где точками обозначены 54—9=45 сомножителей, входящих в каждый из двух членов суммы f со знаком отрицания. Таким образом, существуют только два способа составления расписания, удовлетворяющие всем поставленным требованиям:

1) понедельник: математика, история, химия; среда: математика, физика, физкультура; пятница: физика, математика, свободные часы;

2) понедельник: математика, физика, физкультура; среда: математика, история, химия; пятница: физика, математика, свободные часы. ▶

Вернемся к нашей «задаче об утреннем купании». Поучительно сопоставить приведенное решение этой задачи с тем, которое мог бы предложить учащийся, не знакомый с элементами математической логики. Систему равенств (1) и последующие формальные преобразования этих равенств этот учащийся заменил бы «неформальными рассуждениями» (т. е. рассуждениями, опирающимися не на строго сформулированные законы логики, а на «здравый смысл») примерно такого рода: «Если бы Отец в воскресенье утром пошел купаться, то с ним пошли бы Мать и Сын; но вместе с Сыном пошла бы и Первая Дочь, а вместе с Матерью — Вторая Дочь; а так как в воскресенье из двух Дочерей на море была лишь одна, то Отец не мог пойти купаться» и т. д. Но нетрудно понять, что рассуждения такого рода на самом деле также опираются на строгие законы алгебры высказываний, — и пресловутый «здравый смысл» как раз и заключается в точном следовании этим законам.

Так, например, проведенное только что рассуждение может быть сформулировано так: «по условию

$M \supset O$ и $C \supset O$;

но так как, кроме того,

$Д_1 \supset C$ и $Д_2 \supset M$, $M \supset Д_2$,

то в силу правила (XIV) $M=Д_2$ и, следовательно,

$Д_2 \supset O$,

а в силу правила (XIII)

$Д_1 \supset O$;

таким образом, из высказывания O следуют высказывания $Д_1$ и $Д_2$, а так как из них имело место только одно, то справедливо высказывание $\overline{O}$» и т. д. Таким образом, «формализация» обычных умозаключений, отраженная в приведенном на с. 118—119 решении задачи, состояла лишь в том, что мы точно перечислили все предпосылки, использованные в дальнейших рассуждениях, и ввели математические символы, позволившие кратко записать как исходные правила, так и весь ход решения.

Изложенное в тексте решение «задачи об утреннем купании» легко может быть перепоручено электронной вычислительной машине, поскольку лежащие в его основе правила (I)—(XXI) алгебры высказываний легко заложить в «память» машины, а весь дальнейший ход решения достаточно просто может быть автоматизирован.

С задачами такого рода мы довольно часто встречаемся в практической жизни. Сходный характер имеет, например, задача составления расписания для того или иного учебного заведения, где приходится учитывать множество взаимосвязанных условий: пожелания и возможности преподавателей и учащихся, необходимость чередовать предметы разного характера и разной степени трудности, а также лекционные курсы и практические занятия и т. д. (ср. с разобранной на с. 120—121 задачей). С проблемами такого рода сталкивается диспетчер на транспорте, организующий наиболее рациональный режим работы, скажем, железнодорожной сети, и т. д. В настоящее время при решении подобных задач широко используются вычислительные машины, причем составление программ для их работы базируется на законах математической логики, в частности на аксиомах алгебры высказываний.

Выше мы коснулись также правил, регулирующих употребление символа $\supset$. Установление того, что два высказывания связаны этим символом, можно назвать *выводом*; тогда в записи $p \supset q$ высказывание q будет называться *условием*, а высказывание p — *заключением*, или *следствием*[1].

С такими выводами мы постоянно встречаемся в науке и в практической жизни: например, заключение любой теоремы является следствием ее условия. Правильность вывода обеспечивается соблюдением условий (XII)—(XX) и (XXI), играющих основную роль почти во всех рассуждениях. Так, правило (XIII): «если $p \supset q$ и $q \supset r$, то

[1] Иногда также говорят, что высказывание p доставляет нам *необходимое условие* истинности высказывания q (ибо для того чтобы имело место q, необходимо, чтобы имело место также и p), а высказывание q — *достаточное условие* истинности высказывания p (ибо, для того чтобы имело место p, вполне достаточно, чтобы выполнялось высказывание q); если же $p \supset q$ и $q \supset p$ (т. е. $p = q$), то говорят, что справедливость p представляет собой *необходимое и достаточное условие* того, что q имеет место (и наоборот, q доставляет нам необходимое и достаточное условие справедливости p).

$p \supset r$», другими словами, «если из q следует p и из r следует q, то из r следует p» — позволяет расчленять сложные выводы на ряд этапов. Пусть, скажем, нам требуется доказать, что если *диагонали AC и BD четырехугольника $ABCD$* (рис. 44) *в точке пересечения O делятся пополам* (это есть высказывание p), то *этот четырехугольник — параллелограмм* (высказывание q). Но если $AO = OC$ и $BO = OD$, то треугольники AOB и COD, AOD и COB конгруэнтны (высказывания q_1 и q_2; итак, $q_1 \supset p$ и $q_2 \supset p$); поэтому $\angle CAB = \angle ACD$ и $\angle CAD = \angle ACB$ (высказывания r_1 и r_2; $r_1 \supset q_1$ и $r_2 \supset q_2$), а следовательно, $AB \| CD$ и $AD \| CB$ (высказывания s_1 и s_2; $s_1 \supset r_1$ и $s_2 \supset r_2$). Итак,

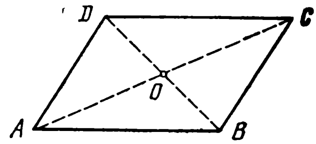


Рис. 44

$$s_1 \supset r_1 \supset q_1 \supset p \text{ и } s_2 \supset r_2 \supset q_2 \supset p;$$

значит,

$$s_1 \supset p \text{ и } s_2 \supset p,$$

— что и доказывает требуемую теорему.

Правило (XXI): «если $p \supset q$, то $\bar{q} \supset \bar{p}$» читается так: «если из высказывания q следует высказывание p, то из отрицания высказывания p вытекает отрицание высказывания q». Это правило лежит в основе весьма распространенного метода вывода (или доказательства) *от обратного* или *приведением к абсурду*. Пусть, например, мы хотим доказать теорему (см. рис. 45): если *прямые AB и CD параллельны* (это есть утверждение p), то *соответственные углы AKM и CLM, образованные этими прямыми с секущей MN, равны между собой* (это есть утверждение q). Вместо того чтобы доказывать соотношение $p \supset q$, мы докажем, что $\bar{q} \supset \bar{p}$, т. е. что из отрицания p вытекает отрицание q. Предположим, что прямые AB и CD не параллельны, т. е. что они пересекаются в некоторой точке P (рис. 46). В таком случае углы AKM и CLM не будут равны (это есть внешний угол треугольника PKL и не смежный с ним внутренний угол). Таким образом, соотношение $\bar{q} \supset \bar{p}$ доказано; тем самым доказано и соотношение $p \subset q$. [Строго говоря, здесь надо применить к соотношению $\bar{q} \supset \bar{p}$ правило (XXI) алгебры логики и воспользоваться законом двойного отрицания (IX): если $\bar{q} \supset \bar{p}$, то $\bar{\bar{p}} \subset \bar{\bar{q}}$, т. е. $p \subset q$.]

Большое значение отношения $p \supset q$ двух высказываний делает полезным рассмотрение еще одной бинарной операции алгебры высказываний, тесно связанной с этим отношением. Эта бинарная операция называется *импликацией* высказываний q и p; она записывается так: $q \Rightarrow p$. Грамматически высказывание $q \Rightarrow p$ образуется из высказываний q и p с помощью выражения «если ..., то ...» или глагола «следует»; оно гласит: «если q, то p», или «из q следует p». Так, например, если высказывания q и p имеют смысл: *Петр — спортсмен* и *слон — насе-*

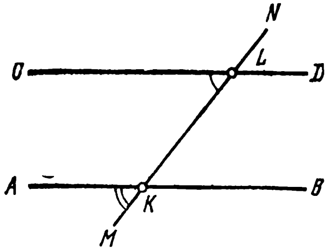


Рис. 45

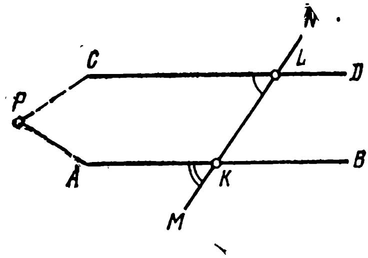


Рис. 46

комое, то высказывание $q \Rightarrow p$ означает: *Если Петр является спортсменом, то слон — насекомое* или *из того, что Петр является спортсменом, следует, что слон — это насекомое*. При этом мы будем считать, что импликация $q \Rightarrow p$ истинна во всех тех (и только тех) случаях, когда $p \supset q$; таким образом, сложное высказывание $q \Rightarrow p$ можно сформулировать также и следующим образом: *отношение* $p \supset q$ *имеет место*. Поэтому если высказывание q является ложным, то высказывание $q \Rightarrow p$ будет истинным при л ю б о м высказывании p (ибо из заведомо ложного высказывания o следует любое высказывание!); так, например, если названный выше Петр физкультурой пренебрегает, то мы будем считать истинным приведенное выше высказывание $q \Rightarrow p$: *если Петр — спортсмен, то слон — это насекомое*.

Необходимо обратить внимание читателя на глубокое различие между *операцией* $q \Rightarrow p$ алгебры высказываний и *отношением* $p \supset q$. Сложное высказывание $q \Rightarrow p$ может быть образовано при л ю б ы х высказываниях p и q; при этом, как и всякое другое высказывание, оно может оказаться истинным или ложным. Отношение же $p \supset q$ связывает лишь н е к о т о р ы е пары высказываний; при этом наличие отношения $p \supset q$ само по себе никаким высказыванием не является — это есть определенный факт, относящийся к высказываниям p и q[1].

Следует отметить одну особенность импликации $q \Rightarrow p$, отличающую ее от известных нам ранее суммы $p+q$ и произведения pq высказываний: операция $q \Rightarrow p$ н е к о м м у т а т и в н а, т. е. высказывание $p \Rightarrow q$, вообще говоря, отличается от высказывания $q \Rightarrow p$. Импликация $p \Rightarrow q$ называется *конверсией* импликации $q \Rightarrow p$. Переход от импликации $q \Rightarrow p$ к ее конверсии $p \Rightarrow q$ равносилен переходу от прямой теоремы «если q, то p» (например, *если все стороны четырехугольника равны, то его диагонали взаимно перпендикулярны*) к о б р а т-

[1] Можно также сказать, что импликация $q \Rightarrow p$ представляет собой функцию, сопоставляющую каждым двум высказываниям p и q новое *высказывание* $q \Rightarrow p$; отношение же $p \supset q$ можно описать как функцию, сопоставляющую паре высказываний p и q число 1 или 0 (если считать, что любое выполняющееся отношение имеет «значение истинности 1», а невыполняющееся — «значение истинности 0» — ср. с § 13).

н о й теореме «если p, то q» (*если диагонали четырехугольника взаимно перпендикулярны, то все его стороны равны*). Но хорошо известно, что формулировки прямой и обратной теорем вовсе не эквивалентны и одна из них может оказаться верной, а вторая — неверной. Равносильна импликации $q \Rightarrow p$ импликация $\bar{p} \Rightarrow \bar{q}$, называемая *контрапозицией* высказывания $q \Rightarrow p$: в самом деле, в силу правила (XXI) отношение $p \supset q$ является истинным в том и только в том случае, когда истинно отношение $\bar{q} \supset \bar{p}$. Переходу от высказывания $q \Rightarrow p$ (т. е. *если q, то p*) к высказыванию $\bar{p} \Rightarrow \bar{q}$ (другими словами, к высказыванию: *если не имеет места p, то не имеет места и q*) равносилен переход от прямой теоремы («если все стороны четырехугольника равны, то его диагонали взаимно перпендикулярны») к теореме, обратной противоположной исходной («если диагонали четырехугольника не взаимно перпендикулярны, то не все его стороны равны»); эта теорема оказывается эквивалентной первоначальной теореме. Импликация же $\bar{q} \Rightarrow \bar{p}$, выражающая теорему, противоположную теореме $q \Rightarrow p$ (в рассматриваемом выше случае — теорему «если все стороны четырехугольника не равны, то диагонали его не перпендикулярны»), не равносильна исходной теореме — она равносильна обратной теореме «если p, то q» (из правила (XXI) вытекает, что отношения следствия $q \supset p$ и $\bar{p} \supset \bar{q}$ выполняются или не выполняются одновременно).

Наряду с импликацией $q \Rightarrow p$ иногда рассматривают также так называемую *двойную импликацию* (или *эквивалентность*[1]) q и p, обозначаемую символом $q \Leftrightarrow p$. Двойная импликация высказываний p и q читается так: «если и только если q, то p» или «p в том и только в том случае, если q». Так, при указанных на с. 123 значениях высказываний p и q высказывание $p \Leftrightarrow q$ гласит: *Петр является спортсменом в том и только в том случае, если слон — это насекомое*. Выделенное курсивом предложение является новым высказыванием (хотя и довольно нелепым!): двойная импликация также представляет собой бинарную операцию алгебры высказываний, сопоставляющую каждым двум высказываниям q и p новое высказывание $q \Leftrightarrow p$. Ясно, что двойная импликация $q \Leftrightarrow p$ так относится к отношению равенства (эквивалентности) высказываний, как простая импликация — к отношению следствия: высказывание $q \Leftrightarrow p$ является истинным в том и только в том случае, если имеет место отношение $q = p$. В противоположность простой импликации двойная импликация высказываний уже коммутативна: для любых двух высказываний q и p высказывания $q \Leftrightarrow p$ и $p \Leftrightarrow q$ эквивалентны, т. е.

$$q \Leftrightarrow p = p \Leftrightarrow q.$$

[1] Мы предпочтем далее употреблять для рассматриваемой (бинарной) операции алгебры высказываний именно термин «двойная импликация», а не (пожалуй, более распространенное) название «эквивалентность», сохранив последнее для (бинарного) отношения $q = p$ между высказываниями — ведь никак недопустимо обозначать одним и тем же словом два разных понятия.

Понятие *множества истинности* высказывания (см. с. 117) позвс ляет перенести новые операции $q \Rightarrow p$ и $p \Leftrightarrow q$ алгебры высказывани и в область алгебры множеств. Пусть q и p — два произвольных вы сказывания, Q и P — их множества истинности. Множества истинно сти высказываний $q \Rightarrow p$ и $q \Leftrightarrow p$ мы обозначим через $Q \Rightarrow P$ и $Q \Leftrightarrow P$ Очевидно, что импликация $q \Rightarrow p$ является истинной в том и только і том случае, если высказывание q является ложным (из ложных пред посылок следуют любые выводы) или если вы сказывания q и p истинны одновременно (из истинных предпосылок следуют истинные вы· воды); другими словами, множество $Q \Rightarrow P$ представляет собой объединение дополнения множества Q и пересечения множеств Q и P (рис. 47, *а*). Отсюда следует, что

$$Q \Rightarrow P = \bar{Q} + QP, \tag{11.6}$$

а следовательно, и

$$q \Rightarrow p = \bar{q} + qp. \tag{11.6'}$$

Таким образом, импликация $q \Rightarrow p$ высказываний q и p может быть определена с помощью основных операций алгебры высказываний: сложения высказываний, умножения высказываний и образования отрицания. Так, приведенное выше высказывание: *если Петр является спортсменом, то слон — это насекомое* равносильно следующему: *или Петр спортсменом не является, или он — спортсмен, а слон — насекомое.*

Аналогично двойная импликация $q \Leftrightarrow p$ истинна в том и только в том случае, если оба высказывания: и q, и p истинны или если оба высказывания ложны. Таким образом, множество $Q \Leftrightarrow P$ представляет собой объединение пересечения множеств Q и P и пересечения множеств $\bar{Q}$ и $\bar{P}$ (рис. 47, *б*):

$$Q \Leftrightarrow P = QP + \bar{Q}\bar{P}. \tag{11.7}$$

Отсюда следует, что двойная импликация $q \Leftrightarrow p$ высказываний также может быть выражена с помощью известных нам ранее операций алгебры высказываний:

$$q \Leftrightarrow p = qp + \bar{q}\bar{p}. \tag{11.7'}$$

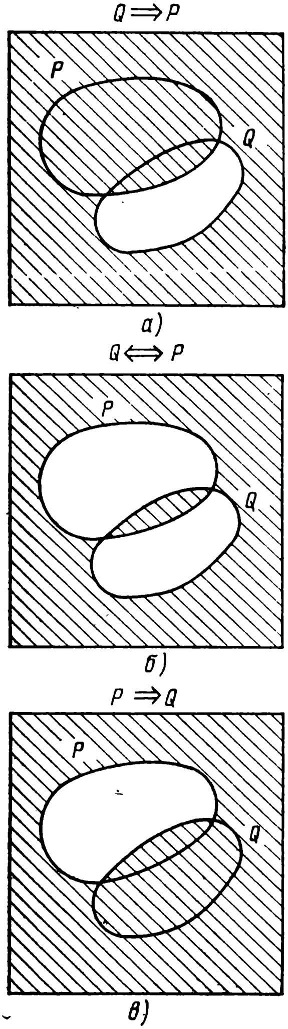


Рис. 47

Из формул (6′) и (7′) сразу следует, что двойная импликация $q \Leftrightarrow p$ представляет собой коммутативную операцию алгебры высказываний, а простая импликация $q \Rightarrow p$ — некоммутативную:

$$p \Leftrightarrow q = pq + \bar{p}\bar{q} = q \Leftrightarrow p, \text{ но } p \Rightarrow q =$$
$$= \bar{p} + pq \neq \bar{q} + qp = q \Rightarrow p$$

(см. рис. 47, *в*, на котором изображено множество $P \Rightarrow Q$ истинности конверсии $p \Rightarrow q$ импликации $q \Rightarrow p$). С другой стороны, контрапозиция $\bar{p} \Rightarrow \bar{q}$ импликации $q \Rightarrow p$ совпадает с самой импликацией: ведь

$$\bar{p} \Rightarrow \bar{q} = p + \bar{p}\,\bar{q},$$

а из рис. 47, *а* видно, что множества $Q \Rightarrow P = \bar{Q} + QP$ и $\bar{P} \Rightarrow \bar{Q} = P + \bar{P}\bar{Q}$ совпадают. Равенство импликации $q \Rightarrow p$ высказываний q и p контрапозиции $\bar{p} \Rightarrow \bar{q}$ этой импликации можно также доказать и без апелляции к чертежу:

$$\bar{p} \Rightarrow \bar{q} = p + \bar{p}\,\bar{q} = p(q + \bar{q}) + \bar{p}\,\bar{q} = (pq + p\bar{q}) + \bar{p}\,\bar{q} =$$
$$= pq + (p\bar{q} + \bar{p}\,\bar{q}) = pq + (p + \bar{p})\bar{q} = pq + i\bar{q} =$$
$$= pq + \bar{q} = \bar{q} + pq = q \Rightarrow p$$

см. аксиомы (VIIIа) и (IVб), (IIIа), (IIа), (Iа), (Iб) алгебры высказываний). Аналогично высказывание $\bar{q} \Rightarrow \bar{p}$ совпадает с конверсией $p \Rightarrow q$ импликации $q \Rightarrow p$:

$$\bar{q} \Rightarrow \bar{p} = q + \bar{q}\,\bar{p} = \bar{p} + pq = p \Rightarrow q.$$

В алгебре высказываний можно также определить *разность*

$$p \setminus q = p\bar{q} \qquad (11.8)$$

высказываний p и q («лингвистически» высказывание $p \setminus q$ образуется так: «p, но не q») и *симметричную разность*

$$p * q = p\bar{q} + \bar{p}q \qquad (11.8')$$

тех же высказываний (из (8′) следует, что высказывание $p * q$ означает «*p или q, но не p и q одновременно*»; его иногда называют *исключающей дизъюнкцией* p и q и обозначают $p \veebar q$). Нетрудно так же доказать все перечисленные на с. 47—48 свойства операций $\setminus$ и $*$ (см. упр. 2).

Операция Шеффера (11.9а)

$$p \mid q = \bar{p}\,\bar{q}$$

и двойственная ей операция

$$p \downarrow q = \bar{p} + \bar{q} \qquad (11.9б)$$

имеют в алгебре высказываний следующий смысл: высказывание $p \mid q$, очевидно означает *ни* p, *ни* q (в силу чего операцию $\mid$ в логике называют: операция «ни ни»), а высказывание $p \downarrow q$ — *не* p *или не* q. Тернарная операция $\{p, q, r\}$ алгебры логики записывается так:

$$\{p, q, r\} = pq + qr + rp = (p + q)(q + r)(r + p); \tag{11.10}$$

ясно, что высказывание $\{p, q, r\}$ означает справедливость **по крайней мере двух** из высказываний p, q и r.

При этом

$$p + q = (p \mid q) \mid (p \mid q) \quad (= (p \downarrow p) \downarrow (q \downarrow q)),$$
$$pq = (p \mid p) \mid (q \mid q) \quad (= (p \downarrow q) \downarrow (p \downarrow q)),$$
$$\bar{p} = p \mid p \quad (= p \downarrow p);$$

следовательно, например,

$$q \Rightarrow p = \bar{q} + qp = \{(q \mid q) \mid [(p \mid p) \mid (q \mid q)]\} \mid \{(q \mid q) \mid [(p \mid p) \mid (q \mid q)]\}$$

и

$q \Leftrightarrow p = pq + \bar{p}\bar{q} = r \mid r$, где $r = [(p \mid p) \mid (q \mid q)] \mid [(p_1 \mid p_1) \mid (q_1 \mid q_1)]$, а $p_1 = p \mid p$ и $q_1 = q \mid q$.

Через тернарную операцию $\{p, q, r\}$ сумма (дизъюнкция) и произведение (конъюнкция) высказываний p и q выражаются так:

$$p + q = \{p, q, i\} \quad \text{и} \quad pq = \{p, q, o\}.$$

Выше мы уже останавливались на связи между операцией $q \Rightarrow p$ и отношением $q \supset p$. С помощью алгебраических символов эта связь может быть записана так:

$$p \supset (q \Rightarrow p)q; \tag{11.11}$$

другими словами, если имеет место импликация $q \Rightarrow p$ и справедливо высказывание q, то истинно и высказывание p. Соотношение (11) с очевидностью следует из формулы (6′):

$$(q \Rightarrow p)q = (\bar{q} + qp)q = o + qp = qp,$$

ибо, как мы знаем, всегда $p \supset qp$ (см. правило (XVIб) алгебры высказываний). Составляющая содержание соотношения (11) форма аргументации представляет собой классический **силлогизм**:

Все люди смертны (т. е. если N — человек, то N смертен; $q \Rightarrow p$);
Петр — человек (q);
Следовательно, *Петр смертен* (p).

Является правильным и рассуждение, выражаемое следующим соотношением:

$$\bar{q} \supset (q \Rightarrow p)\bar{p} \tag{11.11′}$$

— если имеет место импликация $q \Rightarrow p$ и высказывание p ложно, то ложно и высказывание q. Соотношение (11′) также легко выводится из формулы (6′):

$$(q \Rightarrow p)\bar{p} = (\bar{q} + pq)\bar{p} = \bar{q}\bar{p} + (p\bar{p})q = \bar{q}\bar{p} + oq = \bar{q}\bar{p} + o = \bar{q}\bar{p};$$

поэтому $\bar{q} \supset (q \Rightarrow p)\bar{p} = \bar{q}\bar{p}$.

Вот пример, иллюстрирующий применение правила (11′):

Все математики рассуждают логично (если N — математик, то он рассуждает логично: $q \Rightarrow p$);

Павел рассуждает нелогично ($\bar{p}$);

Следовательно, *Павел не математик* ($\bar{q}$).

Точно так же, например,

$$\bar{q} \supset (q \Rightarrow p)(p \Longleftrightarrow r)\bar{r} \qquad (11.11'')$$

— если из q следует p, высказывание p эквивалентно r и r не имеет места, то не имеет места и q. В самом деле, в силу формул (6′) и (7′),

$$(q \Rightarrow p)(p \Longleftrightarrow r)\bar{r} = (\bar{q} + pq)(pr + \bar{p}\bar{r})\bar{r} = \bar{q}p(r\bar{r}) +$$

$$+ \bar{q}\bar{p}(\bar{r}\bar{r}) + (ppq)(r\bar{r}) + (p\bar{p})q(\bar{r}\bar{r}) =$$

$$= o + \bar{q}\bar{p}\bar{r} + o + o = \bar{q}\bar{p}\bar{r}$$

и, следовательно,

$$\bar{q} \supset \bar{q}\bar{p}\bar{r} = (q \Rightarrow p)(p \Longleftrightarrow r)r.$$

Можно, скажем, рассуждать следующим образом:

Если стороны четырехугольника равны, то он является параллелограммом (даже ромбом; $q \Rightarrow p$);

Четырехугольник является параллелограммом в том и только в том случае, если его диагонали делятся в точке пересечения пополам ($p \Longleftrightarrow r$);

Но у четырехугольника ABCD диагонали в точке пересечения не делятся пополам ($\bar{r}$);

Поэтому *все стороны четырехугольника ABCD никак не могут быть равны* ($\bar{q}$).

В противоположность этому, например, следующие два соотношения могут и не иметь места:

$$q \supset (q \Rightarrow p)p \qquad (11.12)$$

и

$$\bar{p} \supset (q \Rightarrow p)\bar{q}. \qquad (11.12')$$

В самом деле,

$$(q \Rightarrow p)p = (\bar{q} + qp)p = \bar{q}p + qp = (q + \bar{q})p = ip = p;$$

$$(q \Rightarrow p)\bar{q} = (\bar{q} + qp)\bar{q} = \bar{q} + (q\bar{q})p = \bar{q} + o = \bar{q},$$

а соотношения

$$q \supset p \quad \text{или} \quad \bar{p} \supset \bar{q},$$

разумеется, сами по себе (безотносительно к смыслу высказываний p и q!) никак не следуют из правил алгебры высказываний. Поэтому следующие две (к сожалению, довольно распространенные, особенно среди нематематиков) формы аргументации не вытекают из аксиом (I)—(XXI) и являются неправильными:

«Из q следует p; но p имеет место, поэтому истинно и высказывание q» (скажем, *противоположные стороны параллелограмма равны; но и у четырехугольника ABCD противоположные стороны AB и CD равны, поэтому ABCD — параллелограмм*);

«Из q следует p; но высказывание q ложно, поэтому ложно и высказывание p (например, *юристы — хорошие ораторы; но N не юрист; поэтому ему не следует поручать выступление: он говорит плохо*).

Связанные с (истинными или ложными!) аргументами (11)—(11″) и (12)—(12′) рассуждения дают достаточное представление о *силлогистике* Аристотеля, составляющей основную часть развитой последним теории доказательства (см. [12]; по поводу современной обработки этого материала см., например, [13] или гл. V книги [1.13]).

Приведенные примеры (число которых, конечно, можно значительно увеличить) достаточно выпукло иллюстрируют роль, которую играют аксиомы булевой структуры (правила (I)—(XXI) формальной логики) в общежитейских и научных рассуждениях.

Упражнения. **11.1.** Решите «задачу об утреннем купании» (см. с. 118)

а) приведя стоящий в левой части (2) многочлен к совершенной нормальной мультипликативной форме;

б) записав условия задачи в виде утверждения о *ложности* определенной системы высказываний и затем преобразовав полученную систему равенств $f_i(p, q, r, \ldots) = 0$ (где $i = 1, 2, \ldots$ и т.д., а $p, q, r, \ldots$ — это наши высказывания O, M, C и т. д.), заменив ее о д н и м равенством $F(p, q, r, \ldots) = o$.

11.2. Проверьте, что логический смысл «сложных» высказываний, записываемых через простые высказывания $\alpha, \beta, \gamma, \ldots$, с помощью выражений, стоящих в левых частях всех «булевых тождеств», отвечающих перечисленным в § 4 тождествам алгебры множеств (эти булевы тождества выписаны на с. 47—48), эквивалентен смыслу сложных высказываний, выражаемых правыми частями тех же тождеств.

11.3. На бумаге нарисован ряд фигур — многоугольных и гладких (без углов и изломов), черных и белых, больших (по площади) и маленьких, вытянутых и округлых. При этом известно, что

1) все многоугольные фигуры черные или большие;
2) все черные фигуры маленькие или округлые;
3) ни одна фигура не является одновременно и маленькой и округлой;
4) вытянутые многоугольники являются черными и большими.

Что вы можете сказать об этих фигурах?

11.4. Некоторые объекты обладают свойствами A, B и C. Что вы можете сказать о следующих условиях:

1) все B суть A; 2) если C, то не B; 3) если A и C, то также и B?

11.5 (задача Э. Шрёдера [1]). Один химик утверждал: «Соли, которые не окрашены, суть ни что иное как соли, которые не являются органическими соединениями, или суть органические соединения, которые не окрашены». Второй химик с ним не согласился. Кто из них был прав?

11.6 (задача П. С. Порецкого[2]). Относительно присутствующих на балу девиц известно, что: 1. Каждая из девиц была или благовоспитана, или весела, или молода, или красива. 2. Все нетанцующие девицы были некрасивы, а танцующие — или молоды, или веселы, или благовоспитаны. 3. Все молодые девицы были или красивы, или веселы, или благовоспитаны. 4. Все молодые или красивые девицы были либо благовоспитаны, либо веселы. 5. Все веселые девицы были или благовоспитаны, или молоды, или красивы. 6. Молодых и веселых, но некрасивых и неблаговоспитанных девиц на балу не было вовсе. 7. Молодые, красивые и веселые девицы все были благовоспитаны. 8. Все благовоспитанные девицы были или молоды, или веселы, или красивы. 9. Все красивые и благовоспитанные девицы были веселы или молоды. 10. Невеселые девицы были или немолоды, или некрасивы, или не благовоспитаны. 11. Все веселые и благовоспитанные, но немолодые девицы были красивы. 12. Немолодые девицы были или не благовоспитаны, или не веселы, или не красивы. 13. Среди некрасивых девиц не было благовоспитанных, молодых и веселых. 14. На балу присутствовали лишь неблаговоспитанные девицы, немолодые девицы, невеселые девицы и некрасивые девицы — иных не было вовсе.

Требуется проанализировать эту систему условий.

(Весьма многочисленные и разнообразные по характеру задачи на материал этого параграфа читатель сможет также найти в книгах [1.2], [1.13], [1.14], [2.1], [2.2], [2.3], [2.21], [2.22], [2.23], и др.)

12. РЕЛЕЙНО-КОНТАКТНЫЕ СХЕМЫ

Важную модель структуры Буля доставляют широко используемые в технике *релейно-контактные схемы.* Здесь мы рассмотрим, в первую очередь, простейший тип таких схем (контактные схемы), на которых можно достаточно ясно продемонстрировать современный алгебраический метод расчета сложных электрических систем.

Рассмотрим электрическую цепь, разорванную рядом контактных выключателей (рис. 48). Участки цепи, содержащие эти выключатели, мы будем обозначать большими буквами A, B, Γ, ... ; они будут служить основными элементами рассматриваемой в этом примере алгебраической системы (одна цепь может содержать, скажем, и несколько контактов A — ясно, что все эти контакты должны быть одновременно замкнуты или одновременно разомкнуты). При этом две цепи, содержащие одни и те же контакты A, B, ..., мы будем считать *одинаковыми* или *равными*, если при одном и том же состоянии всех контактов (A замкнут, B разомкнут и т. д.) обе цепи одновременно пропускают или одновременно не пропускают ток.

---

[1] Немецкий математик Эрнест Шрёдер (1841—1902), автор трехтомных «Лекций по алгебре логики» (Vorlesungen über die Algebra der Logik, Leipzig, 1890—1905 (последний том был издан посмертно))— один из основоположников математической логики.

[2] Платон Сергеевич Порецкий (1846—1907), профессор астрономии в Казанском университете, один из основоположников математической логики.

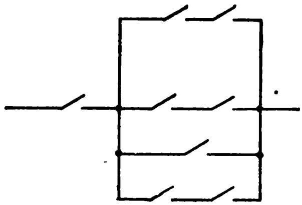


Рис. 48

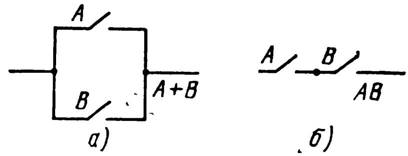


Рис. 49

Под *суммой* $A + B$ двух элементов A и B нашей цепи мы будем понимать цепь, полученную в результате *параллельного* соединения звеньев A и B; так, на рис. 49, *а* изображена сумма $A + B$, где звенья A и B содержат по одному контакту. Очевидно, что сумма $A + B$ пропускает ток в том и только в том случае, если пропускает ток х о т я б ы о д и н из элементов A и B. Под *произведением* AB мы будем понимать цепь, полученную *последовательным* соединением звеньев A и B (см. рис. 49, *б*, где снова звенья A и B в цепи содержат по одному контакту); ясно, что цепь AB пропускает ток лишь в том случае, если пропускают ток о б а ее звена A и B.

Определенные таким образом сложение и умножение электрических цепей коммутативны (см. законы (I) теории булевых структур) и ассоциативны (правила (II); см. рис. 50, на котором изображены тройная сумма $A + B + Г = (A + B) + Г = A + (B + Г)$ и тройное произведение $ABГ = (AB)Г = A\,(BГ)$ звеньев A, B, $Г$). Они также удовлетворяют идемпотентным законам (VI), поскольку параллельное или последовательное соединение двух о д и н а к о в ы х (т. е. сомкнутых или разомкнутых одновременно) контактов A дает такой же эффект, как один-единственный контакт A. Не сложнее проверяются (рис. 51, *а*, *б*) и законы поглощения (VII) — так, например, ясно, что изображенная на рис. 51, *а* цепь пропускает ток в том и только в том случае, когда пропускает ток (замкнут) контакт A. Наконец, рис. 52

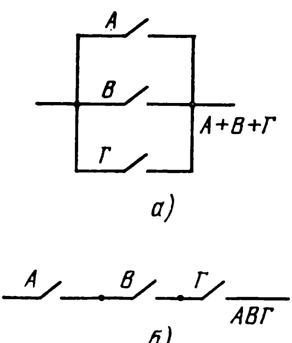


Рис. 50

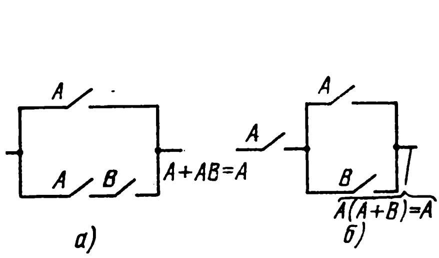


Рис. 51

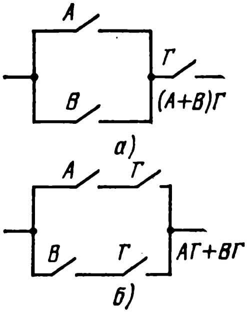


Рис. 52

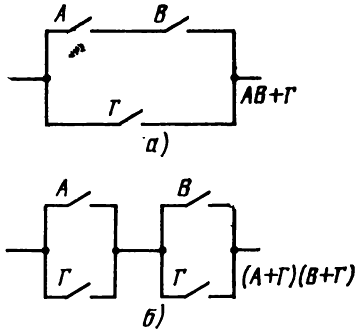


Рис. 53

и 53 иллюстрируют выполнимость в нашей «алгебре электрических схем» дистрибутивных законов (III): на рис. 52,*а* изображена схема $(A+B)\Gamma$, а на рис. 52,*б* — равносильная ей схема $A\Gamma + B\Gamma$; на рис. 53,*а* изображена схема $AB + \Gamma$, а на рис. 53, *б* — равносильная ей схема $(A+\Gamma)(B+\Gamma)$.

Условимся теперь обозначать через I тождественно замкнутый (запаянный) контакт, а через O — контакт, который никогда не замыкается (разрыв цепи). Тогда, очевидно (ср. законы (IV) и (V)),

$A + O = A$ и $AI = A$

(рис. 54), а также

$A + I = I$ и $AO = O$

(рис. 55). Таким образом, роль элементов o и ι нашей алгебры играют контакты I и O.

Договоримся еще обозначать через A и $\bar{A}$ два таких контакта, что когда A замкнут, контакт $\bar{A}$ обязательно разомкнут, и наоборот; технически такую пару контактов осуществить весьма несложно (рис. 56, где изображенный в центре переключатель может занимать всего два положения).

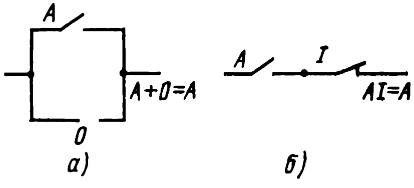


Рис. 54

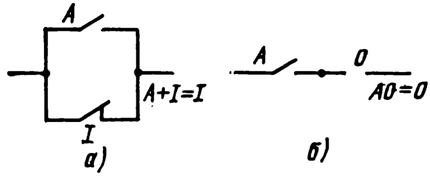


Рис. 55

При этом, очевидно, выполняются правила (VIII)—(X):

$$\overline{\overline{A}} = A,\ \overline{I} = O \text{ и } \overline{O} = I,$$

а также

$$A + \overline{A} = I \text{ и } A\overline{A} = O$$

(рис. 57, *а*, *б*). Нетрудно проверить также выполнимость правил де Моргана (XI *а*, *б*):

$$\overline{A+B} = \overline{A}\,\overline{B} \text{ и } \overline{AB} = \overline{A} + \overline{B}$$

(рис. 58,*а*, *б*; цепи C и $\overline{C}$ определяются тем условием, что если одна из них пропускает ток, то вторая не пропускает, и наоборот).

Наконец, условимся писать $A \supset B$ в том случае, если цепь A всегда пропускает ток, когда пропускает ток цепь B. При этом естественно считать, что $I \supset A$ (цепь I пропускает ток всегда!) и $A \supset O$ (цепь O никогда не пропускает ток!). Не менее очевидны, чем (XV), и законы (XII) — (XIV):

$A \supset A$;
если $A \supset B$ и $B \supset \Gamma$, то $A \supset \Gamma$;
если $A \supset B$ и $B \supset A$, то $A = B$.

Ясно также, что (ср. рис. 49, *а*, *б*)

$$A + B \supset B \text{ и } A \supset AB,$$

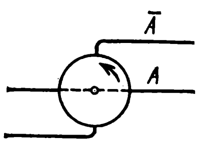


Рис. 56

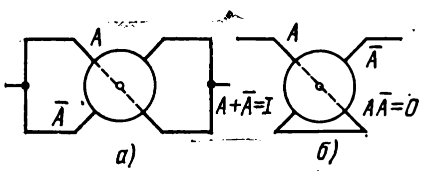


Рис. 57

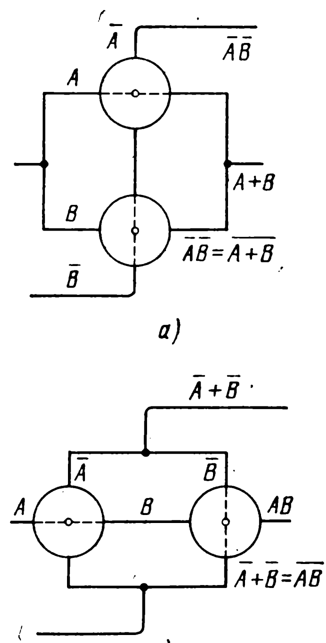


Рис. 58

т. е. в нашей «алгебре контактных цепей» выполняются и правила (XVI). Далее, нетрудно понять, что если $A \supset B$ и $A \supset \Gamma$ (т. е. если B или если Γ пропускают ток, то цепь A наверняка также ток пропускает), то и $A \supset B + \Gamma$, (ведь факт, что $B + \Gamma$ пропускает ток, означает, что ток пропускает или B или Γ!); аналогично устанавливается, что если $B \supset A$ и $\Gamma \supset A$, то $B\Gamma \supset A$. Таким образом, и законы (XIX) имеют у нас место, а из (XIX) и (XVI) вытекают (при ясных определениях) и правила (XVIII).

Из самого смысла отношения $\supset$ вытекают и законы (XX):

если $A \supset B$, то $A + \Gamma \supset B + \Gamma$ и $A\Gamma \supset B\Gamma$;

нетрудно также убедиться, что

если $A \supset B$, то $A + B = A$ и $AB = B$

(эти соотношения (XVII) можно даже принять за определение отношения $\supset$!). Наконец, из определения символа $\supset$ следует, что если $A \supset B$, то цепь B заведомо не пропускает ток, если его не пропускает цепь A; но в силу смысла операции последнее означает, что $\overline{B} \supset \overline{A}$, т. е. и правило (XXI) теории булевых структур выполняется для контактных цепей. Таким образом, *электрические контактные цепи при принятых определениях равенства (равносильности) цепей, суммы, произведения, операции* $\bar{}$ *и отношения* $\supset$ *образуют булеву структуру.*

На возможность использования (к тому времени — уже достаточно разработанного) аппарата булевой структуры для расчета электрических цепей впервые, видимо, указал в 1910 г. знаменитый австро-русско-голландский физик Пауль (или, как его называли в России, Павел Сигизмундович) Эренфест (1880—1933). В напечатанной в журнале Русского физико-химического общества рецензии [14] на русский перевод одного из первых учебников математической логики — книги Л. Кутюра «Алгебра логики» — он писал:

«... уместно коснуться вопроса о том, не встречаются ли в физике или в технике в самом деле такие сложные системы посылок (т. е. те достаточно сложные булевы формулы, преобразования и упрощения которых описаны в книге Кутюра.— *И. Я.*). *Мне думается, что на этот вопрос следует ответить утвердительно.* Пример: пусть имеется проект схемы проводов автоматической телефонной станции. Нужно определить: 1) будет ли она правильно функционировать при любой комбинации, могущей встретиться в ходе деятельности станции; 2) не содержит ли она излишних усложнений.

Каждая такая комбинация является посылкой, каждый маленький коммутатор есть логическое «или — или», воплощенное в эбоните и латуни; все вместе — система чисто качественных (в сети слабого тока именно не количественных) «посылок», ничего не оставляющая желать в отношении сложности и запутанности.

Следует ли при решении этих вопросов навсегда удовлетвориться... рутинным *способом пробования на графике*? Правда ли, что несмотря на существование уже разработанной «алгебры логики», своего рода «алгебра распределительных схем» должна считаться утопией?».

Однако это указание Эренфеста долго оставалось всего лишь гениальной догадкой — на него не было обращено никакого внимания, ибо реально в то время в компактном аппарате для расчета и проектирования сложных электрических сетей еще не было нужды. Лишь с прогрессом электроники отсутствие такого аппарата стало существенно тормозить дальнейший прогресс техники (не говоря уж о том, что без него никак не могли быть созданы ЭВМ) — и в конце 30-х годов независимо от Эренфеста та же идея была высказана и детально разработана сразу несколькими учеными в разных странах: американцем Клодом Шенноном [15], впоследствии прославившимся созданием теории информации; русским В. И. Шестаковым, диссертация [15] которого, к сожалению, не была своевременно опубликована; японцами А. Накасима и М. Ханзава. В наши дни, в связи с появлением ЭВМ и бурным прогрессом электроники, эта идентичность «алгебры электрических цепей» с булевой структурой приобрела особо важное прикладное значение; она предоставляет нам удобный алгебраический аппарат, пригодный для расчета действия сложных электрических сетей и для проектирования таких сетей с наперед заданными свойствами.

Особо ценной оказывается возможность «электромоделирования» фактов и теорем алгебры высказываний (т. е. элементарной математической логики), являющейся такой же моделью абстрактной булевой структуры, как и контактные цепи: ведь каждое «булево выражение» (булев многочлен в смысле § 6) может восприниматься как «сложное высказывание», построенное из определенных «простых высказываний», играющих роль независимых переменных, и в то же время может быть реализовано как электрическая цепь, представляющая собой комбинацию контактов A, B, Γ, ... На этой связи теории электрических цепей и логики (о ней см., например, книгу [2.13] и многие другие из названных в списке литературы пособий, скажем [1.13]) мы еще подробнее остановимся в § 14.

Пример 1. Указать контактную цепь, реализующую булев многочлен (заданный в совершенной нормальной аддитивной форме)

$$F(\alpha, \beta, \gamma) = \alpha\beta\gamma + \alpha\beta\bar{\gamma} + \alpha\bar{\beta}\gamma + \bar{\alpha}\beta\gamma \tag{12.1}$$

◀ Ясно, что многочлен $F(A, B, \Gamma) = AB\Gamma + \ldots$ реализуется изображенной на рис. 59,*а* цепью, содержащей 12 контактов. Однако тот же многочлен F можно реализовать и проще: так как, очевидно,

$$F(\alpha, \beta, \gamma) = (\alpha + \bar{\alpha})\,\beta\gamma + \alpha\,(\bar{\beta}\gamma + \bar{\beta}\gamma) = \beta\gamma + \alpha\,(\bar{\beta}\gamma + \beta\bar{\gamma}), \tag{12.1'}$$

то F реализует и изображенная на рис. 59,*б* цепь, содержащая всего семь контактов. Но и эта цепь не является простейшей электрической моделью F: поскольку в силу коммутативности (Iб), ассоциативности (IIа), идемпотентности (VIа) и закона поглощения (VIIа)

$$\beta\gamma = (\beta\gamma) + (\beta\gamma)\alpha = \beta\gamma + \alpha\beta\gamma + \alpha\beta\gamma,$$

то правую часть (1′) можно переписать так:

$$\beta\gamma + \alpha\beta\gamma + \alpha\beta\gamma + \alpha\beta\bar{\gamma} + \alpha\bar{\beta}\gamma = \beta\gamma + \alpha\beta(\gamma + \bar{\gamma}) + \alpha\gamma(\beta + \bar{\beta}) =$$
$$= \beta\gamma + \alpha\beta\iota + \alpha\gamma\iota = \beta\gamma + \alpha\beta + \alpha\gamma, \quad \text{т. е.}$$

$$F(\alpha, \beta, \gamma) = \beta\gamma + \alpha(\beta + \gamma) \tag{12.1″}$$

(см. изображенную на рис. 59,*в* цепь, содержащую всего пять контактов). ▶

Этот пример поясняет занимающую большое место в прикладной теории булевых структур (и электрических цепей) тематику, связанную с отысканием минимальных (скажем, по числу вхождения отдельных букв) реализаций тех или иных булевых многочленов (см. например, [2.13] или [2.23]). При этом сама постановка вопроса о минимизации требует четкого описания класса допустимых записей булевых многочленов и допустимых электрических цепей; имеющиеся здесь возможности мы проиллюстрируем двумя простыми примерами.

Пример 2. Упростить цепь, изображенную на рис. 60,*а*.

◀ Ясно, что наша цепь реализует булев многочлен

$$G = \alpha(\beta + \gamma\delta) + \varepsilon(\delta + \gamma\beta) \tag{12.2}$$

(в котором, чтобы получить цепь рис. 60, *а*, надо лишь заменить строчные греческие буквы прописными). Но тот же многочлен моделирует и изображенная на рис. 60, *б* цепь, в которой фигурируют лишь пять контактов вместо исходных восьми (и это число, разумеется, уже нельзя уменьшить, поскольку многочлен (2) зависит от пяти переменных α, β, ..., ε): ведь вход M и выход N цепи можно соединить четырьмя путями: $A - B$, $A - \Gamma - \Delta$, $E - \Delta$ и $E - \Gamma - B$, так что наша «мостиковая» цепь (обратите внимание на «перемычку» Γ!) реализует (не отличающийся от G) многочлен

$$\alpha\beta + \alpha\gamma\delta + \varepsilon\delta + \varepsilon\gamma\beta. \blacktriangleright \tag{12.2′}$$

Таким образом, использование *мостиковых* (содержащих перемычки) схем (которое, разумеется, надо заранее разрешить или, напротив, запретить) помогает иногда значительно упростить электрическую цепь.

Пример 1 (продолжение). ◀ Перепишем формулу (1′) для многочлена F так:

$$F(\alpha, \beta, \gamma) = \beta\gamma + \alpha(\beta * \gamma),$$

где $\beta * \gamma$ — симметрическая разность $\beta\bar{\gamma} + \bar{\beta}\gamma$ элементов β и γ (см. (5.6б)). Но комбинацию $A * B$ контактов A и B реализовать весьма просто (см. рис. 61, на котором каждый из указанных кружками внутри «ящика» переключателей может занимать одно из двух возможных положений). Таким образом, изображенную на рис. 59,*б* схему можно еще упростить (см. рис. 59,*г*) — для реального осуществления этой цели достаточны всего пять контактов, два из которых являются переключателями. ▶

Последний пример показывает, как может упростить электрическую цепь использование переключателей; он интересен также и тем, что здесь мы встретились со специальным устройством, модулирующим операцию * булевой структуры. Ясно, что эта операция может быть реализована также изображенным на рис. 61 2—1-полюсником, т. е. электрическим устройством с двумя входами A и B и с одним выходом $A * B$. Еще проще реализуются как 2—1-полюсники операции + и · булевой структуры (см. упр. 1 ниже). Наконец, простым техническим устройством является так называемый *инвертор*, обращающий процесс подачи электрического тока: с выхода инвертора ток поступает в цепь лишь тогда, когда он не подается на вход.

Утверждение о том, что все операции булевой структуры могут быть выражены через одну лишь операцию Шеффера $\alpha \mid \beta = \overline{\alpha\beta}$ (см. с. 62),

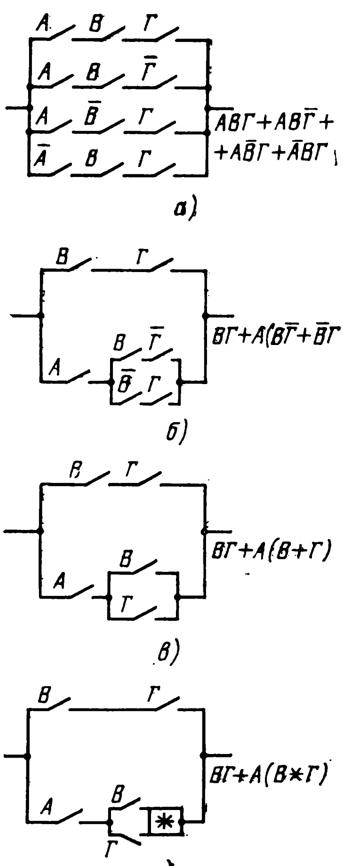


Рис. 59

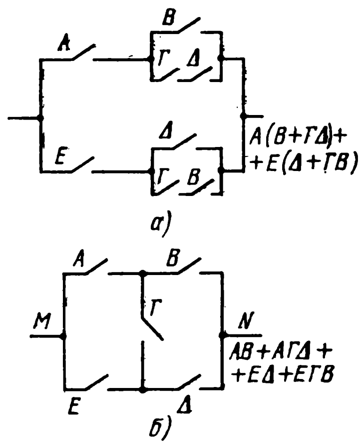


Рис. 60

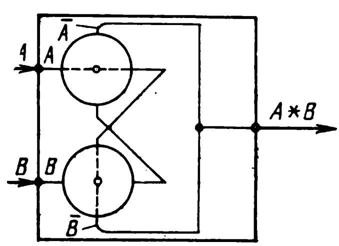


Рис. 61

равносильно возможности конструирования любых контактных электрических сетей с помощью одного 2—1-полюсника Σ, имеющего два входа и один выход, причем ток на выход поступает в том и только в том случае, если ни на один из входов ток не подается. [Такой элемент нетрудно спроектировать, если, например, условиться, что каждому участку цепи отвечают д в а параллельно идущих провода, по одному из которых ток течет всегда.] На рис. 62,*а* — *в* изображены сумма $A + B$ и произведение AB цепей A и B, а также «обращение» $\overline{A}$ цепи A, осуществляемые с помощью «элемента Шеффера» (ср. выше с. 62).

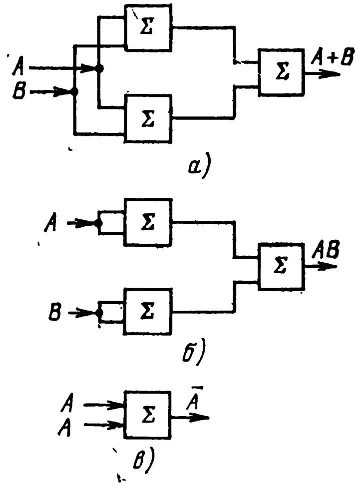


Рис. 62

Аналогичную роль может играть также 3—1-полюсник M, имеющий три входа и один выход, причем на выход ток поступает лишь в том случае, если ток поступает по крайней мере на два из входов элемента M (этот элемент отвечает операции $\{\alpha\beta\gamma\} = \alpha\beta + \beta\gamma + \gamma\alpha = (\alpha + \beta)(\beta + \gamma)(\gamma + \alpha)$ алгебры Буля; ср. с. 63). На рис. 63,*а*, *б* показано, как осуществить с помощью элемента M «сложение» и «умножение» цепей A и B (см. также Ш е н н о н [15], п. 4.2).

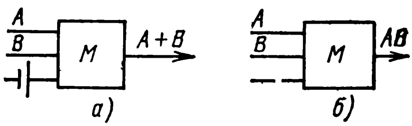


Рис. 63

Электрические цепи, сконструированные с участием логических элементов +, · (или ×), ∗ , ‾ (инвертор), Σ, M и т. д., называются *логическими цепями*; техническая их реализация является несложной. Так, например, рис. 64,*а*, *б* демонстрируют два варианта логической реализации многочлена F из примера 1 (ср. с рис. 59,*г* и *б*). На

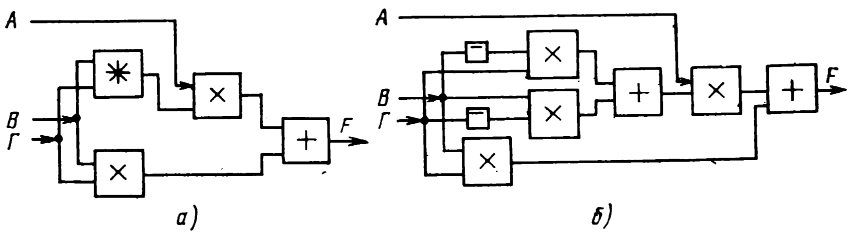


Рис. 64

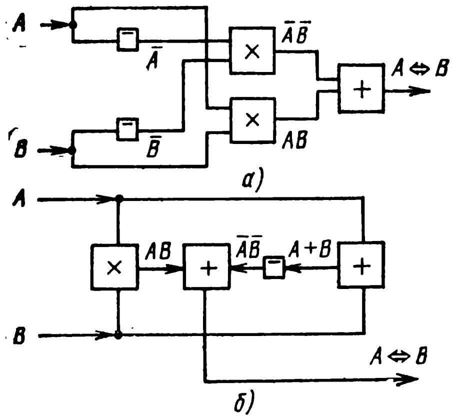


Рис. 65

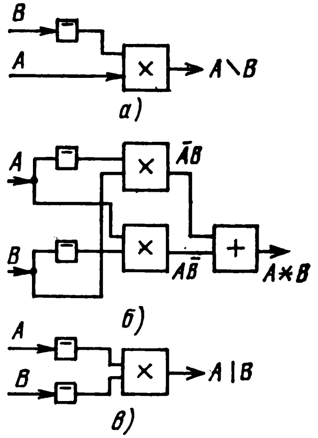


Рис. 66

рис. 65,*а*, *б* изображены два варианта реализации операции $\Leftrightarrow$ (с. 125) с помощью элементов $+$, $\times$ и инвертора$^-$, а на рис. 66, *а* — *в* реализация с помощью тех же элементов операций $\setminus$, $*$ и $|$.

Упражнения. 12.1. Опишите техническое устройство 2—1-полюсников, реализующих логические операции $+$ и $\cdot$

12.2. Опишите контактную цепь, реализующую булев многочлен $\alpha\beta\gamma\delta +$ $+ \alpha\beta\bar\gamma + \bar\beta\gamma\delta$, и упростите эту цепь, заменив ее подходящей мостиковой схемой.

12.3. Постройте логическую цепь, реализующую выражение $\bar A + A\bar B + BC$, и контактную цепь, имеющую тот же смысл.

12.4. Постройте логические цепи (использующие элементы $+$, $\cdot$ и $^-$) для выражений

а) $\alpha \Rightarrow \beta$; б) $\alpha \downarrow \beta$ в) $\{\alpha\beta\gamma\}$,

а также контактные цепи, реализующие те же булевы выражения.

Глава 4

НОРМИРОВАННЫЕ БУЛЕВЫ СТРУКТУРЫ

13. ОПРЕДЕЛЕНИЕ И МОДЕЛИ; ФОРМУЛА ВКЛЮЧЕНИЙ И ИСКЛЮЧЕНИЙ

В основе всей настоящей главы лежит

Определение. Булева структура

$$\mathbf{B} = < \mathscr{B}; +, \cdot, ^-, \supset >, \tag{13.1}$$

где $\mathscr{B} = \{\alpha, \beta, \gamma, \ldots, \iota, o\}$ — некоторое (конечное или бесконечное) множество элементов, в котором выделены «особые» элементы ι и o а операции $+$, $\cdot$, $^-$ и отношение $\supset$ удовлетворяют аксиомам (I)—(XXI)

§ 5, называется *нормированной*, если каждому элементу $\alpha \in \mathcal{B}$ сопоставляется неотрицательное число $|\alpha|$ или $m(\alpha)$ — *абсолютная величина* или *норма* элемента α, причем

H_1: $0 \leqslant |\alpha| \leqslant 1$; $|o| = 0$, $|\iota| = 1$;

H_2: если $\alpha\beta = o$, то $|\alpha + \beta| = |\alpha| + |\beta|$ (здесь, как всегда, $\alpha, \beta, \in \mathcal{B}$ произвольны).

Таким образом, **нормированная булева структура** — это структура

$$\mathbf{B}_н = < \mathcal{B}; +, \cdot, ^-, \supset, ||>, \qquad (13.1')$$

в которой к числу известных нам операций и отношений $+, \cdot, ^-, \supset$ прибавляется еще у н а р н а я о п е р а ц и я $||$, сопоставляющая с каждым элементом $\alpha \in \mathcal{B}$ число $|\alpha| \in \mathcal{R}$ (где $\mathcal{R}$ — множество вещественных чисел[1]), описываемая аксиомами (I) — (XXI) и $H_{1,2}$ (или $Б_{1-8}$ и $H_{1,2}$ — см. с. 45).

Заметим, впрочем, что аксиома H_1 нормы в чем-то является и избыточной. Из того, что для любого элемента $\alpha \in \mathcal{R}$ всегда $\alpha o = o$, $\alpha + o = \alpha$ (см. аксиомы (Vб) и (IVa) булевой структуры), следует в силу H_2

$$|\alpha| = |\alpha + o| = |\alpha| + |o|,$$

откуда вытекает, что (13.2)

$$|o| = |\alpha| - |\alpha| = 0.$$

Таким образом, равенство $|o| = 0$ можно в ы в е с т и из H_2, — и значит, его можно исключить из содержания аксиомы H_1: в настоящем виде наша аксиоматика $H_{1,2}$ нормы является *зависимой*. Более того, весьма часто при определении нормы аксиома H_1 формулируется в виде более слабого требования *неотрицательности* нормы:

H_1': $|\alpha| \geqslant 0$ для всех $\alpha \in \mathcal{B}$ и $|\alpha_0| \neq 0$ для некоторого $\alpha_0 \in \mathcal{B}$.

При этом в силу

$$\alpha + \bar{\alpha} = \iota, \ \alpha\bar{\alpha} = o \qquad (VIII)$$

имеем по H_2

$$|\iota| = |\alpha| + |\bar{\alpha}| \geqslant |\alpha| \qquad (13.3)$$

(см. H_1') — и значит, норма $|\iota| = \nu \geqslant |\alpha_0| > 0$ единичного элемента ι булевой структуры является н а и б о л ь ш е й из всех норм. А далее остается только «нормировать» все числа $|\alpha|$, выбрав «единицу норм» так, чтобы было $|\iota| = 1$ (для этого достаточно поделить все числа $|\alpha|$ на число $\nu > 0$); при этом в силу H_1 и (3) будем иметь $0 \leqslant |\alpha| \leqslant 1$, т. е. аксиому H_1. Впрочем, в некоторых случаях (см., например, ниже

[1] Говорят, что унарная операция $||$ имеет своей «областью отправления» $\mathcal{B}$, а «областью прибытия» $\mathcal{R}$ (ср. [11], с. 100); можно также говорить о заданной на $\mathcal{B}$ (*вещественнозначной*) *функции* $||$ или об *отображении* $||: \mathcal{B} \to \mathcal{R}$.

модели 3 и 5, а также модель 7, правда, моделирующую структуру «решетка с дополнениями», а не булеву структуру) удобнее выбирать единицу измерения норм по-другому.

Перейдем к рассмотрению *моделей* нормированной булевой структуры, первая из которых докажет непротиворечивость соответствующей аксиоматики, а первая и вторая — ее неполноту.

1. Элементами рассмотренной на с. 91 «арифметики двух чисел» являются «числа» 0 и 1. Эти же числа (уже в обычном арифметическом их смысле) можно принять за нормы соответствующих элементов:

$$|0| = 0, \; |1| = 1.$$

При этом очевидным образом выполняется аксиома H_1 определения нормы элемента. Далее, поскольку

$$0 \cdot 0 = 0 \text{ и } |0+0| = 0 = |0| + |0|, \; 0 \cdot 1 = 0 \text{ и } |0 + 1| = 1 = |0| + |1|,$$

то выполнена и аксиома H_2. [Вообще, для любой булевой структуры, для которой выполняется аксиома H_1 определения нормы, аксиома H_2 автоматически выполняется для пары α, β элементов структуры, хотя бы один из которых совпадает с o: при этом $\alpha o = o$ и $|\alpha + o| = |\alpha| = |\alpha| + 0 = |\alpha| + |o|$. Но в нашем случае обращение одного из элементов α, β аксиомы H_2 в o неизбежно.] Таким образом, такое определение нормы превращает «двухэлементную» булеву структуру $\{0,1\}$ в нормированную.

2. Для рассмотренной на с. 91 «четырехэлементной» булевой структуры было $ab = 0$ и $a + b = 1$; поэтому, если требовать выполнения H_1 и H_2, то надо считать:

$$|0| = 0, \; |1| = 1 \text{ и } |a| + |b| = |1| = 1.$$

Пусть фигурирующие в определении этой алгебры Буля «числа» a и b — это произвольные положительные числа, сумма которых равна единице, и пусть

$$|1| = 1, \; |0| = 0, \; |a| = a \text{ и } |b| = b.$$

В таком случае аксиома H_1 будет очевидным образом удовлетворена; аксиома H_2 также будет выполняться, поскольку единственной парой отличных от 0 элементов этой структуры, произведение которых равно 0, является пара элементов a, b; но $|a + b| = |1| = 1 = a + b = |a| + |b|$ (читателя не должно смущать, что в этой одной формуле символы a, b и 1 фигурируют сразу в обоих своих обличиях: как элементы булевой структуры и как вещественные числа). Итак, наше определение норм элементов обращает четырехэлементную булеву структуру в нормированную.

3. Рассмотрим теперь модель, проливающую гораздо больше света на само понятие нормированной булевой структуры. Пусть наша булева структура — это та алгебра множеств, которая рассматривалась в

§ 1 и 2; предположим еще, что универсальное множество I к о н е ч н о: скажем, I содержит N элементов. Условимся считать, что норма каждого подмножества A универсального множества I задается *количеством k входящих в A элементов*; при этом, для того чтобы соблюсти условие $|I| = 1$, мы будем делить все полученные так числа k на N (так что $|A|$ — это *доля* элементов A в универсальном множестве I).

$$|A| = k/N. \tag{13.4}$$

При этом, очевидно, выполняется аксиома H_1. Также и аксиома H_2 имеет здесь совершенно ясный смысл: если множества A и B не пересекаются (т. е. $AB = O$), то число элементов, содержащихся в их сумме $A + B$, получается просто сложением числа k элементов множества A и числа l элементов множества B; поэтому

$$|A + B| = (k + l)/N = k/N + l/N = |A| + |B|.$$

Таким образом, наша булева структура с определенной таким образом нормой элементов является *нормированной* булевой структурой.

Приведенное определение нормы $|A|$ подмножества A универсального множества I можно еще обобщить. Предположим, что отдельные элементы $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_N$ множества I имеют разный «вес», или «цену». Так, в рассматривавшемся выше примере множества шахматных фигур часто оказывается естественным считать, что «цена» различных фигур различна; например, при попытках «обучить» шахматной игре электронную вычислительную машину иногда полагают, что цена слона или коня примерно в 3 раза больше цены пешки, цена ладьи — в 4—5 раз больше цены пешки, цена ферзя больше цены пешки в 8—9 раз, а король стоит несравненно больше, чем пешка, скажем, он оценивается в 1000 пешек (что заставляет каждого из соперников бросать все силы на защиту своего короля, ибо он стоит несравненно больше всех остальных фигур вместе взятых). Пусть цена (вес) отдельных элементов $\alpha_1, \alpha_2, \ldots, \alpha_N$ множества I задается неотрицательными числами $t_1, t_2, \ldots, t_N$; при этом нам удобно будет выбрать такую «единицу измерения цен», что

$$t_1 + t_2 + \ldots + t_N = 1.$$

Если теперь положить

$$|A| = |\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_n}\}| = t_{i_1} + t_{i_2} + \ldots + t_{i_n},$$

где $i_1, i_2, \ldots, i_n$—это какие-то из чисел $1, 2, \ldots, N$, то мы превратим алгебру подмножеств множества I в нормированную булеву структуру. [Это определение норм подмножеств I переходит в предыдущее, если положить $t_1 = t_2 = \ldots = t_N = 1/N$.]

4. Близка к модели 3 и следующая модель. Будем по-прежнему считать, что булева структура — это алгебра подмножеств множества I; только теперь примем за универсальное множество I, скажем, единичный квадрат, так что всевозможные подмножества I — это некоторые фигуры, расположенные внутри квадрата. За норму (абсолютную величину) множества A мы примем *площадь* фигуры A [1]. Ясно, что при этом удовлетворяется аксиома H_1. Аксиома H_2 здесь означает, что если некоторая фигура $C = A + B$ разбивается на непересекающиеся (ибо $AB = O$!) части A и B, то ее площадь равна сумме площадей фигур A и B. Таким образом, наложенные на норму условия имеют в этом случае чрезвычайно простой смысл, близкий к тем условиям, которые определяют площадь фигуры (ср. [17]). Алгебра подмножеств квадрата I превращается при таком выборе нормы в *нормированную* булеву структуру. Разумеется, почти ничего не изменилось бы также, если бы роль универсального множества I играл не единичный квадрат, а какая-либо другая фигура, площадь которой равна S; только в этом случае норму фигуры A следовало бы определить как ее площадь, деленную на число S (т. е. как долю, которую вносит фигура A в общую площадь I). Точно так же, если принять за I какое-либо трехмерное тело, то под нормой его подмножества A естественно понимать *объем* A (деленный, в случае необходимости, на общий объем I).

Этот пример также допускает существенное обобщение. Предположим, что тело I представляет собой плоскую пластинку (т. е. тонкую материальную пластинку постоянной небольшой толщины), изготовленную из произвольного неоднородного материала. Удельный вес этого материала в точке $M = (x, y)$ (т. е. вес, приходящийся на единицу площади) пусть задается некоторой (неотрицательной!) функцией $f(M) = f(x, y)$. Примем за норму $|A|$ подмножества A *вес* части A пластинки I; этот же вес определяется с помощью интеграла

$$|A| \quad \int_A f(M)\, ds = \iint_A f(x, y)\, dx dy, \tag{13.5}$$

где ds — элемент площади пластинки в точке M; при этом единицу измерения веса следует выбрать так, чтобы вес всей пластинки I был равен единице, т. е. чтобы было

$$\int_I f(M)\, ds = \iint_I f(x, y)\, dx dy = 1. \tag{13.5'}$$

Нетрудно понять, что норма, определенная таким образом (с помощью совершенно произвольной неотрицательной функции $f(x, y)$, удовлетворяющей лишь одному условию нормировки (5′)), превращает булеву структуру фигур A в нормированную структуру Буля.

Аналогично можно построить и нормированную булеву структуру, элементами которой являются области, заключенные внутри трехмерного тела I, считая это тело изготовленным из неоднородного материала и принимая за норму области ее вес.

---

[1] При этом следует только потребовать, чтобы все рассматриваемые фигуры A были *квадрируемыми*, т. е. имели площадь (ср., например, [16, с. 204]).

5. Пусть элементами булевой структуры являются всевозможные *делители* натурального числа N, а «сумма» и «произведение» чисел определяются как их *наименьшее общее кратное* и *наибольший общий делитель* (см. модель 3 на с. 92). В таком случае за норму $|a|$ числа a можно принять *логарифм* этого числа, точнее, положить

$$|a| = \log a/\log N, \tag{13.6}$$

поскольку мы требуем, чтобы норма числа N (играющего роль элемента ι булевой структуры) была равна единице [1]. В самом деле, в этом случае, очевидно, выполняется аксиома H_1. Далее, условие $a \otimes b=(a, b)=1$ (роль элемента о нашей булевой структуры играет число 1!) означает, что числа a и b взаимно просты; но в этом случае

$$a \oplus b = [a, b] = ab$$

и, следовательно,

$$\log (a \oplus b) = \log (ab) = \log a + \log b,$$

т. е.

$$|a \oplus b| = |a| + |b|.$$

Тем самым доказано, что и аксиома H_2 нормы здесь выполняется. Таким образом, и в этом случае мы естественно приходим к нормированной структуре Буля, — что проливает новый свет на само понятие логарифма (натурального) числа.

При рассмотрении модели 3 из § 10 мы дополнительно требовали, чтобы *каноническое разложение* $N = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ числа N не содержало квадратов, т. е. чтобы N имело вид $N = p_1 p_2 \ldots p_k$, где $p_1, p_2, \ldots, p_k$ — попарно различные простые числа. Отказ от этого последнего условия приводил к структуре, весьма близкой к булевой, но все же несколько отличающейся от нее, поскольку условия (аксиомы) (VIII) § 5 могут здесь и не иметь места; подобные системы мы назвали *неполными булевыми структурами*. При этом отказ от условий (VIII) нисколько не препятствует определению нормы $|\alpha|$ элемента α структуры. Неполную структуру Буля, для каждого элемента α которой определена норма $|\alpha|$, удовлетворяющая аксиомам H_1 и H_2, можно назвать *нормированной неполной булевой структурой*. Пример нормированной неполной структуры Буля доставляет множество всевозможных

---

[1] Выбор основания системы логарифмов здесь не играет роли, ибо отношение $\log a/\log N$ не зависит от выбора системы логарифмов — переход от логарифмов по основанию b к логарифмам по основанию c сводится лишь к умножению всех логарифмов на постоянный множитель (модуль перехода) $\log_c b$: $\log_c M = \log_c b \cdot \log_b M$.

Вместо равенства $|a| = \log a : \log N$ можно также писать $|a| = \log_N a$ (ибо тогда $|\iota| = \log_N N = 1$).

делителей a натурального числа $N = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ (где $n_1 n_2 \dots n_k > 1$, т. е. хоть один из показателей $n_1, n_2, \dots, n_k$ больше единицы) с нормой (6).

6. Еще один пример неполной булевой структуры мы получим, приняв за элементы этой структуры множество вещественных чисел a, где, скажем, $0 \leqslant a \leqslant 1$, и положив $a \oplus b = \max(a, b)$, $a \otimes b = \min(a, b)$, $\bar{a} = 1 - a$ и, кроме того, $o = 0$, $\iota = 1$ и $a \supset b$, если $a \geqslant b$ (см. модель 4 на с. 97). Эту неполную структуру Буля также легко превратить в нормированную, положив $|a| = a$. При этом аксиома H_1 нормы выполняется очевидным образом. Аксиома же H_2 вытекает из того, что здесь $a \otimes b = 0$, лишь если один из элементов a или b совпадает с 0; но, если, скажем, $b = 0$, то, очевидно,

$$a \oplus b = a \text{ и } |a \oplus b| = |a| = |a| + 0 = |a| + |b|.$$

7. Вот еще более далекая от нашей основной темы, но при том достаточно поучительная модель. Рассмотрим *решетку с дополнениями*, образованную связкой $\mathcal{S}$ прямых и плоскостей обычного (трехмерного) пространства R с центром O (точка O и пространство R также причисляются к числу элементов $\mathcal{S}$) или, общée, множество $\mathcal{S}_n$ всевозможных линейных подпространств n-мерного векторного пространства (см. модель 5 на с. 99). Норму $|z|$ элемента z этой решетки мы определим как его *размерность*, которую еще надо разделить на размерность (n или 3) всего пространства, если мы хотим, чтобы единичный элемент ι решетки (все пространство) имел норму 1. Так, например, в случае связки $\mathcal{S} = \mathcal{S}_3$ прямых и плоскостей обычного пространства положим:

$$|z| = \begin{cases} 0, \text{ если } z \text{ совпадает с точкой } O \\ 1/3, \text{ если } z \text{ есть прямая}, \\ 2/3, \text{ если } z \text{ есть плоскость}, \\ 1, \text{ если } z \text{ совпадает со всем пространством } R. \end{cases}$$

При этом очевидным образом выполняется аксиома H_1 нормы. Далее, если $zt = O$, то сумма $z + t$ представляет собой плоскость, когда z и t — две прямые, и все пространство R, когда один из элементов z и t представляет собой плоскость, а другой — прямую; отсюда вытекает, что и аксиома H_2 нормы здесь имеет место (ср. ниже упр.4). Таким образом, и в этом случае удается ввести естественную норму элементов решетки, удовлетворяющую аксиомам H_1 и H_2,— что превращает связку $\mathcal{S}_3$ (или $\mathcal{S}_n$) в *нормированную решетку с дополнениями.*

Еще две модели нормированной булевой структуры, специально связанные с разобранными в § 11 и 12 моделями, мы рассмотрим в § 14.

Перейдем теперь к выводу дальнейших свойств норм, которые можно установить, исходя из аксиом H_1 и H_2. Прежде всего, из равенства (3) и условия $|\iota| = 1$ (см. H_1) вытекает

$$|\bar{\alpha}| = 1 - |\alpha| \text{ для всех } \alpha \in \mathcal{B}. \tag{13.7}$$

Далее, как нетрудно видеть,

$$\text{если } \alpha \supset \beta, \text{ то } |\alpha| \geqslant |\beta|. \qquad (13.8)$$

◀ Для любых α, $\beta \in \mathscr{B}$, где $\alpha \supset \beta$, существует такой элемент ξ («прямая разность» элементов α и β), что

$$\alpha = \beta + \xi, \quad \beta\xi = o$$

(см. с. 39; элемент ξ мы обозначали символом $\alpha - \beta$). Поэтому

$$|\alpha| = |\beta + \xi| = |\beta| + |\xi| \geqslant |\beta|,$$

— что и требовалось доказать. ▶

Далее, для любых α, $\beta \in \mathscr{B}$

$$|\alpha + \beta| = |\alpha| + |\beta| - |\alpha\beta|. \qquad (13.9)$$

◀ Из факта существования «(прямой) разности» $\gamma - \delta$ элементов γ и δ, где $\gamma \supset \delta$, вытекает справедливое для любых α, $\beta \in \mathscr{B}$ равенство

$$(\alpha + \beta) = \alpha + (\beta - \alpha\beta),$$

где $\beta - \alpha\beta = \eta$ $(= (\alpha + \beta) - \alpha)$ таково, что $\alpha\eta = o$; кроме того,

$$\beta = \alpha\beta + \eta, \text{ а } (\alpha\beta)\eta = o$$

(см. упр. 1). Отсюда в силу H_2

$$|\alpha + \beta| = |\alpha| + |\eta| \text{ и } |\beta| = |\alpha\beta| + |\eta|.$$

Вычитая почленно последние два равенства (связывающие некоторые ч и с л а), мы и получим (9). ▶

Так, если $|A|$ и $|B|$ суть площади двух фигур A и B (см. модель 4, с. 143), то в сумме $|A| + |B|$ площадь пересечения AB засчитывается два раза (рис. 67,*а*); поэтому

$$|A + B| = |A| + |B| - |AB|.$$

Аналогично, если z и t—два подпространства векторного пространства R *размерностей* p и q, а u и v — их («векторная») сумма (т. е. наименьшее подпространство R, содержащее как z, так и t) и пересечение, то размерности h и d подпространств u и v связаны соотношением

$$|u| = |z| + |t| - |v| \text{ или } \frac{h}{n} = \frac{p}{n} + \frac{q}{n} - \frac{d}{n} \qquad (13.10)$$

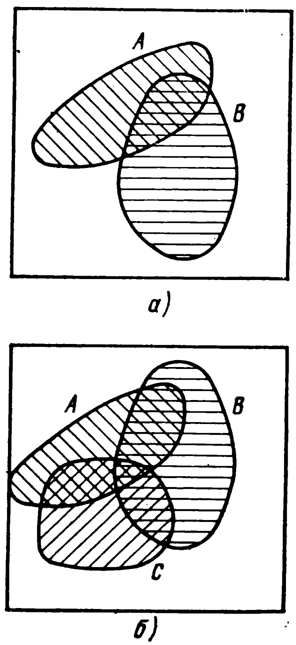


Рис. 67

(см. модель 7 на с. 146; заметьте, что вывод формулы (9) не опирается на дистрибутивные законы (III) и потому применим и к решетке линейных подпространств векторного пространства!), т. е.

$$d + h = p + q. \tag{13.10'}$$

Эта формула часто используется в теории векторных пространств.

Пример. В группе имеется 22 студента; 10 из них умеют играть в шахматы, 8 — в шашки; и в шахматы, и в шашки играют 3 студента. Сколько студентов не умеют играть ни в шахматы, ни в шашки?

◀ Обозначим множество студентов, умеющих играть в шахматы, символом *Шах*, а множество студентов, умеющих играть в шашки, — символом *Шаш*. Нам надо определить число студентов в множестве

$$\overline{Шах}\cdot\overline{Шаш} = \overline{Шах + Шаш}$$

(см. правило де Моргана (XIa)). Но так как здесь естественно считать (ср. модель 3 на с. 142):

$$|Шах| = \frac{10}{22}, \quad |Шаш| = \frac{8}{22} \text{ и } |Шах\cdot Шаш| = \frac{3}{22},$$

то в силу (9)

$$|Шах + Шаш| = |Шах| + |Шаш| - |Шах\cdot Шаш| =$$
$$= \frac{10}{22} + \frac{8}{22} - \frac{3}{22} = \frac{15}{22}$$

и, следовательно (см. формулу (7)),

$$|\overline{Шах}\ \ \overline{Шаш}| = |\overline{Шах + Шаш}| = 1 - |Шах + Шаш| =$$
$$= 1 - \frac{15}{22} = \frac{7}{22}.$$

Таким образом, не умеют играть ни в шахматы, ни в шашки 7 студентов. ▶

Ясно, что равенство (9) представляет собой обобщение аксиомы H_2 нормы; при $\alpha\beta = o$ оно переходит в аксиому H_2. Из (9) следует также, что для любых элементов α и β нормированной булевой структуры **B**

$$|\alpha + \beta| \leqslant |\alpha| + |\beta| \tag{13.11}$$

— это свойство абсолютных величин элементов $\mathscr{B}$ аналогично известному свойству абсолютных величин чисел. С помощью метода математической индукции из (11) без труда выводится (см. упр. 3 а)), что при любом n

$$|\alpha_1 + \alpha_2 + \ldots \alpha_n| \leqslant |\alpha_1| + |\alpha_2| + \ldots + |\alpha_n|, \tag{13.11'}$$

где равенство достигается лишь в том случае, если все $|\alpha_i\alpha_j| = o$ (где $i \neq j$, $i, j = 1, 2, \ldots, n$).

Аналогично переходу от (11) к (11′) можно обобщить и формулу (9). ◀ Рассмотрим, для начала, три элемента $\alpha_1, \alpha_2, \alpha_3$ нормированной булевой структуры **B**. В силу (9) имеем

$$|\alpha_1 + \alpha_2 + \alpha_3| = |\alpha_1 + (\alpha_2 + \alpha_3)| = |\alpha_1| + |\alpha_2 + \alpha_3| - |\alpha_1 (\alpha_2 + \alpha_3)| = |\alpha_1| + (|\alpha_2| + |\alpha_3| - |\alpha_2\alpha_3|) - |\alpha_1\alpha_2 + \alpha_1\alpha_3| = |\alpha_1| + |\alpha_2| + |\alpha_3| - |\alpha_2\alpha_3| - (|\alpha_1\alpha_2| + |\alpha_1\alpha_3| - |(\alpha_1\alpha_2)(\alpha_1\alpha_3)|) = |\alpha_1| + |\alpha_2| + |\alpha_3| - |\alpha_1\alpha_2| - |\alpha_1\alpha_3| - |\alpha_2\alpha_3| + |\alpha_1\alpha_2\alpha_3|, \qquad (13.9')$$

ибо, очевидно, $(\alpha_1\alpha_2)(\alpha_1\alpha_3) = (\alpha_1\alpha_1)\alpha_2\alpha_3 = \alpha_1\alpha_2\alpha_3$.

Подобно этому доказывается, что

$$\begin{aligned}
&|\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4| = |\alpha_1 + (\alpha_2 + \alpha_3 + \alpha_4)| = \\
&= |\alpha_1| + |\alpha_2 + \alpha_3 + \alpha_4| - |\alpha_1 (\alpha_2 + \alpha_3 + \alpha_4)| = \\
&= |\alpha_1| + (|\alpha_2| + |\alpha_3| + |\alpha_4| - |\alpha_2\alpha_3| - \\
&- |\alpha_2\alpha_4| - |\alpha_3\alpha_4| + |\alpha_2\alpha_3\alpha_4|) - \\
&- |(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4)| = \\
&= |\alpha_1| + |\alpha_2| + |\alpha_3| + |\alpha_4| - |\alpha_2\alpha_3| - \\
&- |\alpha_2\alpha_4| - |\alpha_3\alpha_4| + |\alpha_2\alpha_3\alpha_4| - \\
&- (|\alpha_1\alpha_2| + |\alpha_1\alpha_3| + |\alpha_1\alpha_4| - \\
&- |(\alpha_1\alpha_2)(\alpha_1\alpha_3)| - |(\alpha_1\alpha_2)(\alpha_1\alpha_4)| - \\
&- |(\alpha_1\alpha_3)(\alpha_1\alpha_4)| + |(\alpha_1\alpha_2)(\alpha_1\alpha_3)(\alpha_1\alpha_4)|) = \\
&= |\alpha_1| + |\alpha_2| + |\alpha_3| + |\alpha_4| - \\
&- |\alpha_1\alpha_2| - |\alpha_1\alpha_3| - |\alpha_1\alpha_4| - |\alpha_2\alpha_3| - \\
&- |\alpha_2\alpha_4| - |\alpha_3\alpha_4| + |\alpha_1\alpha_2\alpha_3| + |\alpha_1\alpha_2\alpha_4| + \\
&+ |\alpha_1\alpha_3\alpha_4| + |\alpha_2\alpha_3\alpha_4| - |\alpha_1\alpha_2\alpha_3\alpha_4|. \qquad (13.9'')
\end{aligned}$$

Выводы формул (9′), (9″) базируются на следующей идее. Ясно, что $|\alpha_1 + \alpha_2 + \alpha_3| \leqslant |\alpha_1| + |\alpha_2| + |\alpha_3|$; однако равенство здесь, вообще говоря, места иметь не будет, ибо, интерпретируя норму элемента α булевой структуры как площадь фигуры α, мы в сумме $|\alpha_1| + |\alpha_2| + |\alpha_3|$ учитываем дважды все площади $|\alpha_1\alpha_2|$, $|\alpha_1\alpha_3|$, $|\alpha_2\alpha_3|$ попарных пересечений фигур (рис. 67,*б*). Поэтому для того, чтобы оценить величину $|\alpha_1 + \alpha_2 + \alpha_3|$, нам надо исключить эти «двукратные вхождения», т. е. вычесть из суммы $|\alpha_1| + \ldots + |\alpha_3|$ сумму $|\alpha_1\alpha_2| + \ldots + |\alpha_2\alpha_3|$. Но теперь оказывается, что мы даже «перестарались»: в самом деле, мы полностью исключили тройное пересечение $\alpha_1\alpha_2\alpha_3$, площадь $|\alpha_1\alpha_2\alpha_3|$ которого трижды фигурирует в сумме $|\alpha_1| + \ldots$ (часть $\alpha_1\alpha_2\alpha_3$ входит в каждое из трех слагаемых) и трижды — в сумме $|\alpha_1\alpha_2| + \ldots$ (она входит и в каждое из парных пересечений), в результате чего величина $|\alpha_1\alpha_2\alpha_3|$ нами никак не учитывается. Поэтому «тройное вхождение» $|\alpha_1\alpha_2\alpha_3|$ надо дополнительно включить (прибавить к выражению $|\alpha_1| + \ldots - |\alpha_1\alpha_2| - \ldots$), что и дает результат (9′). Так же можно получить и формулу (9″). ▶

Та же идея (или прямое использование метода математической индукции — см. ниже упр. 2б)) приводит к следующей общей формуле включений и исключений:

$$|\alpha_1+\alpha_2+\alpha_3+\ldots+\alpha_n| = \sum_i |\alpha_i| - \sum_{(i_1,\, i_2)} |\alpha_{i_1}\alpha_{i_2}| +$$

$$+ \sum_{(i_1,\, i_2,\, i_3)} |\alpha_{i_1}\alpha_{i_2}\alpha_{i_3}| - \ldots + (-1)^{n-2} \sum_{(i_1,\, i_2,\ldots,\, i_{n-1})} |\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_{n-1}}| +$$

$$+(-1)^{n-1}|\alpha_1\alpha_2\ldots\alpha_n|, \tag{13.12}$$

где символ $(i_1, i_2, \ldots, i_k)$ под знаком суммирования означает, что сумма распространена на всевозможные *сочетания* индексов $i_1, i_2, \ldots, i_k$, каждый из которых может быть равен $1, 2, 3, \ldots$ или n (здесь $k=1, 2, \ldots$ $\ldots, n$ и сумма $\sum\limits_{(i_1,\, i_2,\, \ldots,\, i_n)}$ содержит всего одно слагаемое, из-за чего последнее выражение в (12) справа не содержит знака суммы).

Приведем ряд примеров, иллюстрирующих разнообразные применения формулы включений и исключений (12) (по поводу дальнейших примеров, см., скажем, [18]).

Пример 1. При обследовании сотрудников некоторого научного учреждения выяснилось, что 60% из них могут читать английскую специальную литературу, 30% — французскую, 20% — немецкую, 15% — и английскую, и французскую, 5% — английскую и немецкую, 2% — французскую и немецкую и 1% может читать на всех трех языках. Спрашивается, каков процент сотрудников, не способных читать ни на одном из трех языков?

◀ Обозначим множества сотрудников, владеющих (в смысле этого примера) соответственно английским, французским и немецким языками через $а$, $ф$ и $н$. В силу формулы (9′) (см. модель 3, с. 142)

$$|а+ф+н| = |а| + |ф| + |н| - |аф| - |ан| - |фн| + |афн| =$$

$$= 60\% + 30\% + 20\% - 15\% - 5\% - 2\% + 1\% = 89\%.$$

Таким образом (см. правило (XIа) и упр. 2.4а), а также соотношение (7)),

$$|\bar{а}\cdot\bar{ф}\cdot\bar{н}| = |\overline{а+ф+н}| = 1 - |а+ф+н| = 100\% - 89\% =$$

$$= 11\%! ▶$$

Пример 2. Чему равна площадь пересечения кругов радиуса a, центрами которых служат вершины: 1) равностороннего треугольника со стороной a, 2) квадрата со стороной a?

◀ 1) Изображенная на рис. 68, *а* фигура[1] представляет собой, очевидно, объединение $s_1+s_2+s_3$ трех секторов радиуса a с центрами A_1, A_2, A_3, центральным углом $\pi/3$ и площадью $\pi a^2/6$ (сектор s_1 заштрихован на рис. 68,*а*); пересечением любых двух из этих секторов, так же как и их тройным пересечением, является $\Delta A_1A_2A_3$ площади $a^2\sqrt{3}/4$. Отсюда имеем (см. модель 4 на с. 143 и формулу (9′)):

$$(s_1+s_2+s_3)=|s_1|+|s_2|+|s_3|-|s_1s_2|-|s_1s_3|-|s_2s_3|+|s_1s_2s_3|=$$

$$=3\frac{\pi}{6}a^2-3\frac{a^2\sqrt{3}}{4}+\frac{a^2\sqrt{3}}{4}=\frac{\pi-\sqrt{3}}{2}a^2.$$

2) Пусть S_1, S_2, S_3, S_4 — фигурирующие на рис. 68,*б* секторы радиуса a с центрами A_1, A_2, A_3, A_4, центральным углом $\pi/2$ и площадью $\pi a^2/4$; нам надо определить $|S_1S_2S_3S_4|$. Но по формуле (9″) (см. также ниже упр. 3)

$$|S_1S_2S_3S_4| = |S_1|+|S_2|+|S_3|+|S_4|-$$
$$-|S_1S_2|-\ldots-|S_3S_4|+|S_1S_2S_3|+\ldots$$
$$\ldots+|S_2S_3S_4|-|S_1+S_2+S_3+S_4|; \qquad (13.13)$$

поэтому надо лишь найти все фигурирующие в правой части (13) величины. Но $|S_1|=\ldots=|S_4|=\pi a^2/4$ и $|S_1+\ldots+|S_4|=a^2$ (ибо объединение четырех секторов — это полный квадрат *I*); остается определить площади двойных и тройных пересечений секторов.

Ясно, что фигура S_1S_2 отличается от изображенного на рис. 68,*а* треугольника Рело лишь отсутствием «нижнего» сегмента — это есть объединение двух секторов s_1 и s_2, а не трех таких секторов. Поэтому

$$|S_1S_2|=|S_2S_3|=|S_3S_4|=|S_4S_1|=$$

$$=|s_1+s_2|=|s_1|+|s_2|-|s_1s_2|=$$

$$=2\frac{\pi}{6}a^2-\frac{a^2\sqrt{3}}{4}=\frac{4\pi-3\sqrt{3}}{12}a^2.$$

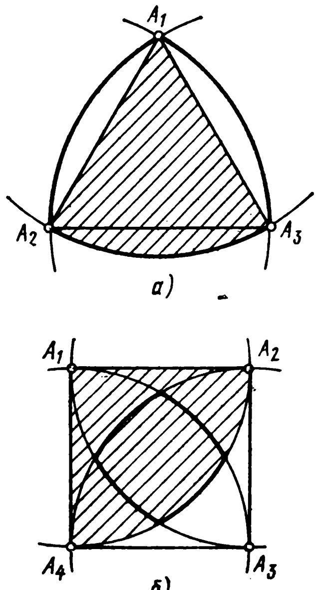


Рис. 68

[1] По имени швейцарского механика XIX в. Франсуа Рело (F. Reuleaux), впервые изучившего замечательные свойства этой фигуры, изображенный на рис. 68, *а* криволинейный треугольник называется *треугольником Рело* (об этой фигуре см., например, § 7 книги [19]).

Далее $|S_1 + S_3|$ есть весь квадрат I площади a^2; поэтому (ср. с тем же упр. 3):

$$|S_1S_3| = |S_2S_4| = |S_1| + |S_3| - |S_1 + S_3| =$$
$$= 2\frac{\pi}{4}a^2 - a^2 = \frac{\pi-2}{2}a^2.$$

Наконец, как легко видеть, в силу (9) (ср. гл. 1)

$$|S_1S_2S_3| + |S_1S_3S_4| = |S_1S_2S_3 + S_1S_3S_4| + |S_1S_2S_3 \cdot S_1S_3S_4| =$$
$$= |S_1S_3(S_2 + S_4)| + |S_1S_2S_3S_4| = |S_1S_3I| + |S_1S_2S_3S_4| =$$
$$= |S_1S_3| + |S_1S_2S_3S_4| = \frac{\pi-2}{2}a^2 + |S_1S_2S_3S_4|,$$

откуда с очевидностью вытекает, что

$$|S_1S_2S_3| + \ldots + |S_2S_3S_4| = 2\left[\frac{\pi-2}{2}a^2 + |S_1S_2S_3S_4|\right] =$$
$$= (\pi-2)a^2 + 2|S_1S_2S_3S_4|.$$

Подставляя все эти результаты в (13), находим

$$|S_1S_2S_3S_4| = 4\frac{\pi}{4}a^2 - 4\frac{4\pi - 3\sqrt{3}}{12}a^2 - 2\frac{\pi-2}{2}a^2 +$$
$$+ (\pi-2)a^2 + 2|S_1S_2S_3S_4| - a^2,$$

откуда

$$|S_1S_2S_3S_4| = -\pi a^2 + \left(\frac{4}{3}\pi - \sqrt{3}\right)a^2 + (\pi-2)a^2 - (\pi-2)a^2 + a^2 =$$
$$= \left(\frac{1}{3}\pi + 1 - \sqrt{3}\right)a^2. \blacktriangleright$$

Пример 3 (см. [20], задача 89). В классе 25 учеников. 17 из них умеют ездить на велосипеде, 13 умеют плавать и 8 — ходить на лыжах. Ни один ученик не владеет сразу всеми тремя видами спорта, но как велосипедисты, так и пловцы и лыжники имеют хорошие или удовлетворительные оценки по математике, в то время как 6 учеников класса не успевают по математике. Сколько учеников класса имеют отличные оценки по математике? Сколько пловцов умеют ходить на лыжах?

◀ Обозначим множества учеников, умеющих ездить на Велосипеде, Плавать и ходить на Лыжах, буквами *В*, *П* и *Л*; далее обозначим множества Отличников, Успевающих по математике учеников (имеющих оценку «3» или «4») и Неуспевающих учеников буквами *О*, *У* и *Н*.

В таком случае условия задачи могут быть записаны в следующем виде:

1) $|В| = 17/25$, $|П| = 13/25$, $|Л| = 8/25$;

2) $|ВПЛ| = 0$;

3) $|УВ| = |В|$, $|УП| = |П|$, $|УЛ| = |Л|$;

4) $|Н| = 6/25$;

в задаче требуется определить величины $|О|$ и $|ПЛ|$.

Очевидно,

$$|О| + |У| + |Н| = |О + У + Н| = |I| = 1;$$

следовательно,

$$|О| + |У| = 1 - |Н| = 1 - 6/25 = 19/25.$$

С другой стороны, если $У_0$, $У_1$ и $У_2$ — множества успевающих учеников, не владеющих ни одним видом спорта, владеющих одним или двумя видами спорта соответственно (напоминаем, что тремя видами спорта не владеет ни один учащийся!), то

$$|У| = |У_0| + |У_1| + |У_2|;$$

таким образом, можно написать:

$$|О| + |У_0| + |У_1| + |У_2| = 19/25. \tag{13.14}$$

Но

$$|У_1| + |У_2| = |УВ + УП + УЛ| = |УВ| + |УП| + |УЛ| -$$
$$- |УВП| - |УВЛ| - |УПЛ| = |В| + |П| + |Л| - |УВП| -$$
$$- |УВЛ| - |УПЛ| = 17/25 + 13/25 + 8/25 - |У_2| = 38/25 - |У_2|$$

(здесь мы снова используем то, что никто из учащихся не владеет тремя видами спорта), т. е.

$$|У_1| + 2|У_2| = 38/25. \tag{13.14'}$$

Вычтем теперь из удвоенного равенства (14) равенство (14′). Мы получим

$$2|О| + 2|У_0| + |У_1| = 0.$$

Но сумма трех неотрицательных чисел может быть равна нулю лишь в том случае, если каждое из этих чисел равно нулю. Итак,

$$|О| = 0, \ |У_0| = 0, \ |У_1| = 0.$$

Далее остается только заметить, что условие $|У_1| = 0$ означает, что каждый из учащихся, владеющих хоть одним видом спорта, владеет еще одним видом спорта. Учитывая это, мы приходим к следующей системе уравнений:

$$17/25 = |В| = |ВП + ВЛ| = |ВП| + |ВЛ|,$$

$$13/25 = |П| = |ВП + ПЛ| = |ВП| + |ПЛ|$$

$$8/25 = |Л| = |ВЛ + ПЛ| = |ВЛ| + |ПЛ|;$$

из которой следует

$$|ВП| = \frac{11}{25}, \quad |ВЛ| = \frac{6}{25}, \quad |ПЛ| = \frac{2}{25}.$$

Итак, число учащихся, имеющих отличные оценки по математике, равно 0; число пловцов, умеющих ходить на лыжах, равно 2. ▶

Пример 4. На джинсах, общая поверхность которых равна 1, имеется 5 заплат, площадь каждой из которых не меньше $^1/_2$. Докажите, что найдутся две заплаты, площадь общей части которых не меньше $^1/_5$.

◀ Обозначим заплаты (подмножества джинсов I) через A_1, A_2, A_3, A_4 и A_5, их попарные пересечения — через A_{12}, A_{13} и т. д. Нам известно, что $|I| = 1$ и $|A_i| \geqslant 1/2$, где $i = 1, 2, 3, 4, 5$ (см. модель 4 на с. 143); требуется оценить величины $|A_{ij}|$. Согласно формуле (12) имеем

$$1 = |I| \geqslant |A_1 + A_2 + A_3 + A_4 + A_5| = \sum_{i=1}^{5} |A_i| - \sum_{(ij)} |A_{ij}| + \\ + \sum_{(ijk)} |A_{ijk}| - \sum_{(ijkl)} |A_{ijkl}| + |A_{12345}|$$

или

$$1 - \sum_{i} |A_i| + \sum_{(ij)} |A_{ij}| - \sum_{(ijk)} |A_{ijk}| + \sum_{(ijkl)} |A_{ijkl}| - |A_{12345}| \geqslant 0. \quad (13.15)$$

Из полученного неравенства надо исключить член $\Sigma|A_{ijk}|$ и последующие члены. Это можно сделать так. Используя ту же самую формулу (12), получаем

$$|A_1| \geqslant |A_{12} + A_{13} + A_{14} + A_{15}| = \sum_{i=2}^{5} |A_{1i}| - \sum_{(ij)} |A_{1ij}| + \\ + \sum_{(ijk)} |A_{1ijk}| - |A_{12345}|,$$

где индексы суммирования i, j, k пробегают значения 2, ..., 5. Выписав аналогичные неравенства для величин $|A_2|$, $|A_3|$, $|A_4|$ и $|A_5|$ и сложив все полученные неравенства, будем иметь

$$\sum_{i=1}^{5} |A_i| \geqslant 2 \sum_{(ij)} |A_{ij}| - 3 \sum_{(ijk)} |A_{ijk}| + 4 \sum_{(ijkl)} |A_{ijkl}| - 5|A_{12345}|,$$

или

$$\sum_i |A_i| - 2\sum_{(ij)} |A_{ij}| + 3\sum_{(ijk)} |A_{ijk}| - 4\sum_{(ijkl)} |A_{ijkl}| + $$
$$+ 5|A_{12345}| \geqslant 0. \tag{13.15'}$$

Умножим неравенство (15′) на $^1/_3$ и сложим его с неравенством (15). Из полученного неравенства выпадет выражение $\Sigma|A_{ijk}|$:

$$1 - \frac{2}{3}\sum_i |A_i| + \frac{1}{3}\sum_{(ij)} |A_{ij}| - \frac{1}{3}\sum_{(ijkl)} |A_{ijkl}| +$$
$$+ \frac{2}{3}|A_{12345}| \geqslant 0. \tag{13.16}$$

Но ясно, что каждая из пяти величин $|A_{1234}|$, $|A_{1235}|$, $|A_{1245}|$, $|A_{1345}|$ и $|A_{2345}|$ не меньше $|A_{12345}|$; поэтому

$$\sum_{(ijkl)} |A_{ijkl}| \geqslant 5|A_{12345}| \text{ и } \frac{1}{3}\sum_{(ijkl)} |A_{ijkl}| - \frac{2}{3}|A_{12345}| \geqslant |A_{12345}| \geqslant 0.$$

Следовательно, неравенство (16) можно переписать еще и так:

$$1 - \frac{2}{3}\sum_i |A_i| + \frac{1}{3}\sum_{ij} |A_{ij}| \geqslant 0, \tag{13.16'}$$

откуда получаем

$$\sum_{(ij)} |A_{ij}| \geqslant 2\sum_i |A_i| - 3 \geqslant 2\left(5 \cdot \frac{1}{2}\right) - 3 = 2.$$

А так как число слагаемых суммы $\sum_{(ij)} |A_{ij}|$ равно $C_5^2 = 10$, то хоть один из этих членов не меньше $2/10 = 1/5$,— что и требовалось доказать. ▶

Полученная оценка является точной. Этот результат можно значительно обобщить (ср. [21]; см. упр. 5).

Пример 5. Пусть $N = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ — некоторое целое положительное число ($p_1, p_2, \ldots, p_k$ — простые делители числа N). Определить число $\varphi(N)$ целых положительных чисел, не превосходящих числа N и взаимно простых с N. [Функция $\varphi(N)$ целого положительного аргумента N называется *функцией Эйлера*.]

◀ Обозначим множество целых положительных чисел m, где $1 \leqslant m \leqslant N$, делящихся на простое число p_i, через A_i, множество чисел m, делящихся на простые числа p_i и p_j,— через A_{ij} и т. д.; здесь $i, j \ldots = 1, 2, 3, \ldots$ или k. Нам надо определить число целых положительных чисел, не делящихся ни на одно из чисел $p_1, p_2, \ldots, p_k$, т. е. число элементов множества $\bar{A}_1 \bar{A}_2 \ldots \bar{A}_k = \overline{A_1 + A_2 + \ldots + A_k}$ (ср. упр. 2.4а)).

Очевидно, что (см. выше, модель 3, с. 142)

$$|A_i| = \frac{N}{p_i} : N = \frac{1}{p_i},\ |A_{ij}| = \frac{N}{p_i p_j} : N = \frac{1}{p_i p_j}$$

и т. д. Поэтому (см. формулу (12))

$$|A_1 + A_2 + \ldots A_k| = \sum_i |A_i| - \sum_{(ij)} |A_{ij}| + \sum_{(ijk)} |A_{ijk}| - \ldots +$$

$$+(-1)^{k-1} |A_{12\ldots k}| = \left(\frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_k}\right) - \left(\frac{1}{p_1 p_2} + \frac{1}{p_2 p_3} + \ldots\right.$$

$$\left.\ldots + \frac{1}{p_{k-1} p_k}\right) + \left(\frac{1}{p_1 p_2 p_3} + \ldots + \frac{1}{p_{k-2} p_{k-1} p_k}\right) - \ldots (-1)^{k-1} \frac{1}{p_1 p_2 \ldots p_k}$$

и, следовательно (см. (7)),

$$|\bar{A}_1 \cdot \bar{A}_2 \cdot \ldots \cdot \bar{A}_k| = |(\overline{A_1 + A_2 + \ldots + A_k})| = 1 - |A_1 + A_2 + \ldots A_k| = 1 -$$

$$-\left(\frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_k}\right) + \left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \ldots + \frac{1}{p_{k-1} p_k}\right) -$$

$$-\left(\frac{1}{p_1 p_2 p_3} + \ldots + \frac{1}{p_{k-2} p_{k-1} p_k}\right) + \ldots + (-1)^k \frac{1}{p_1 p_2 \ldots p_k} =$$

$$= (1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_k).$$

А так как

$$|\bar{A}_1 \bar{A}_2 \ldots \bar{A}_k| = \varphi(N)/N,$$

где $\varphi(N)$ — число элементов подмножества $\bar{A}_1 \cdot \bar{A}_2 \cdot \ldots \cdot \bar{A}_k$ множества $I = \{1, 2, 3, \ldots, N\}$, то окончательно получаем:

$$\varphi(N) = N \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right). \blacktriangleright \qquad (13.17)$$

Пример 6. Пусть $u_1, u_2, \ldots, u_k$ — линейные подпространства векторного пространства R размерностей $n_1, n_2, \ldots, n_k$; размерности попарных, тройных и т. д. пересечений этих пространств мы обозначим через $d_{12}, d_{13}, \ldots, d_{k-1,k}$; $d_{123}, d_{124}, \ldots, d_{k-2,k-1,k}$ и т. д. Требуется определить размерность h наименьшего линейного подпространства U, содержащего $u_1, u_2, \ldots, u_k$.

◀ Применим формулу (12) (ср. со сказанным на с. 148 по поводу формулы (10)) к нормированной решетке подпространств векторного пространства (модель 7). Мы получим

$$h = n_1 + n_2 + \ldots + n_k - d_{12} - d_{13} - \ldots - d_{k-1,k} +$$

$$+ d_{123} + d_{124} + \ldots + d_{k-2,k-1,k} - \ldots \pm d_{123\ldots k}$$

(ср. с формулой (10′) на с. 148). ▶

Пример 7. Пусть $a_1, a_2, \ldots, a_n$ — какие угодно целые положительные числа. Как, зная эти числа, а также общие наибольшие делители всевозможных комбинаций этих чисел, найти их общее наименьшее кратное?

◀ Здесь нам придется воспользоваться нормированной неполной булевой структурой, составляющей содержание рассмотренной выше (с. 145) модели 5. Для этой структуры не выполняются правила (VIII) «полной» булевой структуры; поэтому неприменимы никакие следствия из этих правил, скажем, формула (7). Однако вывод «формулы включений и исключений» (12) не зависит от аксиом (VIII) булевой структуры; поэтому формула (12) применима и к нормированным неполным булевым структурам.

Пусть теперь $a_1, a_2, a_3, \ldots, a_n$ — какие угодно различные целые положительные числа, которые, естественно, всегда можно рассматривать как делители некоторого большого числа N (например, числа $N = a_1 a_2 a_3 \ldots a_n$). В силу формулы (12) имеем:

$$|a_1 \oplus a_2 \oplus a_3 \oplus \ldots \oplus a_n| = \sum_i |a_i| - \sum_{(ij)} |a_i \otimes a_j| + \sum_{(ijk)} |a_i \otimes a_j \otimes a_k| -$$
$$- \ldots + (-1)^{n-1} |a_1 \otimes a_2 \otimes a_3 \otimes \ldots \otimes a_n|$$

или.

$$\frac{\log\,[a_1, a_2, a_3, \ldots, a_n]}{\log N} = \sum_i \frac{\log a_i}{\log N} - \sum_{(ij)} \frac{\log\,(a_i, a_j)}{\log N} +$$
$$+ \sum_{(ijk)} \frac{\log\,(a_i, a_j, a_k)}{\log N} - \ldots + (-1)^{n-1} \frac{\log\,(a_1, a_2, a_3, \ldots, a_n)}{\log N}.$$

Умножая обе части последнего равенства на $\log N$ и потенцируя, получаем:

$$[a_1, a_2, a_3, \ldots, a_n] = a_1 a_2 \ldots a_n\,(a_1, a_2)^{-1}\,(a_1, a_3)^{-1} \ldots (a_{n-1}, a_n)^{-1} \times$$
$$\times (a_1, a_2, a_3)\,(a_1, a_2, a_4) \ldots (a_{n-2}, a_{n-1}, a_n) \ldots (a_1, a_2, a_3, \ldots, a_n)^{\pm 1}.$$

Так, например,

$$[10, 12, 30, 75] = \frac{10 \cdot 12 \cdot 30 \cdot 75 \cdot (10, 12, 30)\,(10, 12, 75)\,(10, 30, 75)\,(12, 30, 75)}{(10, 12)\,(10, 30)\,(10, 75)\,(12, 30)\,(12, 75)\,(30, 75)\,(10, 12, 30, 75)} =$$
$$= \frac{10 \cdot 12 \cdot 30 \cdot 75 \cdot 2 \cdot 1 \cdot 5 \cdot 3}{2 \cdot 10 \cdot 5 \cdot 6 \cdot 3 \cdot 15 \cdot 1} = 300. \blacktriangleright$$

Пример 8. Пусть $a_1, a_2, \ldots, a_k$ — произвольные неотрицательные числа. Доказать, что

$$\max\,(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \ldots + a_k -$$
$$- \min\,(a_1, a_2) - \min\,(a_1, a_3) - \ldots - \min\,(a_{k-1}, a_k) + \min\,(a_1, a_2, a_3) +$$
$$+ \ldots + \min\,(a_{k-2}, a_{k-1}, a_k) - \ldots \pm \min\,(a_1, a_2, \ldots, a_k).$$

◀ Определим норму элемента неполной структуры Буля, образованной системой вещественных чисел (см. модель 4 из § 10), по формуле $|a| = a$ (см. выше модель 6). Далее нам остается только применить в этом случае формулу (12) (разумеется, вместо заданных чисел a_1, $a_2, \ldots, a_k$ мы всегда можем рассмотреть числа $a_1' = a_1/N$, $a_2' = a_2/N, \ldots, a_k' = a_k/N$, где N таково, что $0 \leqslant a_i \leqslant 1$ при всех $i = 1, 2, \ldots, k$). ▶

Заметим еще в заключение, что вопрос о возможных способах введения меры в алгебре делителей целого числа N (см. выше модель 5) сводится к задаче определения таких функций $f(a)$ целых положительных чисел a, что для взаимно простых чисел a и b (т. е. таких, что $a \otimes b = (a, b) = 1$) имеет место равенство $f(a \oplus b) = f[a, b] = f(ab) = f(a) + f(b)$ (логарифм $\log a$ числа a является лишь одной из подобных функций). Этот вопрос тесно связан с вопросом о *мультипликативных функциях* целых чисел, т. е. таких функциях $F(a)$, что при $(a, b) = 1$ имеет место равенство $F(ab) = F(a) F(b)$. Мультипликативные функции играют заметную роль в теории чисел (см., например, [22, гл. II]). К их числу принадлежат: a^c (где c произвольно); сумма всех делителей числа a; сумма s-х степеней всех делителей a; число c^k, где c произвольно, $k = k(a)$ — число различных простых делителей числа a; функция Эйлера $\varphi(a)$ (см. выше, пример 5) и т. д.; логарифм любой из этих функций [например, число $\log \varphi(a)$ или число $k(a)$], взятый с некоторым постоянным множителем, может быть принят за норму $|a|$ числа a.

Упражнения. 13.1. Докажите совпадение «прямых разностей» $\xi = \beta - \alpha\beta$ и $\xi_1 = (\alpha + \beta) - \alpha$ при любых $\alpha, \beta \in \mathscr{B}$.

13.2. Докажите:

а) формулу (11′); б) формулу включений и исключений (12).

13.3. Как, зная меры $|\alpha_i|$, $|\alpha_i + \alpha_j|$, $|\alpha_i + \alpha_j + \alpha_k|, \ldots$ (где $i, j, k, \ldots \ldots = 1, 2, \ldots, n$) всевозможных сумм элементов $\alpha_1, \alpha_2, \ldots, \alpha_n$ нормированной булевой структуры, найти норму произведения $|\alpha_1, \alpha_2 \ldots \alpha_n|$?

13.4. Докажите, что определение: $|z| = \dim z/n$, где $\dim z$ — размерность линейного подпространства z n-мерного векторного пространства R, обращает решетку линейных подпространств пространства R в нормированную решетку, т. е. что так введенная величина $|z|$ удовлетворяет аксиомам H_1 и H_2 нормы.

13.5. Внутри квадрата 1 площади 1 расположены n многоугольников $M_1, M_2, \ldots, M_n$.

а) Пусть площадь $|M_i|$ каждого из многоугольников M_i (где $i = 1, 2, \ldots, n$) не меньше σ, оцените наименьшую возможную площадь наибольшей из общих частей $M_{ij} = M_i \cdot M_j$ многоугольников M_i и M_j ($i, j = 1, 2, \ldots, n$; $i \neq j$);

б) Пусть площадь $|M_i|$ каждого из многоугольников M_i не меньше σ; оцените наименьшую возможную площадь наибольшего k-кратного пересечения многоугольников (т. е. площадь общей части $M_{i_1 i_2 \ldots i_k} = M_{i_1} \cdot M_{i_2} \cdot \ldots \cdot M_{i_k}$ многоугольников $M_{i_1}, M_{i_2}, \ldots, M_{i_k}$, где $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$; разумеется, $k \leqslant n$);

в) Пусть каждое из l-кратных пересечений $M_{i_1 i_2 \ldots i_l} = M_{i_1} \cdot M_{i_2} \cdot \ldots \cdot M_{i_l}$ многоугольников имеет не большую σ площадь; оцените наименьшую возможную площадь наибольшего из k-кратных пересечений $M_{i_1 i_2 \ldots i_k} = M_{i_1} \cdot M_{i_2} \cdot \ldots \cdot M_{i_k}$ многоугольников (здесь l и k — фиксированные числа, причем $1 \leqslant l \leqslant k \leqslant n$).

14. БУЛЕВЫ ФУНКЦИИ; АЛГЕБРА ВЫСКАЗЫВАНИЙ И АЛГЕБРА КОНТАКТНЫХ СХЕМ КАК НОРМИРОВАННЫЕ БУЛЕВЫ СТРУКТУРЫ

Обратимся теперь к нормированным булевым структурам, элементами которых служат высказывания (см. § 11) и электрические контактные схемы (§ 12). Высказывания мы нормируем, приписав каждому высказыванию p его *значение истинности* $|p|$, равное 1, если p истинно, и 0, если p ложно; аналогично нормой $|A|$ контактной схемы A будет служить ее *проводимость*, равная 1, если A пропускает ток, и 0, если A ток не пропускает. Ясно, что так определенная норма $|p|$ высказывания p (и норма $|A|$ контактной схемы A) удовлетворяет аксиоме H_1 нормы (с. 141). Выполняется здесь и аксиома H_2. В самом деле $pq = o$ тогда и только тогда, когда хотя бы одно из высказываний p и q ложно; но если, скажем, q ложно, то $p + q$ истинно, если p истинно, и $p+q$ ложно, если p ложно, а в обоих этих случаях

$$|p + q| = |p| = |p| + |q|$$

(ибо, ведь здесь $|q| = 0$).

Все операции алгебры высказываний можно характеризовать указанием значений истинности полученных сложных высказываний в зависимости от значений истинности их компонент: так, *сумма* (дизъюнкция) $p + q$ высказываний p и q характеризуется тем, что $p + q$ истинно в том и только в том случае, если истинно хотя бы одно из высказываний p и q, в то время как *произведение* (конъюнкция) pq тех же двух высказываний истинно в том и только в том случае, если истинны оба высказывания p и q; высказывание $\bar{p}$ истинно лишь в том случае, если p ложно. Таким образом, операции $p + q$, pq и $\bar{p}$ могут быть описаны с помощью следующих «таблиц истинности»:

$\|p\|$	$\|q\|$	$\|p+q\|$	$\|pq\|$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

$\|p\|$	$\|\bar{p}\|$
1	0
0	1

Ниже приведены также таблицы, характеризующие *разность* $\setminus$ и *симметрическую разность* (исключающую дизъюнкцию) $*$ двух высказываний p и q, а также импликацию $\Rightarrow$, двойную импликацию (эквивалентность) $\Leftrightarrow$, операцию Шеффера «ни, ни» $|$ и «двойственную операцию Шеффера» $\downarrow$, наконец, тернарную операцию $\{pqr\}$ (см. с. 47, 123—125, 127 и 128):

$\|p\|$	$\|q\|$	$\|p \setminus q\|$	$\|p * q\|$	$\|p \Rightarrow q\|$	$\|p \Longleftrightarrow q\|$	$\|p \mid q\|$	$\|p \downarrow q\|$
1	1	0	0	1	1	0	0
1	0	1	1	0	0	0	1
0	1	0	1	1	0	0	1
0	0	0	0	1	1	1	1

$\|p\|$	$\|q\|$	$\|r\|$	$\|\{pqr\}\|$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0

$\|p\|$	$\|q\|$	$\|r\|$	$\|\{pqr\}\|$
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Последняя таблица истинности показывает, что значение истинности высказывания $\varphi(p, q, r) = \{pqr\}$ совпадает со значением истинности б о л ь ш и н с т в а (двух из трех или даже всех трех) аргументов p, q, r функции φ, в силу чего функцию $\{p, q, r\}$ трех высказываний p, q, r иногда называют *функцией большинства.*

Таблица истинности n-арной операции $f = f(p_1, p_2, \ldots, p_n)$, определяющая значения истинности высказывания f в зависимости от значений истинности простых высказываний $p_1, p_2, \ldots, p_n$, представляет собой не что иное, как таблицу значений *булевой функции* $f = f(p_1, p_2, \ldots, p_n)$, каждый из аргументов $p_1, p_2, \ldots, p_n$ которой, как и сама функция f, может принимать лишь два значения 0 или 1. Таким образом, всевозможные операции алгебры высказываний могут быть описаны как булевы функции (ср. упр. 4.16), что делает само понятие булевой функции весьма важным. Например операциям $\bar{p}$, $p+q$, pq, $p*q$, $p\Rightarrow q$, $p \mid q$ и $\{pqr\}$ отвечают следующие булевы функции: $f(p)$, $f_1(p, q)$, $f_2(p, q)$, $f_3(p, q)$, $f_4(p, q)$, $f_5(p, q)$ и $\varphi(p, q, r)$, где

$$f(1) = 0,\ f(0) = 1;$$

$$f_1(1,1) = f_1(1,0) = f_1(0,1) = 1,\ f_1(0,0) = 0;$$

$$f_2(1,1) = 1,\ f_2(1,0) = f_2(0,1) = f_2(0,0) = 0;$$

$$f_3(1,1) = f_3(0,0) = 0,\ f_3(1,0) = f_3(0,1) = 1;$$

$$f_4(1,1) = f_4(0,1) = f_4(0,0) = 1,\ f_4(1,0) = 0;$$

$$f_5(1,1) = f_5(1,0) = f_5(0,1) = 0,\ f_5(0,0) = 1;$$

$$\varphi(1,1,1) = \varphi(1,1,0) = \varphi(1,0,1) = \varphi(0,1,1) = 1,\ \varphi(1,0,0) =$$

$$= \varphi(0,1,0) = \varphi(0,0,1) = \varphi(0,0,0) = 0.$$

Равенства

$$p * q = p\bar{q} + \bar{p}q, \quad p \Rightarrow q = q + \bar{p}\bar{q}, \quad p \mid q = \bar{p}\bar{q};$$

$$p + q = (p \mid q) \mid (p \mid q), \quad pq = (p \mid p) \mid (p \mid p), \quad \bar{p} = p \mid p;$$

$$p + q = \{pqi\}, \quad pq = \{pqo\}, \quad \{p\bar{p}q\} = q$$

(см. с. 47, 127, 61, 62 и 63—64) на языке булевых функций могут быть записаны так:

$$f_3(p, q) = f_1(f_2(p, f(q)), f_2(f(p), q)),$$
$$f_4(p,q) = f_1(q, f_2(f(p), f(q))),$$
$$f_5(p, q) = f_2(f(p), f(q));$$
$$f_1(p,q) = f_5(f_5(p, q), f_5(p,q)),$$
$$f_2(p,q) = f_5(f_5(p,p), f_5(q,q)),$$
$$f(p) = f_5(p, p);$$
$$f_1(p, q) = \varphi(p, q, 1), f_2(p, q) = \varphi(p, q, 0),$$
$$\varphi(p, f(p), q) = q.$$

Так как число различных наборов значений аргументов булевой функции $f(p_1, p_2, \ldots, p_n)$ является конечным (оно равно 2^n, поскольку каждый аргумент может принимать всего два значения: 0 или 1) и каждому набору значений аргументов может соответствовать либо значение 0, либо значение 1 функции f, то общее число различных булевых функций от n переменных (а значит, и общее число n-арных булевых операций) является конечным: оно равно 2^{2^n} (поскольку число этих функций совпадает с числом способов, каким можно приписать два значения (0 или 1) системе из 2^n величин — наборов значений аргументов функции f; ср. с. 53). Однако это число растет с ростом n чрезвычайно быстро: если имеется лишь две «булевы функции от 0 аргументов» (булевы постоянные) 0 и 1 и лишь четыре булевы функции $f(p)$ от одного аргумента (а именно, $f(p) = 0, f(p) = 1, f(p) = p$ и $f(p) = \bar{p}$), то при дальнейшем увеличении n число различных булевых функций от n аргументов растет с большой скоростью:

n	Число различных булевых функций от n аргументов
0	$2^1 = 2$
1	$2^2 = 4$
2	$2^4 = 16$
3	$2^8 = 256$
4	$2^{16} = 65\,536$
5	$2^{32} = 4\,294\,967\,296$
6	$2^{64} = 18\,446\,744\,073\,709\,551\,616$
и т. д.	

Это обстоятельство делает задачу описания всевозможных булевых функций достаточно сложной.

Весьма важной является задача *конструирования по известным булевым функциям* (например, по описанным выше функциям $f(p)$, $f_1(p, q)$, $f_2(p, q)$, $f_3(p, q)$, $f_4(p, q)$, $f_5(p, q)$ и $\varphi(p, q, r)$) новых функций, характеризующих операции с заранее заданными таблицами истинности; другими словами, задача нахождения аналитических выражений для булевых функций, заданных таблицами своих значений.

Нетрудно показать, как может быть решена эта задача в общем виде. Пусть нам требуется найти булеву функцию $f = f(p, q, r)$, описываемую, скажем, следующей таблицей ее значений:

$\|p\|$	$\|q\|$	$\|r\|$	$\|f\| = \|f(p, q, r)\|$
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	0

(14.1)

Таким образом, высказывание f истинно в том и лишь в том случае, если 1) истинны все высказывания: и p, и q, и r, *или* 2) истинны высказывания p и q, а r ложно, *или* 3) истинны высказывания p и r, а q ложно, *или* 4) истинны высказывания q и r, а p ложно. Употребление частицы «или» подсказывает нам мысль о том, чтобы представить высказывание f в виде *суммы* четырех высказываний f_1, f_2, f_3 и f_4, где, например, высказывание f_1 истинно лишь тогда, когда: 1) истинно p и 2) истинно q и 3) истинно r. Для построения высказывания f_1 нам, очевидно, целесообразно использовать произведение высказываний (употребление союза «и»): $f_1 = pqr$; аналогично $f_2 = pq\bar{r}$, $f_3 = p\bar{q}r$ и $f_4 = \bar{p}qr$. Таким образом, окончательно получаем

$$f = pqr + pq\bar{r} + p\bar{q}r + \bar{p}qr. \qquad (14.1')$$

Ясно, что использованный здесь метод может быть применен для построения функции $f = f(p_1, p_2, \ldots, p_n)$, определяемой при помощи любой наперед заданной таблицы истинности; при этом либо мы придем к функции $f = o$, либо получим *совершенную нормальную аддитивную форму*

$$f = \Sigma p_1' p_2' \ldots p_n' \qquad (14.2)$$

булева многочлена f, где через p_i' (здесь $i = 1, 2, 3, \ldots$, или n) обозначено p_i или $\bar{p}_i$ и все члены стоящей в правой части суммы различны (см. § 6). А именно, каждому набору $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ значений истинности

$(|p_1|, |p_2|, \ldots, |p_n|)$, где все $\varepsilon_i = 0$ или 1, которому в столбце значений величины $|f(p_1, p_2, \ldots, p_n)|$ отвечает *единица*, соответствует слагаемое $p_1' p_2' \ldots p_n'$ суммы (2), причем здесь p_i' есть p_i, если $\varepsilon_i = 1$, и p_i' есть $\bar{p}_i$, если $\varepsilon_i = 0$. Если же в последнем столбце таблицы истинности стоит *нуль*, то отвечающее соответствующему набору $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ истинностей переменных $p_1, p_2, \ldots, p_n$ слагаемое суммы (2) вообще отсутствует. [Ср. с образованием по таблице (1) многочлена (1'); из сказанного также следует, что $f = o$, лишь если $|f(p_1, p_2, \ldots, p_n)| \equiv 0$.]

Из этого описания процедуры отыскания аналитического выражения функции f по ее таблице истинности следует, что каждой возможной таблице отвечает своя совершенная нормальная аддитивная форма f, откуда вытекает, что общее число булевых функций $f(p_1, p_2, \ldots, p_n)$ равно числу возможных совершенных нормальных аддитивных форм булевых многочленов от n переменных, что снова дает нам уже знакомую величину 2^{2^n} для количества булевых функций n переменных (см. с. 53; ср. также ниже упр. 1).

Пример (ср. § 3.1 книги [23], где указан совершенно другой путь решения подобных задач). Пусть наблюдатель *Н* попал в один из двух городов *Ч* и *Л*, где все жители города *Ч* говорят правду, а жители города *Л* всегда лгут; в городе он встретил жителя *Ж* (который мог зайти в этот город и из другого города). Какой вопрос должен задать наблюдатель *Н* жителю *Ж*, для того чтобы выяснить, в каком городе он находится?

◀ Пусть p означает высказывание: *Это город Ч*, а q — *Ты правдив*. Ясно, что вопросы об истинности высказываний p и q, заданные жителю *Ж*, сами по себе не могут помочь нам выяснить, где находится *Н*; поэтому приходится искать подходящую комбинацию $f(p, q)$ высказываний p и q. При этом нужна такая комбинация, чтобы ответ «да» на соответствующий вопрос независимо от значения истинности высказывания q означал истинность высказывания p, а ответ «нет» — ложность высказывания p. Таким образом, требуемая функция f высказываний p и q должна определяться следующей таблицей:

$\|p\|$	$\|q\|$	Желаемый ответ	$\|f\|$
1	1	да	1
1	0	да	0
0	1	нет	0
0	0	нет	1

(14.3)

(заметим, что если житель *Ж* правдив, то ответ «да» соответствует истинному высказыванию f, а если *Ж* лжет — то ложному высказыванию f). Но нетрудно видеть, что искомую таблицу истинности имеет высказывание

$$f(p, q) = pq + \bar{p}\bar{q}. \tag{14.3'}$$

Таким образом, вопрос, который H должен задать жителю $Ж$, может звучать так: *Правда ли, что это город Ч и ты правдив или это город Л и ты лжец.* (Нетрудно указать и другие формы вопроса f, решающего поставленную задачу.) ▶

Форма (2) произвольной булевой функции означает, что *все булевы функции можно представить в виде суперпозиции «элементарных» булевых функций* $f(p)$, $f_1(p, q)$ и $f_2(p, q)$. Так, функция $f(p, q, r)$, заданная таблицей (1) (с. 162), может быть записана так:

$$f = f_1\{f_1[f_2(f_2(p, q), r), f_2(f_2(f(p), q), r)], f_1[f_2(f_2(p, f(q)), r), f_2(f_2(p, q), f(r))]\}.$$

Но в силу соотношений де Моргана (XI):

$$pq = \overline{\overline{p} + \overline{q}} \text{ и } p + q = \overline{\overline{p}\,\overline{q}}$$

функция f_2 может быть представлена в виде суперпозиции функций f_1 и f, а функция f_1 — в виде суперпозиции функций f_2 и f:

$$f_2(p, q) = f\{f_1[f(p), f(q)]\}; \quad f_1(p, q) = f\{f_2[f(p), f(q)]\}.$$

Отсюда следует, что *каждая булева функция от любого числа переменных может быть представлена в виде суперпозиции* одних лишь *функций* $f(p)$ *и* $f_1(p, q)$ *или* одних лишь *функций* $f(p)$ *и* $f_2(p, q)$. Наконец, так как функции $f(p)$, $f_1(p, q)$ и $f_2(p, q)$ могут также быть выражены через функцию Шеффера $f_5(p, q)$ (см. с. 161), то *каждая булева функция может быть получена в результате* специально подобранной *суперпозиции функции* $f_5(p, q)$.

Систему булевых функций, обладающую тем свойством, что л ю б у ю булеву функцию можно представить в виде суперпозиции функций нашей системы, принято называть *полной*; таким образом, полными являются, например, следующие системы булевых функций:

$$\{f_1(p, q), f_2(p, q), f(p)\}; \quad \{f_1(p, q), f(p)\} \text{ или даже } \{f_5(p, q)\}.$$

Исчерпывающее описание всех возможных полных систем булевых функций было дано американским логиком Э. П о с т о м. А именно, Пост показал, что *для того, чтобы система*

$$\{f_1(p_1, p_2, \ldots, p_{n_1}), f_2(p_1, p_2, \ldots, p_{n_2}), \ldots, f_k(p_1, p_2, \ldots, p_{n_k})\}$$

была полной, необходимо и достаточно, чтобы среди функций $f_1, f_2, \ldots, f_k$ *было хотя бы по одной функции каждого из следующих пяти классов булевых функций:*

А. Класс функций, *не сохраняющих константу* 0 (т. е. класс таких функций $f(p_1, p_2, \ldots, p_n)$, что $f(0, 0, \ldots, 0) \neq 0$);

Б. Класс функций, *не сохраняющих константу* 1 (т. е. таких, что $f(1, 1, \ldots, 1) \neq 1$);

В. Класс функций, *не являющихся монотонными* (т. е. таких, что для хотя бы одной пары наборов аргументов $p_1, p_2, \ldots, p_n$ и $q_1, q_2, \ldots, q_n$, где $p_i \geqslant q_i$ для всех $i = 1, 2, \ldots, n$, имеет место неравенство $f(p_1, p_2, \ldots, p_n) < f(q_1, q_2, \ldots, q_n)$; напоминаем, что каждое из чисел p_i, q_i и f равно 0 или 1);

Г Класс функций, *не являющихся двойственными сами себе* (т. е. таких, что хотя бы для одного набора значений $p_1, p_2, \ldots, p_n$ имеет место неравенство $f(\overline{p}_1, \overline{p}_2, \ldots, \overline{p}_n) \neq \overline{f}(p_1, p_2, \ldots, p_n)$; здесь, как обычно, положено $\overline{0} = 1$ и $\overline{1} = 0$);

Д. Класс функций, *не являющихся линейными* (т. е. не представимых в виде $f(p_1, p_2, \ldots, p_n) = a_0 + a_1 p_1 + a_2 p_2 + \ldots + a_n p_n$, где каждый из коэффициентов $a_0, a_1, \ldots, n_n$ равен 0 или 1 и сложение определено как в арифметике вычетов по модулю 2).

Так, например, функция $f_5(p, q)$, определяющая операцию Шеффера, не является ни сохраняющей константу 0 (ибо $f_5(0,0) = 1$), ни сохраняющей константу 1 (ибо $f_6(1,1) = 0$), ни монотонной (ибо $f_6(0,0) > f_6(1,1)$), ни двойственной самой себе (например, $f_6(1, 0) = 0$, а $f_6(\bar{1},\bar{0}) = f_6(0,1) = 0 \neq \overline{f_6}(1,0)$), ни линейной (ибо функция $f_6(p, q)$ отлична, как легко проверить, от каждой из восьми функций $a_0 + a_1p + a_2q$, где $a_0, a_1, a_2 = 0,1$ и сложение, в отличие от правил, задающих сложение в алгебре Буля, определяется равенствами $0+0=1+1=0$, $1+0=0+1=1$). Поэтому все булевы функции могут быть выражены через единственную «функцию Шеффера» $f_6(p, q)$.

Аналогично этому система функций $f(p)$, $f_1(p, q)$, определяющих операции $\bar{p}$ и $p + q$ (булево сложение), также удовлетворяет условиям теоремы Поста, ибо функция $f(p)$ не сохраняет ни 0, ни 1 и не является монотонной, а функция $f_1(p, q)$ не является ни двойственной самой себе, ни линейной; поэтому через функции $f(p)$ и $f_1(p, q)$ также могут быть выражены все булевы функции. Полной является и система из одной функции $\{f_6'(p, q)\}$, отвечающей операции $p \downarrow q$ (см. упр. 2 и 4), или функции $\varphi(p, q, r)$, отвечающей операции $\{p, q, r\}$ (см. упр. 2б)). Напротив система функций $\{f_1(p, q), f_2(p, q)\}$ определяющих (булево) сложение и умножение, условию теоремы Поста не удовлетворяет (ибо обе функции f_1 и f_2 сохраняют 0, сохраняют 1 и являются монотонными); поэтому через эти две функции все булевы функции выразить нельзя.

Относительно доказательства теоремы Поста см, например, [2.2] или [24].

Аналогия между нормированными структурами *высказываний* и *контактных цепей* порождает возможность естественного (взаимно-однозначного или биективного) отображения множества высказываний на множество контактных цепей. Контактные цепи мы условились характеризовать исключительно их проводимостью, подобно тому как высказывания характеризуются их истинностью, — и каждой сложной контактной цепи, включающей контакты A, B, Γ и т. д., отвечает своя *булева функция*, указывающая значения проводимости $|\Phi|$ цепи Φ в зависимости от состояния (замкнут, разомкнут) отдельных контактов, задаваемого значениями их проводимости $|A|$, $|B|$, $|\Gamma|$, ... (число $|A|$ равно 1, если контакт A замкнут, и равно 0, если он разомкнут). При этом естественно сопоставить друг другу высказывания и контактные цепи, которым соответствует о д н а и т а ж е булева функция (ведь безразлично, выражают ли числа, являющиеся аргументами и значением булевой функции, истинности или проводимости!). Так, например, сложному высказыванию (1′), задаваемому таблицей (1) значений отвечающей ему булевой функции, очевидно, соответствует изображенная на рис. 59,*а* цепь, роль аргументов которой играют контакты A, B, Γ, заменяющие высказывания p, q, r. Рассмотренные выше возможные варианты упрощения этой цепи (см. рис. 59,*б* —*г*) указывают одновременно пути упрощения отвечающего таблице (1) сложного высказывания f.

Возникающая здесь аналогия между сложными высказываниями и электрическими цепями может быть использована двояким образом. Во-первых, она дает возможность *моделировать логические соотношения при помощи электрических цепей*; при этом для того, чтобы проверить, является ли соответствующее высказывание истинным или ложным, достаточно убедиться, пропускает ли ток наша электрическая цепь. Во-вторых, мы можем *записывать строение электрической* *сети при помощи составного высказывания* и конструировать электрические цепи с заданными свойствами с помощью тех приемов, которые выше были использованы для построения сложных высказываний.

Проиллюстрируем сказанное на нескольких несложных примерах (ср. также упр. 7; по поводу других примеров такого же рода см., например, [1.13, 2.1, 2.21, 1.16 —1.19 или 2.23—2.26]).

Пример 1. Требуется спроектировать электрическую цепь для спальни, где имеется одна лампочка, и желательно иметь два независимых выключателя: один — у двери, а второй — над постелью; при этом поворот каждого выключателя независимо от состояния второго выключателя должен размыкать цепь, если она до этого была замкнута, и замыкать, если ранее она была разомкнута.

Рассмотрите также аналогичную задачу о цепи с тремя или большим числом независимых выключателей.

◀ Обозначим (контактные) выключатели буквами A и B. Задача состоит в построении такой электрической цепи, содержащей контакты A и B, что изменение значения проводимости одного контакта при любом значении проводимости второго контакта изменяет значение проводимости всей цепи. Так, например, решение задачи может подсказываться следующей таблицей, в которой собраны значения проводимости контактов A, B и значение проводимости всей цепи $\Phi = \Phi(A, B)$:

$\|A\|$	$\|B\|$	$\|\Phi(A, B)\|$
1	1	0
1	0	1
0	1	1
0	0	0

(14.4)

Соответствующую булеву функцию можно представить, например, в следующем виде:

$$\Phi(A, B) = A\overline{B} + \overline{A}B \quad (= A * B); \tag{14.4'}$$

ее реализует электрическая сеть, изображенная на рис. 61 (с. 138)— она-то и доставляет решение нашей задачи.

Аналогично этому решение «задачи о трех выключателях» A, B и Γ решает следующий булев многочлен:

$$\Phi_3(A, B, \Gamma) = (A * B) * \Gamma \quad (= A * B * \Gamma). \tag{14.5}$$

В самом деле, мы только что видели, что булева функция $|\Phi| = |\Delta * \Gamma|$ (ср. с (4')) меняет свое значение, когда меняет значение любой из ее аргументов $|\Delta|$, $|\Gamma|$. Положим теперь $\Delta = A * B$; тогда мы придем к выражению (5). Но изменение проводимости любого из контактов A, B, по доказанному, меняет значение величины $|A * B|$, т. е.

первого из аргументов $|\Delta|$ рассматриваемой функции $|\Phi_3| = |\Delta * \Gamma|$, а изменение проводимости контакта Γ меняет значение второго аргумента $|\Gamma|$ этой функции, — что и подытоживает рассуждения.

Решение задачи о n выключателях доставляет функция

$$\Phi_n (A_1, A_2, \ldots, A_n) = A_1 * A_2 * \ldots * A_n \tag{14.5'}$$

(ассоциативность операции $*$ позволяет отбросить скобки в правой части); доказать это легко, скажем, с помощью метода математической индукции (см. упр. 5). ▶

Пример 2. Комитет состоит из трех членов; голосование «за» осуществляется нажатием кнопки; решение принимается большинством голосов. Спроектируйте такую электрическую цепь, чтобы положительный результат голосования указывался загоранием лампочки над столом председателя.

◀ Нам требуется найти такую функцию $\varphi (A, B, \Gamma)$ трех контактов A, B и Γ, чтобы проводимость φ означала включение большинства (двух или всех трех) из наших контактов. Можно было бы искать аналитическое выражение функции φ стандартным путем, но в данном случае в этом нет нужды: ясно, что требуемым условиям отвечает «функция большинства»

$$\varphi (A, B, \Gamma) = \{AB\Gamma\} = AB + A\Gamma + B\Gamma \tag{14.6}$$

(см. таблицу истинности функции φ на с. 160). На рис. 69 изображено несколько вариантов реализации соответствующей электрической цепи; иное ее строение описано на с. 162. ▶

Пример 3. Спроектируйте *двоичный сумматор* — электрическую цепь с $2n$ входами и $n + 1$ выходом (рис. 70): n первых входов отвечают разрядам двоичной записи первого слагаемого A (где поступление

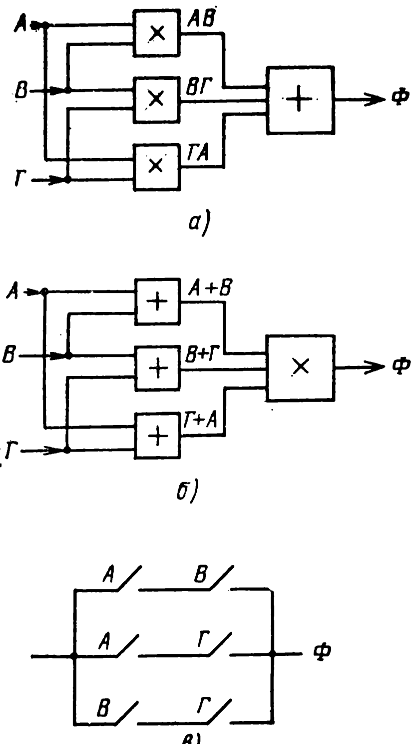


Рис. 69

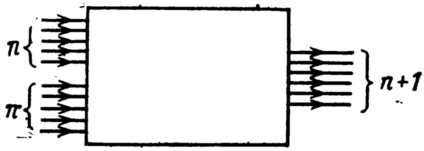


Рис. 70

тока на k-й вход означает, что k-й разряд числа A равен 1, а непоступление — что он равен 0), а следующие n входов — разрядам числа B; $n+1$ выходов сумматора должны указывать значения разрядов суммы (арифметической, а не булевой!) $S = A + B$.

◀ Рассмотрим отдельно устройство, отвечающее какому-то фиксированному i-му разряду чисел A, B и S. Это устройство, очевидно, должно иметь три входа, на которые поступят i-е разряды a_i и b_i чисел A и B и значение p_{i-1} возможного переноса разряда в результате сложения предшествующих разрядов чисел A и B (при $i = 1$ вход p_{i-1}, разумеется, отсутствует); выходы s_i и p_i указывают интересующий нас i-й разряд числа S и (возможный) перенос в следующий разряд p_i (рис. 71). При этом правила двоичной арифметики указывают следующие таблицы значений булевых функций s_i (a_i, b_i, p_{i-1}) и p_i (a_i, b_i, p_{i-1}):

a_i	b_i	p_{i-1}	s_i	p_i
1	1	1	1	1
1	0	1	0	1
0	1	1	0	1
0	0	1	1	0
1	1	0	0	1
1	0	0	1	0
0	1	0	1	0
0	0	0	0	0

(14.7)

Если $i = 1$, то достаточно ограничиться нижней половиной таблицы (7), отвечающей значению $p_{i-1} = 0$; здесь функция p_i (в данном случае p_1) есть просто *булево произведение* аргументов, а функция s_1 — их *симметрическая разность*:

$$s_1 = a_1 * b_1, \quad p_1 = a_1 b_1 \tag{14.8}$$

(ср. рис. 71,*а*). Полная таблица (7) даст более сложные значения функций s_i и p_i: здесь, как легко видеть,

$$s_i = a_i * b_i * p_{i-1} \quad (= (a_i * b_i) * p_{i-1}) \tag{14.8'}$$

(ср. с примером 1; заметьте, что функция s_i меняет значение при изменении значения любого из ее аргументов), а

$$p_i = a_i b_i p_{i-1} + a_i \bar{b}_i p_{i-1} + \bar{a}_i b_i p_{i-1} + a_i b_i \bar{p}_{i-1} =$$

$$= a_i b_i \left((p_{i-1} + \bar{p}_{i-1}) + (a_i \bar{b}_i + \bar{a}_i b_i\right) p_{i-1},$$

т. е.

$$p_i = a_i b_i + (a_i * b_i)\, p_{i-1}$$

(рис. 71, *б*).

На рис. 72 изображен искомый сумматор для сложения трехзначных чисел A и B, реализованный в виде логической цепи (ср. с. 139); ясно, что техническое осуществление подобной схемы не представляет труда. ▶

Пример 4 (см. [25], с. 214). Надо спроектировать электрическую цепь управления лифтом (число этажей, для простоты, полагаем равным двум). Цепь должна содержать два контакта, управление которыми осуществляется нажимом кнопок, одна из которых находится в кабине лифта (кнопка спуска), а вторая — у двери лифта на первом этаже (кнопка вызова); дополнительные контакты связаны с дверями лифта на первом и втором этажах, с внутренней дверью кабины лифта, а также с давлением пассажира на пол. Электрическая цепь, управляющая движением лифта вниз, должна включаться лишь в том случае, когда кабина находится на втором этаже и, кроме того, выполнены следующие условия:

1) обе двери лифта и дверь кабины закрыты; пассажир находится в лифте и нажимает кнопку спуска или 2) обе двери лифта закрыты, дверь кабины лифта открыта или закрыта, пассажира в кабине нет, и кнопка вызова лифта нажата.

◀ Обозначим контактные выключатели, регулирующие включение цепи, следующим образом: B — выключатель, замыкающийся лишь

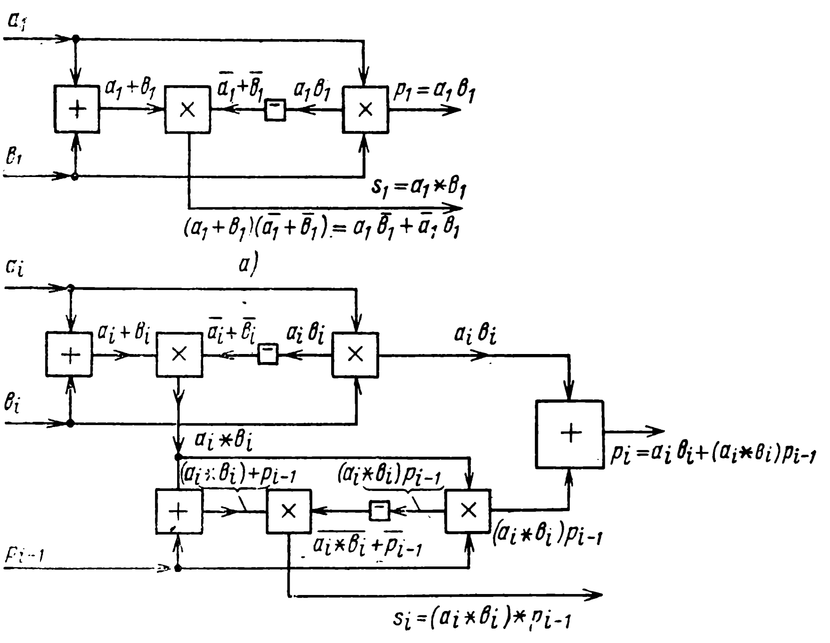


Рис. 71

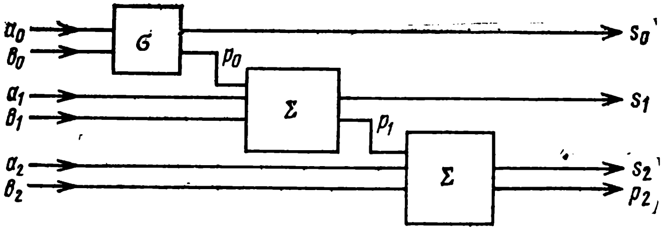


Рис. 72

в том случае, когда кабина находится на 2-м этаже, $Д_1$ и $Д_2$ — выключатели, замыкающиеся при закрывании Дверей лифта на 1 и 2-м этажах, $Д_к$ — аналогичный выключатель, связанный с дверью Кабины, $П$ — выключатель, связанный с полом кабины и замыкающийся от тяжести Пассажира; $К_с$ и $К_в$ — выключатели, связанные с Кнопкой Спуска в кабине лифта и с Кнопкой Вызова на 1-м этаже у дверей лифта. Согласно условию значение проводимости цепи $f = f\ (В,\ Д_1,\ Д_2,\ Д_к,\ П,\ К_с,\ К_в)$ равно 1 в том и лишь в том случае, когда равно 1 значение проводимостей контактов $В$, $Д_1$, $Д_2$, $Д_к$, $П$ и $К_с$ или когда равно 1 значение проводимостей контактов $В$, $Д_1$, $Д_2$, $К_в$ и равно 0 значение проводимости контакта $П$. Но отсюда следует (ср. с. 162—163), что функцию f можно представить так:

$$f = ВД_1Д_2Д_кПК_с + ВД_1Д_2К_в\bar{П} =$$
$$= ВД_1Д_2\ (ПД_кК_с + \bar{П}К_в).$$

Соответствующая электрическая цепь изображена на рис. 73.

Аналогично может быть построена и цепь, управляющая движением лифта наверх. ▶

Ранее мы всегда считали, что значение истинности (норма $|p|$ высказывания p) может иметь лишь одно из двух значений: 1 (p истинно) и 0 (p ложно). Однако человеческая логика не всегда работает по такой, несколько слишком прямолинейной схеме. В последнее время довольно много внимания уделяется так называемым *многозначным логикам*, где значение истинности высказывания может принимать более чем два значения, скажем 1 (истинно), 0 (ложно) и 1/2 (возможно). Подобные построения (ср., например, [1.14, 2.12]) можно связать и с введением в алгебре высказываний норм элементов, принимающих

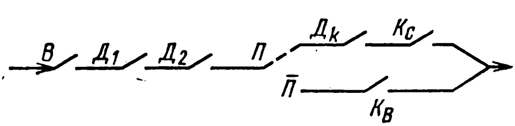


Рис. 73

более чем два значения; впрочем, они очень осложняются тем, что в случае «двузначной нормы» мы имеем естественное отображение булевой структуры высказываний в булеву структуру из двух элементов, в то время как в случае, скажем, *трехзначной* логики мы никак не можем сохранить и в множестве истинностей булеву структуру, поскольку булевых структур из трех элементов вообще не существует (ср. с. 177).

Не останавливаясь на рассмотрении логик с тремя значениями истинности (например, «истина», «ложь» и «неопределенно» или «бессмысленно») и вообще конечнозначных логик (приобретающих в последнее время все большее значение), мы перейдем теперь к наиболее интересному и плодотворному обобщению алгебры высказываний, оперирующему с бесконечным множеством значений истинности, которые естественно интерпретировать как в е р о я т н о с т и какого-либо события («вероятностная логика»).

Упражнения 14.1. Выпишите совершенные нормальные формы

а) аддитивные, б) мультипликативные (см. § 6)

всех 16 бинарных алгебраических операций (т. е. булевых функций от двух переменных; ср. с. 160).

14.2. а) Составьте таблицу 16 бинарных операций булевой структуры (см. упр. 1), указав для каждой операции (булевой функции двух переменных) название, формулу (по возможности — простую), а также то, удовлетворяет или не удовлетворяет эта функция каждому из фигурирующих в условиях теоремы Поста (с. 164) условий А — Д.

б) Проверьте, что булева «функция большинства» $\varphi(p, q, r) = pq + qr + rp$ (см. с. 63 и 160) удовлетворяет всем условиям А—Д теоремы Поста [и значит, одна функция $\varphi(p, q, r)$ (см. с. 160) образует п о л н ы й класс функций]

14.3. Какие из следующих наборов унарных и бинарных операций булевой структуры (булевых функций одной и двух переменных) образуют полную систему функций; в случае положительного ответа выразите через операции этого набора все известные вам булевы операции:

а) $+$ и $\Rightarrow$ (т. е. $f_1(p, q) = p + q$ и $f_2(p, q) = p \Rightarrow q$); б) $^-$ и $\Rightarrow$;

в) $^-$ и $\Longleftrightarrow$; г) $+$, $\cdot$, $\Rightarrow$ и $\Longleftrightarrow$?

14.4. Перечислите все булевы операции $\circ$ (булевы функции $f(p, q) = p \circ q$ двух переменных), такие что все без исключения булевы операции можно выразить через

а) операцию $\circ$, б) операции $^-$ и $\circ$.

14.5. Докажите, что функция (5а) (с. 167) действительно решает «задачу о n выключателях»; опишите строение соответствующей электрической цепи.

14.6. Опишите электрическую контактную цепь, реализующую

а) импликацию $p \Rightarrow q$ двух переменных p и q; б) эквивалентность $p \Longleftrightarrow q$.

14.7. а) Комитет состоит из пяти членов; опишите «функцию большинства» пяти переменных p_0, p_1, p_2, p_3, p_4 (ср. с. 160) и постройте такую электрическую цепь, чтобы лампочка зажигалась в том и только в том случае, если большинство из членов комитета нажмут кнопки;

б) опишите функцию, аналогичную функции упр. а), но отвечающую условию о том, что решение принимается в случае голосования за него большинства членов комитета, включая председателя (переменное p_0);

в) спроектируйте такую электрическую цепь, что зажигание лампочки отвечает принятию решения комитетом из $2n + 1$ членов, если голосование «за» осуществляется нажиманием кнопки (включением контакта) и для положительного решения необходимо просто большинство;

г) спроектируйте цепь, аналогичную электрической цепи упр. в), но отвечающую случаю, когда для положительного решения надо, чтобы за него голосовало большинство, включающее обладающего правом «вето» председателя.

15. ЧТО ТАКОЕ ТЕОРИЯ ВЕРОЯТНОСТЕЙ

Вернемся снова к булевой структуре, элементы которой мы в этом параграфе будем обозначать большими буквами латинского алфавита и называть *событиями*, как это принято в теории вероятностей. В остальном можно считать, что мы по-прежнему имеем дело с тем вариантом структуры Буля, которому был посвящен § 11, поскольку рассматриваемые здесь события характеризуются некоторыми высказываниями (*завтра будет дождь*, *подброшенная монета упала гербом кверху*, *эта деталь бракованная* и т. д.), под суммой $A + B$ и произведением AB событий A и B понимаются события «A или B», соответственно «A и B», а «дополнение» $\bar{A}$ события A определяется как событие «не A». Из числа всех событий мы выделим *достоверные* события I, которым отвечают заведомо и с т и н н ы е высказывания (*за субботой следует воскресенье*, *монета упала кверху гербом или кверху цифрой*) и *невозможные* события O, которым отвечают л о ж н ы е высказывания (*за субботой следует понедельник*, *монета упала кверху гербом и цифрой одновременно*).

Предположим теперь, что алгебра событий нормирована с соблюдением условий § 13: норму $|A|$ элемента A рассматриваемой булевой структуры мы теперь будем обозначать через $p(A)$ а аксиомы H_1 и H_2 нормы (основные аксиомы теории вероятностей!) будем обозначать через B_1 и B_2:

B_1 : $0 \leqslant p(A) \leqslant 1$; $p(I) = 1$, $p(O) = 0$.

B_2: если $AB = O$, то $p(A + B) = p(A) + p(B)$.

Норму $|A|$ или $p(A)$ элемента A мы по-прежнему будем понимать как своеобразное «значение истинности» характеризующего A высказывания: если $p(A) = 1$, то это высказывание является истинным, т. е. событие A можно считать достоверным[1]; если $p(A) = 0$, то A следует признать невозможным, т. е. характеризующее A высказывание

---

[1] В рамках теории вероятностей достоверное событие может быть о п р е д е л е н о условием $p(A) = 1$, а невозможное — условием $p(A) = 0$; однако, такое определение понятий невозможности и достоверности совпадает с общепринятым лишь в случае к о н е ч н ы х вероятностных структур (см. с. 177). В самом деле, скажем, в рассмотренной на с. 174 задаче каждому конкретному значению длины хорды (например, равному диаметру круга) при любом разумном введении вероятностей следует приписать нулевую вероятность — из чего общежитейски (не математически) мыслящий человек заключит, пожалуй, что невозможна н и к а к а я длина хорды.

ложно; если же $0 < p(A) < 1$, то число $p(A)$ характеризует в е р о я т н о с т ь того, что рассматриваемое высказывание окажется верным, иными словами, вероятность того, что событие A произойдет. Изучение этой нормированной алгебры Буля и составляет предмет теории вероятностей.

Итак, объектом **теории вероятностей** является некоторая совокупность элементов, образующих нормированную булеву структуру; другими словами, *предметом теории вероятностей является изучение математической структуры*

$$\langle \mathscr{B};\ +,\ \cdot,\ ^{-},\ \supset,\ p\rangle, \tag{15.1}$$

описываемой аксиомами (I) — (XXI) (или, если угодно, скажем, аксиомами $Б_{1-8}$ § 5) *и аксиомами* $В_{1,2}$. При этом элементы $A, B, C, \ldots \in \mathscr{B}$ называются *событиями*, а их нормы $p(A)$, $p(B)$, $p(C)$, ... — *вероятностями* этих событий.

При таком определении теории вероятностей (предложенном в 1917 г. замечательным русским математиком Сергеем Натановичем Б е р н ш т е й н о м (1880—1968; см. [26]) требуется задать заранее булеву структуру рассматриваемых событий; множествам событий разного характера (содержащим конечное число элементов; бесконечным, но счетным; множествам, еще более богатым событиями) отвечают разные разделы теории вероятностей. При этом выбор значений вероятностей н е о т н о с и т с я к теории вероятностей: этот выбор должен быть так или иначе произведен заранее. Задачи теории вероятностей состоят в указании правил, позволяющих по известным вероятностям тех или иных событий A, B, C и т. д. находить вероятности других событий, так или иначе связанных с исходными,— например событий AB, $(A + B)\bar{C}$, $(A + B)^n$ и т. д. Следует, однако, иметь в виду, что указанная здесь общая постановка задач теории вероятностей конкретизируется в огромном числе вопросов, зачастую имеющих совершенно разный характер, и наше краткое определение предмета теории вероятностей не может дать никакого представления об этой обширной и важной науке (см., например, [1.10, 1.11, 2.17]).

Заметим еще, что в настоящее время теорию вероятностей чаще определяют не совсем так, как указано выше. Мы уже упоминали (см. с. 78) об одном из основных результатов теории булевых структур, в силу которого каждая такая структура может рассматриваться как алгебра множеств, элементами которой являются определенные подмножества некоторого универсального множества I (т е о р е м а С т о у н а). Это позволяет положить в основу теории вероятностей так называемое «полное множество элементарных событий» I, различные подмножества которого отождествляются с рассматриваемыми событиями; нормы элементов соответствующей булевой структуры (ср. с примерами 3 и 4 из § 13) определяются аксиоматически, при помощи требований, которым они должны удовлетворять. Такой путь построения теории вероятностей, предложенный в 1929 г. Андреем Николаевичем Колмогоровым (род. в 1903 г., см. [27]), обладает рядом преимуществ. Мы, однако, не можем здесь остановиться на этом подробнее.

То обстоятельство, что мы оставили открытым очень важный вопрос о том, как задавать исходные вероятности, не должно нас смущать. Ведь и в геометрии мы имеем лишь возможность сравнивать между собой те или иные расстояния и углы (так, мы можем, например, доказать, что если угол ABC равен 90°, то квадрат расстояния AC равен сумме квадратов расстояний AB и BC); однако вопрос о том, как определяются расстояния и углы, фактически выходит за рамки геометрии. Ясно, что нормы (вероятности) рассматриваемых событий, лежащие в основе содержательной теории, должны согласовываться с нашей интуицией (так, скажем, событию *утром восходит солнце* следует приписать вероятность 1, но никак не 0) и с физическими экспериментами, о которых мы еще скажем ниже. Но ясно, что установление такого соответствия по существу не может относиться к компетенции какой-либо математической дисциплины, поскольку математика, будучи дедуктивной наукой, исходит из опыта и интуиции, но строиться должна лишь чисто формально (ср. с [II, §§. 1 и 7]).

Чтобы пояснить это положение, поставим вопрос об определении вероятности того, что брошенная наугад игральная кость упадет кверху стороной, на которой отмечены 6 очков. Наличие у кости шести сторон побуждает нас приписать этому событию вероятность 1/6. Может, однако, оказаться, что кость на самом деле является фальшивой: она изготовлена из неоднородного материала, например наполнена с одной стороны свинцом, так что при бросании она почти наверняка будет выпадать шестеркой кверху. В этом случае мы вынуждены будем придавать рассматриваемому событию вероятность, значительно большую, чем 1/6. Но ясно, что вопрос о физическом строении конкретной игральной кости, которой пользуется тот или иной игрок (возможно, — шулер!), может интересовать милицию, но никак не математику: к столь абстрактной дисциплине, как теория вероятностей, этот вопрос не имеет никакого отношения.

Вот еще один хорошо известный пример такого же рода. Рассмотрим задачу об определении вероятности того, что *проведенная наугад в круге K хорда AB* окажется *больше стороны вписанного в круг правильного треугольника*. Здесь можно рассуждать следующим образом. Рассмотрим все хорды, параллельные заданному направлению l; хорды, бо́льшие стороны UV вписанного в круг K правильного треугольника, высекают на перпендикулярном l диаметре PQ отрезок $MN = 1/2 \cdot PQ$ (рис. 74,*а*), исходя из чего хочется приписать интересующей нас вероятности значение 1/2. С другой стороны, можно рассмотреть все хорды, проходящие через данную точку U окружности; бо́льшие UV хорды заполняют угол, равный 1/3 развернутого угла (рис. 74,*б*); поэтому искомой вероятности естественно приписать значение 1/3. Наконец, середина S проведенной хорды AB может совпасть с любой точкой круга K; если $AB > UV$, то S принадлежит меньшему кругу k, площадь которого составляет 1/4 часть площади круга K (рис. 74,в); поэтому можно думать, что искомая вероятность равна 1/4.

Какое из этих трех решений задачи является правильным? Верный ответ на этот вопрос состоит в следующем. Сформулированная выше задача неправильно поставлена: мы указали множество $\mathfrak{B}$ рассматриваемых событий (которые можно отождествлять с множествами хорд круга K), но не указали, каким образом вводятся нормы $p(A)$ элементов A этого множества. Таким образом, мы пока не имеем нормированной структуры (1), изучение которой составляет предмет теории вероятностей [1], а до задания этой структуры математику здесь делать нечего: предложить ему изучать такую структуру, не фиксировав в ней нормы p, столь же нелепо, как, скажем, просить его о решении уравнения с «засекреченной» правой частью. Наши три ответа «задачи о хорде» соответствуют трем различным способам введения норм,— но не дело математика выяснять, какой из этих трех способов введения норм является «лучшим»: с его точки зрения все они совершенно равноправны. Таким образом, полученное противоречие, которое придумавший его известный французский математик Жозеф Бертран (1822—1900) считал опровергающим теорию вероятностей, лишь способствовало прояснению ее содержания (ср. [28]).

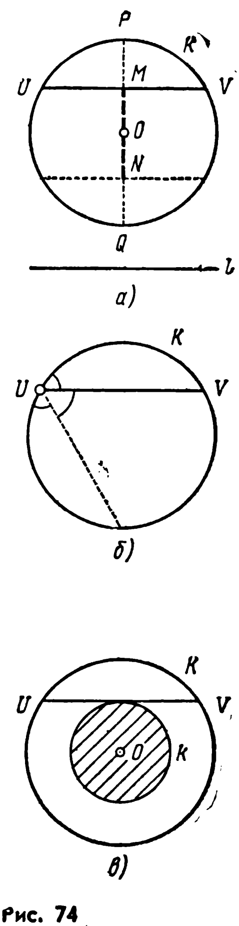


Рис. 74

Своеобразным отражением взаимоотношений между «черно-белой» (или двузначной) аристотелевой логикой и «серой» или «размытой» (бесконечнозначной) вероятностной логикой может служить принадлежащая известному американскому исследователю Л. А. Заде теория так называемых *нечетких* или *размытых* множеств. Сам Заде постулировал необходимость обращения к этой теории во всех проблемах «гуманистического» характера, т. е в проблемах, связанных с человеческой психикой с ее принципиально «размытым» характером (ср. со сказанным на с. 115), и, в частности, во всех науках гуманитарного цикла вроде лингвистики, психологии или экономики. Характерен успех, который имела созданная Заде теория! Возникла она, по-видимому, где-то в середине 60-х годов (одним из первых решительно поддержал ее ведущий американский специалист по прикладной математике Рихард Бел-

[1] Поскольку множество $\mathfrak{B}$ в этом случае совпадает с множеством подмножеств некоторого универсального множества I, введение фигурирующих в (1) операций и отношения ($+$, $\cdot$, $^-$ и $\supset$) здесь производится по общим правилам алгебры множеств (см. гл. I); однако нормы p должны быть введены тем или иным специальным соглашением.

л м а н, первые публикации которого на эту тему появились почти одновременно с работами Заде), а в настоящий момент ей посвящена уже колоссальная литература, лишь весьма незначительную часть которой составляют 60 книг и статей, перечисленных в библиографии к вышедшей в свет в 1973 г. книге [29] Л. Заде (и 25 названий более поздних работ, указанных в дополнительной библиографии к опубликованному в 1976 г. русскому переводу этой книги) Еще более показательным надо считать появление во Франции в 1972—1975 гг. четырехтомного (!) учебника [30] по теории размытых множеств [1] (в настоящее время частично переведенного и на английский язык), рассчитанного на студентов и на лиц, профессионально заинтересованных в этой теории, но не имеющих основательного математического образования. Общий объем этого учебника, автор которого, известный педагог и пропагандист математики А. Кофман, хорошо известен нашим читателям по переводам ряда книг (например [1.12, 2.16]), составляет около 1500 страниц. Наконец, недавно был создан специализированный «Международный журнал по теории размытых множеств» (International Journal of Fuzzy Sets and Systems).

Основные предпосылки созданной Л. Заде теории заключаются в следующем. Исходным понятием эскизно намеченной в гл. 1 настоящей книги «наивной» (неаксиоматической) теории множеств является понятие *принадлежности* $x \in A$ элемента x универсального множества I к определенному подмножеству $A \subset I$; копируя построения, приводящие к концепции нормированной структуры Буля, можно говорить о *мере* $m_A(x)$ принадлежности x множеству A: эта мера равна 1, если $x \in A$, и равна 0, если $x \notin A$. Переходя теперь к нечетким множествам, вроде, скажем, множеств умных людей, красивых женщин или великих писателей, Заде предлагает оценивать меру принадлежности элемента x множеству A (скажем, Глеба Успенского или Гюстава Флобера множеству великих писателей) величиной $m_A(x)$, где $0 \leqslant m_A(x) \leqslant 1$ (если $m_A(x) = 1$, то x безусловно принадлежит A, если $m_A(x) = 0$, то x наверняка A не принадлежит). При этом полная характеристика (нечеткого) множества $A \subset I$ дается (числовой [2]) функцией $m_A(x)$ с областью определения I («размытой» мерой принадлежности x к A). «Размытые» *объединение* $A \dot{+} B$ и *пересечение* AB множеств A и B, *дополнение* $\bar{A}$ множества A и условие *принадлежности* $A \subset B$ множества A множеству B вводятся так:

$$m_{A+B}(x) = m_A(x) \oplus m_B(x); \qquad (а)$$

$$m_{AB}(x) = m_A(x) \otimes m_B(x); \qquad (б)$$

$$m_{\bar{A}}(x) = 1 - m_A(x); \qquad (в)$$

$A \subset B$ *тогда и только тогда, когда* $m_A(x) \leqslant m_B(x)$ при всех $x \in I$, (г)

где «булева сумма» $f_1 \oplus f_2$ и «булево произведение» $f_1 \otimes f_2$ двух числовых функций $f_1(x)$ и $f_2(x)$ с общей областью определения I понимаются в смысле порожденной множеством рассматриваемых функций неполной булевой структуры:

$$f_1(x) \oplus f_2(x) = \max [f_1(x), f_2(x)], \quad f_1(x) \otimes f_2(x) = \min [f_1(x), f_2(x)] \qquad (д)$$

(ср. § 10, модель 4).

---

[1] Последний том этого сочинения представляет собой задачник по теории размытых множеств; при этом он охватывает лишь содержание первого тома основной части [30], так что можно предполагать, что эта книга пока еще не завершена.

[2] Мы не коснемся здесь дальнейших обобщений теории Заде, в которых значения $m_A(x)$ «меры принадлежности x к A» являются не (вещественными) числами, а элементами иного частично упорядоченного множества, например, решетки или булевой структуры.

[Укажем еще, что наряду с «теоретико-множественными» суммой $A+B$ и произведением AB двух множеств A и B в теории Заде существуют также их «арифметические» сумма $A \oplus B$ и произведение $A \otimes B$:

$$m_{A\otimes B}(x)=m_A(x)\cdot m_B(x); \tag{е}$$

$$m_{A\oplus B}(x)=m_A(x)+m_B(x)-m_A(x)\,m_B(x)\ (=m_A(x)+m_B(x)-m_{A\otimes B}(x)) \tag{ж}$$

(заметьте, что $m_A(x)+m_B(x)-m_{AB}(x)=m_{A+B}(x)$ — ср. с формулой (11) ниже).] Ясно, что для «четких» множеств, где $m_A(x)=1$ или 0 введенные равенствами (а) — (в) операции (и введенное с помощью (г) отношение) совпадают с рассматриваемыми в гл. 1; операции $\oplus$ и $\otimes$ над множествами здесь совпадают с операциями, задаваемыми условиями (а) и (б) и поэтому бессодержательны

На этой базе Заде строит и свою «нечеткую» (или «размытую») логику, оперирующую с «нечеткими высказываниями» типа: x принадлежит A, где A — «нечеткое» множество (вроде уже упоминавшегося выше высказывания: *Глеб Успенский — великий писатель*) и их («размытыми») значениями истинности; он определяет («размытые») операции над такого рода высказываниями: дизъюнкцию, конъюнкцию, отрицание и др., а также «размытые» отношения между ними (следует или не следует из высказывания q: *Андрей — хороший математик*, высказывание p: *Андрей — умный человек*?). Мы, однако, не имеем возможности остановиться здесь подробно на этой содержательной теории, по поводу которой уместно отослать читателя к названным выше книгам [29 и 30]

Практически введение вероятностей (норм) легче всего осуществить в случае так называемых к о н е ч н ы х вероятностных структур — структур (1), в которых множество $\mathcal{B}$ событий является конечным. Мы знаем (ср. § 7), что каждая конечная булева структура является *атомарной* — она характеризуется наличием конечного числа k атомов (их уместно обозначить через $A_1, A_2, \ldots, A_k$), таких что

$$A_iA_j=O,\quad i\neq j,\quad i,j=1,2,\ldots,k \tag{15.2}$$

(ср. с (8.11)), и что каждое $A\in\mathcal{B}$ представляется в виде суммы конечного числа атомов A_i

$$A=A_{i_1}+A_{i_2}+\ldots+A_{i_q}, \tag{15.3}$$

где $1\leqslant i_1<i_2<\ldots<i_q\leqslant k$ (ср. с (8.17)). В теории вероятностей попарно несовместимые (см. (2)) события A_i принято называть *элементарными* событиями, их совокупность $\{A_1, A_2, \ldots, A_k\}$ именуют *полной группой элементарных событий*. При этом для того, чтобы задать все вероятности $p(A)$, достаточно иметь таблицу вероятностей $p(A_i)=$ $=p_i$ всех «атомов» (элементарных событий) A_i

События	$A_1\quad A_2\ldots A_k$
Вероятности	$p_1\quad p_2\ldots p_k$

(15.4)

В таблице (4), разумеется, $0\leqslant p_i\leqslant 1$ для всех i и, поскольку A_1+ $+A_2+\ldots+A_k=I$ (ср. (8.19)), то в силу B_2 (ср. (2)) и B_1

$$p_1+p_2+\ldots+p_k=p(A_1)+p(A_2)+\ldots+$$
$$+p(A_k)=p(A_1+A_2+\ldots+A_k)=p(I)=1. \tag{15.5}$$

Для подобных конечных вероятностных структур *ранга* k (ср. § 7) имеется всего 2^k возможных событий и вероятность $p(A)$ задаваемого формулой (3) события A равна

$$p(A) = p_{i_1} + p_{i_2} + \ldots + p_{i_q}. \tag{15.3'}$$

В случае счетного множества $\{A_1, A_2, \ldots, A_n, \ldots\}$ элементарных событий (атомов) A_i (см., например, [1.9]) задание норм (вероятностей) $p(A)$ также можно осуществить прямым указанием значений норм $p(A_i) = p_i$ элементарных событий — только здесь таблица (4) будет уже бесконечной и ее роль, чаще всего, играет явная формула для величин $p_i = p(i)$. Так, например, большое место в теории вероятностей занимают так называемые *пуассоновы*[1] структуры, где $p_i = (a^{i-1}/(i-1)!)\, e^{-a}$, a фиксировано. Ясно, что в случае бесконечного (счетного) множества событий A_i суммы (3') могут обращаться в бесконечные ряды (а стоящая в левой части (5) сумма $\sum_i p_i$ всегда является рядом). Однако в других случаях необходимы иные способы задания вероятностей. Так, если «полное» множество событий можно изобразить множеством точек некоторой фигуры I на прямой, на плоскости или в (обыкновенном или многомерном [2]) пространстве, то вероятности чаще всего задаются указанием *плотности вероятности* $f(M)$, определенной для каждой точки $M \in I$: в таком случае вероятность $p(A)$ события A, изображаемого множеством $A \subset I$, вычисляется по формуле

$$p(A) = \int\limits_{M \in A} f(M)\, dM, \tag{15.6}$$

где под dM понимается элемент длины, площади или (трехмерного или многомерного) объема (ср. со сказанным по поводу модели 4 из § 13).

В случае конечной вероятностной структуры часто есть основания считать элементарные события $A_1, A_2, \ldots, A_k$ *равноправными* и, следовательно, приписывать им одинаковую вероятность, в силу (5) равную $1/k$ (так называемый *классический* случай). Например, при рассмотрении совокупности событий, связанных с бросанием игральной кости, полную группу элементарных событий образуют события $A_1, A_2, \ldots, A_6$, заключающиеся в выпадении соответственно 1, 2, ..., 6 очков. Если дополнительно указано, что кость сделана из однородного материала, то это следует понимать как постулирование равноправности событий A_1, A_2, A_3, A_4, A_5 и A_6; другими словами, как указание на равенство всех вероятностей $p_i = p(A_i)$, где $i = 1, 2, \ldots, 6$, т. е. на то, что $p_1 = p_2 = \ldots = p_6 = 1/6$.

---

[1] Симеон Пуассон (1781—1840) — видный французский математик.
[2] См., например, [11, § 6] или [31].

В классическом случае вероятность «сложного» события $A = A_{i_1} + A_{i_2} + \ldots + A_{i_q}$ равна

$$p(A) = \underbrace{1/k + 1/k + \ldots + 1/k}_{q \text{ раз}} = q/k, \tag{15.7}$$

т. е. *отношению числа элементарных событий* $A_{i_1}, A_{i_2}, \ldots, A_{i_q}$, *благоприятствующих* A, *к общему числу* k *всех элементарных событий*; так, например, при бросании «правильной» кости вероятность выпадения $Ч$ четного числа очков равна $3/6 = 1/2$ (ибо событию $Ч$ благоприятствуют исходы A_2, A_4 и A_6). Однако в очень многих случаях такой подход к вероятностям (*классическое определение вероятности* (7)) является невозможным.

В основе всех практических применений понятия вероятности лежит основной принцип, утверждающий, что вероятность события A близка к частоте осуществления этого события в длинной серии однотипных испытаний. Так, например, частота выпадения шестерки в длинной серии бросаний однородной игральной кости при большом числе бросаний обязательно будет близка к 1/6; если же эта частота отличается от 1/6, то это свидетельствует о неоднородности кости, — и в этом случае мы обязаны отказаться от принятия вероятностей $p_i = 1/6$ при всех i. Этот принцип открывает дорогу для экспериментального определения вероятностей, основанного на многократном повторении соответствующего эксперимента. Во многих случаях такой («статистический») путь определения вероятностей является единственно возможным; так, например, при выяснении эффективности определенного метода прогноза погоды мы вынуждены принять за фигурирующие в этом критерии вероятности (вероятность того, что прогноз оправдается; вероятности той или иной погоды) частóты соответствующих событий в длинной серии испытаний, поскольку никакое другое («теоретическое») определение этих вероятностей в настоящее время невозможно. Однако ясно, что осуществление подобных экспериментов не может относиться к математической теории вероятностей — и ссылка на них лишь указывает на пути практического применения теории вероятностей, математическое построение которой базируется исключительно на описывающих структуру (1) аксиомах, без каких бы то ни было апелляций к явлениям реальной жизни.

В приведенном выше примере с определением вероятности того, что хорда AB круга K превзойдет по величине сторону a вписанного в K правильного треугольника (рис. 74), мы можем так организовать соответствующий эксперимент, чтобы частота осуществления рассматриваемого события в длинной серии испытаний была близка к 1/2, или к 1/3, или к 1/4; можно также придумать такую постановку опыта, что она не окажется близкой ни к одному из этих трех чисел. Так, например, если много раз бросать проволочное кольцо K на лист бумаги, разграфленный системой параллельных линий, расстояние между каждыми двумя соседними из которых равно диаметру K, то частота случаев, когда хорда круга K, высеченная одной из проведенных линий, окажется больше стороны вписанного в K правильного треугольника, будет близка к 1/2. Если бросать наугад с большого расстояния на плоскость, на которой изображен круг K, острием вниз иголку и каждый раз, когда иголка падает внутрь K, проводить хорду AB, которую острие иголки делит пополам, то процент проведенных хорд, превышающих сторону UV вписанного в K правильного треугольника, будет близок к 25% (доля случаев, когда $AB > UV$, будет близка к 1/4). Если укрепить в точке A, ограничивающей круг окружности подвижную тонкую стрелку, подобную стрелке компаса, и много раз раскручивать ее, то доля случаев, при которых высеченная после остановки этой стрелкой из круга K хорда окажется больше стороны вписанного в K правильного треугольника, будет близка к 1/3. Поэтому все три варианта введения вероятностей, использованные в трех решениях задачи, могут считаться допустимыми, — и для чистого математика любой из них ничем не хуже и не лучше двух других!

Остановимся еще на простейших свойствах вероятностей, вытекающих из их определения как норм элементов нормированной булевой структуры. Мы уже знаем, что $0 \leqslant p(A) \leqslant 1$ и что если события A и B *несовместимы* (т. е. $AB = O$), то

$$p(A + B) = p(A) + p(B), \tag{15.8}$$

а также что

$$p(\bar{A}) = 1 - p(A) \tag{15.9}$$

(ср. с (13.7)) и

$$\text{если } A \supset B, \text{ то } p(A) \geqslant p(B) \tag{15.10}$$

(см. (13.8)).

Формула (8) легко может быть обобщена на произвольную совокупность *попарно несовместимых* событий $A_1, A_2, \ldots, A_n$ (т. е. таких событий, что $A_iA_j = O$ для всех $i, j = 1, 2, \ldots, n$): для этих событий

$$p(A_1 + A_2 + \ldots + A_n) = p(A_1) + p(A_2) + \ldots + p(A_n). \tag{15.8'}$$

Если же события A и B не несовместимы, то формула (8) заменяется следующей:

$$p(A + B) = p(A) + p(B) - p(AB) \tag{15.11}$$

(см. формулу (13.9)). Также и формула включений и исключений (13.12) полностью переносится в область вероятностей (ср. упр. 1 и пример 4).

Формула (11) делает важным понятие вероятности $p(AB)$ п р о и з в е д е н и я двух событий. Величину $p(AB)$ часто оказывается удобным представить в виде произведения двух сомножителей:

$$p(AB) = p(A)\, p_A(B), \tag{15.12}$$

где величина $p_A(B)$ (определенная только если $p(A) \neq 0$) называется *условной вероятностью* события B при условии осуществления события A:

$$p_A(B) = p(AB)/p(A). \tag{15.12'}$$

Заметим, что формула (12') (или 12)) дает нам о п р е д е л е н и е условной вероятности $p_A(B)$: никакого другого определения условной вероятности в рамках математической теории вероятности предложено быть не может.

Если $p_A(B) = p(B)$, то события A и B называются *независимыми*. Таким образом, независимые события A и B определяются как такие, что

$$p(AB) = p(A)p(B). \tag{15.13}$$

Строгое математическое определение (13) независимости двух событий часто заменяют описанием независимых событий как таких, что осуществление или неосуществление события A нисколько не влияет на условия опыта, с осуществлением которого связана реализация события B, и поэтому вероятность события B не зависит от того, имеет или не имеет место событие A. Однако это словесное описание апеллирует к представлению о вероятности как о частоте осуществления определенного результата в серии каких-то экспериментов — и поэтому имеет естественнонаучный, а не формально-математический характер. Кроме того, высказанное выше утверждение не является достаточно четким, и можно считать, что математическим его выражением как раз и является формула (13).

Если имеет место равенство (13), то, очевидно,

$$p_A(B) = p(B) \text{ и } p_B(A) = p(A); \tag{15.14}$$

таким образом, независимость событий A и B можно характеризовать как первым, так и вторым из равенств (14). Более того, из того, что $p(AB) = p(A)\,p_A(B)$ и $p(AB) = p(BA) = p(B)\,p_B(A)$, вытекает следующая полезная зависимость между условными вероятностями $p_A(B)$ и $p_B(A)$:

$$p_A(B)/p_B(A) = p(B)/p(A) \text{ или } p_B(A) = [p(A)/p(B)]\,p_A(B). \tag{15.15}$$

В течение столетий все изложения теории вероятностей обязательно начинались с «теоремы сложения вероятностей» (8) и «теоремы умножения вероятностей» (13), доказываемых, однако, на достаточно шаткой логической основе — и даже глубокая попытка Рихарда М и з е с а (1883—1958) строго обосновать статистический (частотный) подход к вероятностям (см., например, [32]) с современных «бурбакистских» позиций (ср. [5] или [II, § 3]) интересна, в первую очередь, в свете обсуждения вопроса о взаимоотношениях «чистой» и прикладной математики, так сказать, «математики-логики» и «математики-физики». Разумеется, формулы (8) и (13) сохранили свое значение и поныне, но они больше не рассматриваются как теоремы: первая из них переведена в разряд а к с и о м, а вторая принимается за о п р е д е л е н и е независимости событий.

Ясно, что независимыми являются события A и B, состоящие, скажем, в извлечении наугад дамы пик из тщательно перетасованной колоды в 52 карты и в выпадении шестерки на брошенной наугад игральной кости, сделанной из однородного материала: здесь $p(A) = 1/52$, $p(B) = 1/6$ и $p(AB) = 1/52 \cdot 6 = 1/312$ $(= p(A)\,p(B))$, что нетрудно вывести из «классического определения вероятности» (возможность применения которого утверждается оговорками о т щ а т е л ь н о п е р е м е ш а н н о й колоде и об о д н о р о д н о с т и игральной кости). Но вот пример, в котором заранее усмотреть независимость рассматриваемых событий гораздо труднее. Пусть мы два раза бросаем (однородную) игральную кость и пусть событие A состоит в том, что *в первый раз выпало больше очков, чем во второй*, а событие B — в том, что *в первый раз выпало нечетное число очков, а во второй — число очков, не разлагающееся на простые множители.* Эти события также независимы. В самом деле, здесь $p(A) = 15/36 = 5/12$ ибо всего мы имеем $6 \cdot 6 = 36$ равноправных результатов, которые могут иметь место в результате повторного бросания игральной кости, а удовлетворяют нашему первому условию следующие 15 пар значений выпавших очков: (6, 1), (6,2), (6,3), (6,4) (6,5); (5,1), (5,2), (5,3), (5,4); (4,1), (4,2), (4,3); (3,1), (3,2); (2,1) Далее $p(B) = 12/36 = 1/3$, ибо здесь благоприятными являются следующие 12 пар значений чисел выпавших очков: (1,1), (1,2), (1,3), (1,5); (3,1), (3,2), (3,3), (3,5); (5,1), (5,2), (5,3), (5,5). Наконец, $p(AB) = 5/36 = 5/12 \cdot 1/3 = p(A)\,p(B)$ (здесь благоприятными являются всего следующие пять пар: (3,1), (3,2), (5,1) (5,2) и (5,3)). В применении к этой паре событий A и B объяснить утверждение о том, что «осуществление или не осуществление результата A не влияет на результат B», легче всего прямой ссылкой на формулу (13).

Формальный характер определения (13) независимости приводит также к некоторым результатам, которые могли бы показаться парадоксальными при попытке ограничиться «разговорной» (или «содержательной») трактовкой этого понятия. Рассмотрим тот же круг событий, связанных с двукратным бросанием игральной кости, и пусть $Ч$ и $Н$ — события, состоящие в выпадении ч е т н о г о числа очков при 1-м бросании; выпадении н е ч е т н о г о числа очков при 2-м бросании, а событие $ОЧ$ означает, что при обоих бросаниях кости выпали количества очков о д и н а к о в о й ч е т н о с т и. Эти три события, очевидно, попарно независимы, ибо в силу классического определения вероятности $p(Ч) = p(Н) = p(ОЧ) = 1/2$; $p(Ч \cdot Н) = 1/4 = p(Ч) \cdot p(Н)$, $p(Ч \cdot ОЧ) = 1/4 = p(Ч) \cdot p(ОЧ)$ и $p(Н \cdot ОЧ) = 1/4 = p(Н) \cdot p(ОЧ)$. Однако в совокупности все т р и события уже не независимы, ибо $p(Ч \cdot Н \cdot ОЧ) = 0 \neq 1/8 = p(Ч) \cdot p(Н) \cdot (ОЧ)$ — ведь все три события одновременно иметь место никак не могут!

Таким образом, в то время как из аксиомы (8) легко выводится теорема (8′), в условии которой надо лишь потребовать, чтобы все события $A_1, A_2, \ldots, A_n$ были п о п а р н о н е с о в м е с т и м ы м и, из определения (13) никак не вытекает, что для п о п а р н о н е з а в и с и м ы х событий $A_1, A_2, \ldots, A_n$ имеет место равенство

$$p(A_1 A_2 \ldots A_n) = p(A_1)\,p(A_2) \ldots p(A_n) \qquad (5\ 13')$$

— обобщением определения (13) является о п р е д е л е н и е (13′) *независимых в совокупности* событий $A_1, A_2, \ldots, A_n$.

На условные вероятности можно распространить весьма многие свойства обыкновенных («безусловных») вероятностей. Так, например,

$$0 \leqslant p_A(B) \leqslant 1;$$

в самом деле, в силу правила (XVIб) $A \supset AB$, а следовательно (см. (10)), $p(AB) \leqslant p(A)$ и, значит, $p_A(B) = p(AB)/p(A) \leqslant 1$. При этом $p_A(B) = 0$, если событие B невозможно (ибо в этом случае $AB = AO = O$ в силу правила (Vб) и $p_A(B) = p(AB)/p(A) = 0$) или если события A и B несовместимы (ибо в этом случае также $p(AB) = 0$); $p_A(B) = 1$, если событие B достоверно (ибо в этом случае $p(AB) = p(AI) = p(A)$ в силу правила (IVб) и $p_A(B) = p(AB)/p(A) = 1$) или если $B \supset A$ [здесь также $p(AB) = p(A)$; см., правило (XVIIб)].

Далее, если события B и C несовместимы (т. е. $BC = O$), то

$$p_A(B + C) = p_A(B) + p_A(C). \tag{15.8'}$$

В самом деле в этом случае события AB и AC также несовместимы (ибо $(AB)(AC) = A(BC) = AO = O$) и, следовательно,

$$p(AB + AC) = p(AB) + p(AC),$$

откуда получаем:

$$p_A(B + C) = p[A(B + C)]/p(A) =$$
$$= p(AB + AC)/p(A) = [p(AB) + p(AC)]/p(A) =$$
$$= p(AB)/p(A) + p(AC)/p(A) = p_A(B) + p_A(C).$$

Из формулы (8′) и из того, что $p_A(I) = 1$, следует также, что

$$p_A(\overline{B}) = 1 - p_A(B). \tag{15.9'}$$

Наконец, из той же формулы (8′) нетрудно вывести, что

$$\text{если } B \supset C, \text{ то } p_A(B) \geqslant p_A(C); \tag{15.10'}$$

доказать это мы предоставим читателю.

Пусть теперь события B и C не несовместимы. В таком случае

$$p_A(B + C) = p_A(B) + p_A(C) - p_A(BC). \tag{15.11'}$$

В самом деле

$$p_A(B + C) = p[A(B + C)]/p(A) = p(AB + AC)/p(A) =$$
$$= [p(AB) + p(AC) + p(AB \cdot AC)]/p(A) =$$
$$= [p(AB) + p(AC) - p(ABC)]/p(A) =$$
$$= p(AB)/p(A) + p(AC)/p(A) - p(A \cdot BC)/p(A) =$$
$$= p_A(B) + p_A(C) - p_A(BC).$$

Заметим еще, что если $A_1, A_2, \ldots, A_n$ есть полная группа элементарных событий (если $A_1 + A_2 + \ldots + A_n = I$, $A_iA_j = O$; $i, j = 1, 2, \ldots, n$ и $i \neq j$), то при любом событии B (где $p(B) \neq 0$)

$$p(B) = p(A_1)\, p_{A_1}(B) + p(A_2) p_{A_2}(B) + \ldots + p(A_n) p_{A_n}(B). \qquad (15.16)$$

◀ В самом деле в этом случае $B = BI = B(A_1 + A_2 + \ldots + A_n) = (A_1 + A_2 + \ldots + A_n)B = A_1B + A_2B + \ldots + A_nB$. Но события $A_1B, A_2B, \ldots, A_nB$ также попарно несовместимы (ибо $(A_iB)(A_jB) = (A_iA_j)B = OB = O$) — и поэтому в силу (8′) и (12)

$$p(B) = p(A_1B + A_2B + \ldots + A_nB) = p(A_1B) + p(A_2B) + \ldots + p(A_nB) = p(A_1)\, p_{A_1}(B) + p(A_2) p_{A_2}(B) + \ldots + p(A_n)\, p_{A_n}(B). \blacktriangleright$$

[(16) называется **формулой полной вероятности.**]

Пример 1. Из тщательно перетасованной колоды в 52 карты извлекается наугад одна карта. Какова вероятность, что эта карта окажется «тузом» или «козырем» (например, картой масти пик)?

◀ Указание о «тщательно перетасованной» колоде следует понимать как предположение о том, что мы находимся в условиях классического определения вероятностей (см. с. 178), т. е, $p(T) = 4/52 = 1/13$, $p(K) = 13/52 = 1/4$ и $p(TK) = 1/52$, где T, K и TK — события, состоящие в извлечении из колоды Туза, Козыря и Козырного Туза (в колоде 52 карты, из них 13 козырей, 4 туза и 1 козырной туз). Но (см. (11)) $p(T + K) = p(T) + p(K) - p(TK) = 1/13 + 1/4 - 1/52 = 4/13$. ▶

Пример 2 (задача кавалера де Мере [1]). Что вероятнее — при четырехкратном бросании игральной кости хоть один раз получить шесть очков или в 24 бросаниях одновременно двух костей хоть раз выбросить две шестерки сразу?

◀ Пусть A_g и $B_{i,g}$ (где $i, g = 1, \ldots, 6$) — выпадение g очков, соответственно выпадение i очков на 1-й и g очков на 2-й кости; $p(A_g) = 1/6$ и $p(B_{i,g}) = 1/36$; $p(\bar{A}_g) = 5/6$ и $p(\bar{B}_{i,g}) = 35/36$ (см (9)). Нам требуется оценить $p(A_6^{(1)} + \ldots + A_6^{(4)})$ и $p(B_{6,6}^{(1)} + \ldots + B_{6,6}^{(24)})$ где число сверху указывает номер бросания. Использование (13.12) здесь громоздко. Проще использовать правило де Моргана (XIa) (см. также упр. 2.4): $\overline{A_6^{(1)} + A_6^{(2)} + A_6^{(3)} + A_6^{(4)}} = \bar{A}_6^{(1)} \bar{A}_6^{(2)} \bar{A}_6^{(3)} \bar{A}_6^{(4)}$. Но так как

[1] Страстный игрок в кости кавалер де Мере вошел в историю математики рядом содержательных задач, которые он поставил перед своим другом Блезом Паскалем (1623—1662) — великим ученым и одним из создателей теории вероятностей. [Заметим, что интерес де Мере к формулируемым им задачам был чисто практическим, так что и здесь мы сталкиваемся — правда в несколько шаржированном виде — с фактом влияния запросов практики на развитие теоретической математики.]

все события $\overline{A}_6^{(i)}$ независимы (ср. ниже упр. 3), $p(\overline{A}_6^{(1)} \ldots \overline{A}_6^{(4)}) = p(\overline{A}_6^{(1)}) \ldots p(\overline{A}_6^{(4)}) = (5/6)^4 = 625/1296$ и значит (см. (9)), $p(A_6^{(1)} + \ldots + A_6^{(4)}) = 1 - p(\overline{A_6^{(1)} + \ldots + A_6^{(4)}}) = 1 - 625/1296 = 671/1296 \approx 0{,}52$.

Далее $p(B_{6,6}^{(1)} + \ldots + B_{6,6}^{(24)}) = 1 - p(\overline{B_{6,6}^{(1)} + \ldots + B_{6,6}^{(24)}}) = 1 - p(\overline{B}_{6,6}^{(1)} \ldots \overline{B}_{6,6}^{(24)}) = 1 - p(\overline{B}_{6,6}^{(1)}) \ldots p(\overline{B}_{6,6}^{(24)}) = 1 - (35/36)^{24} \approx 0{,}49.$

Таким образом,

$p(A_6^{(1)} + \ldots + A_6^{(4)}) > p(B_{6,6}^{(1)} + \ldots + B_{6,6}^{(24)})$. ▶

Пример 3. Шесть карточек с буквами A, A, A, $П$, $П$, X перевернуты буквами книзу, тщательно перемешаны и выложены одна за другой. Какова вероятность, что, перевернув их буквами вверх, мы получим слово *ПАПАХА*?

◀ Во всех задачах, связанных с приложениями теории вероятностей, явно или неявно содержатся указания на то, как именно вводятся нормы (вероятности) в рассматриваемом пространстве событий; в данной задаче эту роль играют слова о том, что карточки «тщательно перемешиваются», имеющие в виду применимость *классического определения* вероятностей. Далее имеем

$$p(ПАПАХА) = p(П)\cdot p_П(АПАХА) =$$
$$= p(П)\cdot p_П(А)\cdot p_{ПА}(ПАХА) = \ldots =$$
$$= p(П)\cdot p_П(А)\cdot p_{ПА}(П)\cdot p_{ПАП}(А)\cdot p_{ПАПА}(X)\cdot p_{ПАПАХ}(А) =$$
$$= 2/6\cdot 3/5\cdot 1/4\cdot 2/3\cdot 1/2\cdot 1/1 = 1/60$$

(ибо $p(П) = 2/6$, $p_П(А) = 3/5$ и т. д.). ▶

Пример 4. В студенческой группе имеется n студентов. Предположим, что перед экзаменами каждый из них выучил по одному из n вопросов экзаменационной программы. Будем считать, что на экзамене вопросы раздаются студентам совершенно случайно; какова в этом случае вероятность того, что хотя бы один из студентов сдаст экзамен?

◀ Пусть событие A_i означает, что i-й студент случайно получил на экзамене выученный им вопрос; здесь $i = 1, 2, \ldots, n$. Нам требуется определить вероятность (см (13.12))

$$p(A_1 + A_2 + \ldots + A_n) = \sum_i p(A_i) - \sum_{(i,j)} p(A_iA_j) + \sum_{(i,j,k)} p(A_iA_jA_k) -$$
$$- \sum_{(i,j,k,l)} p(A_iA_jA_kA_l) + \ldots \pm p(A_1A_2A_3\ldots A_n).$$

Но $p(A_i) = 1/n$, $p(A_iA_j) = 1/[n(n-1)]$, $p(A_iA_jA_k) = 1/[n(n-1)(n-2)]$ и т. д. (ибо 2 студента могут получить 2 вопроса $n(n-1)$ способами, 3 студента — 3 вопроса $n(n-1)(n-2)$ способами и т. д.). А так как число событий A_i равно n, число событий A_iA_j равно C_n^2, число событий $A_iA_jA_k$ равно C_n и т. д., то

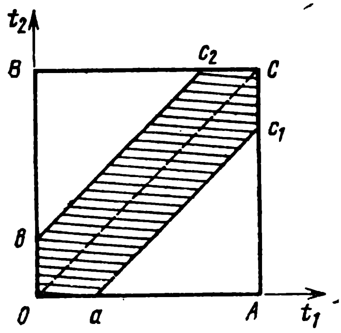


Рис. 75

$p(A_1+A_2+\dots+A_n) = n\cdot 1/n - C_n^2 \times 1/[n(n-1)] + C_n^3\cdot 1/[n(n-1)(n-2)] - \dots \pm 1/[n(n-1)(n-2)\dots 1] = n\cdot 1/n - n(n-1)/2!\cdot 1/[n(n-1)] + n(n-1)(n-2)/3!\cdot 1/[n(n-1)(n-2)] - \dots \pm 1/[n\times (n-1)(n-2)\dots 1] = 1 - 1/2! + 1/3! - \dots \pm 1/n!$.

Так как известно (см. любой курс математического анализа или [33]), что $\frac{1}{e} = e^{-1} = 1 - 1/1! + 1/2! - 1/3! + \dots$ (где $e = 2{,}71828\dots$ — основание системы натуральных логарифмов), то число $p(A_1+A_2+\dots+A_n)$ очень близко к $1 - 1/e = 0{,}63212\dots$. ▶

Пример 5 (задача о встрече). Двое лиц условились встретиться у вокзала под часами между 12 и 13 ч; при этом они договорились, что каждый пришедший ждет другого 15 мин (если он придет не позднее, чем в 12 ч 45 мин) и затем уходит. Считая, что каждое лицо с одинаковой вероятностью может прийти на свидание в любой момент между 12 и 13 ч, найдите, какова вероятность, что встреча состоится?

◀ В этой задаче роль информации о том, как именно вводятся нормы (вероятности) в рассматриваемом (бесконечном) пространстве событий, играет (с точки зрения «строгой» математики — достаточно туманное) указание на «одинаковую вероятность» прибытия каждого лица на свидание в любой момент времени; понимать его можно как утверждение, что вероятность «сложного» события, изображаемого областью A фигурирующего на рис. 75 квадрата $I = OACB$, равна площади области A. Но событие B («встреча») задается условием $|t_1 - t_2| \leqslant 1/4$, т. е. изображается шестиугольником $Ш = Oac_1Cc_2b$ (рис. 75). Поэтому $p(B) = S_Ш = S_I - S_{Aac_1} - S_{Bc_2b} = 1 - (1/2)(3/4)^2 - (1/2)(3/4)^2 = 1 - 18/32 = 7/16$. ▶

Дальнейшие примеры и задачи читатель сможет найти в любых пособиях по теории вероятностей (скажем, в [1.11, 2.17 или 34]).

Упражнения. **15.1.** Выразите а) вероятность $p(A+B+C)$ суммы трех событий; б) вероятность $p(A_1+A_2+\dots+A_n)$ суммы n событий через вероятность самих событий и их попарных, тройных, ..., и т.д произведений (вероятностный вариант формулы включений и исключений).

15.2. Студенту предстоит сдать в сессию четыре экзамена; он сам оценивает вероятность провала на каждом экзамене в 0,1, считает эти события (провалы на отдельных экзаменах) строго независимыми (полагает, что они зависят лишь от того, какой он вытащит билет). Как оценивает студент вероятность провалить сессию?

15.3. События A и B независимы; докажите независимость событий

а) A и $\bar{B}$, б) $\bar{A}$ и B, в) $\bar{A}$ и $\bar{B}$.

15.4. Имеются две тщательно перетасованные колоды карт — одна из 36 карт а вторая — из 52. Из одной колоды, которая с равными шансами может оказаться как первой, так и второй, извлекается карта. Какова вероятность, что извлечена будет «дама»; что извлечена будет «пиковая дама»?

ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ

1.2. а) $A+B$; б) A; в) $A+D$.

1.3. Воспользуйтесь методом математической индукции (по числу n).

1.4. Пусть $M=\sum\limits_{i_1, i_2, \ldots, i_k} A_{i_1}A_{i_2}\ldots A_{i_k}$ (где $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$), а $N=\prod\limits_{i_1, i_2, \ldots, i_l} (A_{i_1}+A_{i_2}+\ldots+A_{i_l})$ (где $l=n-k+1$, а Σ и Π — знаки суммы и произведения); докажите, что $M \subset N$ и что $N \subset M$ (в смысле § 3).

2.2. а) A; б) $A+B$; в) O (где O—пустое множество); г) $A+B+C$; д) $A+B$.

2.3. в) $\overline{\bar{A}+\bar{B}+C}+\overline{\bar{A}+B}+\bar{A}+C=I$ **2.4.** См. указание к упр. 1.3.

4.2. Воспользуйтесь формулой (3′).

4.3. См. указание к упр. 1.3

4.4. а) $\bar{A}+B$; б) $AB+\bar{A}\,\bar{B}\,(=A*\bar{B}=\bar{A}*B)$.

4.7. Воспользуйтесь формулой (7′)

4.9. а) Обозначим левую и правую часть доказываемого неравенства через M и N и пусть $x \in M$; тогда либо есть такое i, что $x \in A_i$, либо есть такое j, что $x \in B_j$. Пусть $x \in A_i$ где i фиксировано (разумеется, $1 \leqslant i \leqslant n$), тогда $x \notin B_j$ для всех j, где $1 \leqslant j \leqslant n$; значит, $x \in A_i * B_i$, а следовательно, и $x \in N$. Если $x \in B_j$, где j фиксировано то рассуждаем аналогично.

4.11. Воспользуйтесь тем, что $\overline{A+B}=I\diagdown(A+B)$; $\overline{AB}=I\diagdown AB$.

4.12. Ср. упр. 4.4 б)

4.16. ω задается функцией $c=f(a,b)$ двух переменных, где $a, b, c \in \{0,1\}$; здесь a (или b, или c) равны 0 или равны 1 в зависимости от того, имеем мы $x \in A$ или $x \notin A$ и $x \in B$ или $x \notin B$; $x \in C$ или $x \notin C$ соответственно, а их имеется 16.

5.1. «Двойственная разность» η элементов α и β определена при $\beta \supset \alpha$ и задается условиями $\alpha=\beta\eta$ и $\beta+\eta=\iota$; ее можно ввести формулой $\eta=\alpha+\bar{\beta}$.

5.3. 2^n (в общем случае).

6.1. а) $\alpha+\beta=\alpha\beta+\alpha\bar{\beta}+\bar{\alpha}\beta$.

6.4. При $k=1$ имеем структуру из 4 элементов (см. § 10).

7.6. а) $\alpha \mid \beta=[(\alpha\downarrow\alpha)\downarrow(\beta\downarrow\beta)]\downarrow[(\alpha\downarrow\alpha)\downarrow(\beta\downarrow\beta)]$;
$\alpha\downarrow\beta=[(\alpha\mid\alpha)\mid(\beta\mid\beta)]\mid[(\alpha\mid\alpha)\mid(\beta\mid\beta)]$.

8.1. Искомое число равно количеству различных последовательностей из k нулей и единиц (где приписанная определенному элементу $\alpha \in I$ единица означает, что α входит в рассматриваемое подмножество, а нуль — что не входит).

8.4. Подставим в P_7': $\lambda+\lambda\mu=\lambda$ вместо μ элемент $\lambda+\lambda \in \mathscr{L}$; получим $\lambda+\lambda(\lambda+\lambda)=\lambda$; но в силу P_7' (где только μ заменено на λ) $\lambda(\lambda+\lambda)=\lambda$; поэтому $\lambda+\lambda=\lambda$.

8.5. а) Это утверждение двойственно (9).

8.6. б) Так как $\lambda+\mu\supset\lambda\supset\lambda\mu$, $\mu+\nu\supset\mu\supset\lambda\mu$ и $\nu+\lambda\supset\lambda\supset\lambda\mu$, то и $\Lambda=(\lambda+\mu)(\mu+\nu)(\nu+\lambda)\supset\lambda\mu$. Аналогично устанавливается, что $\Lambda\supset\mu\nu$ и $\Lambda\supset\nu\lambda$, откуда и следует требуемое неравенство.

8.7. Для случая немодулярной решетки см. упр. 10 в); если же $\mathbf{L}$ модулярна, но не дистрибутивна, то в силу упр. 6 существуют $\lambda, \mu, \nu \subset \mathscr{L}$ такие, что неравенство упр. 6б) не обращается в равенство; но тогда элементы $\Lambda=(\lambda+\mu)(\mu+$

$+\nu)(\nu+\lambda)$, $M=\lambda\mu+\mu\nu+\nu\lambda$, $\alpha=\Lambda(M+\lambda)$ $(=M+\lambda\Lambda)$, $\beta=$ $=\Lambda(M+\mu)$ $(=M+\mu\Lambda)$ и $\gamma=\Lambda(M+\nu)$ $(=M+\nu\Lambda)$ образуют решетку, изоморфную решетке рис. 31,*б*.

8.10. в) Решетка L не модулярна, если существуют λ, μ, $\nu\in\mathscr{L}$ такие, что $\lambda\supset\nu$ и $\lambda(\mu+\nu)\supset\lambda\mu+\nu$; далее рассмотрите элементы α, β, γ, δ, ε.

8.11. а) Она содержит пять попарно неизоморфных подструктур.

8.15. а) Множество всевозможных «конечных сумм» (т. е. объединений) всевозможных полуинтервалов $\{x\mid x\in\mathscr{R}$ и $a<x\leqslant b\}$ вещественной оси $\mathscr{R}$ (где возможны также значения $b=\infty$ и $a=-\infty$).

б) Например, алгебра высказываний, где логически эквивалентные высказывания отождествляются между собой или фактор-структура структуры всех подмножеств бесконечного множества по идеалу конечных множеств.

9.2. $\alpha\dot{-}\beta=\alpha*\beta$.

9.8. а) Если $\alpha\in J$ и $\bar\alpha\in J$, то $\iota=\alpha+\bar\alpha\in J$, т. е. J совпадает со всей структурой и не является собственным идеалом; отсюда также следует, что идеал J, удовлетворяющий условиям упражнения, является максимальным: к нему нельзя присоединить ни одного элемента, не расширив его сразу же до в с е й структуры. Если же для идеала J существует такое $\alpha\in\mathscr{B}$, что и $\alpha\notin J$ и $\bar\alpha\notin J$, то множество $\{J,\alpha\}$ порождает содержащий J собственный идеал

9.9. Проверьте выполнение условий (21).

9.11. Доказательство (включающее и некоторые тонкости) опирается на результат упр. 8а), из которого, в частности, сразу следует, что $A_{\bar\alpha}=\bar A_\alpha$; несложно проверяются и условия: $A_{\alpha+\beta}=A_\alpha+A_\beta$; $A_{\alpha\beta}=A_\alpha A_\beta$; $A_\iota=I$, $A_o=O$.

10.4. б) $(n_1+1)(n_2+1)\ldots(n_k+1)$

10.5. Воспользуйтесь определениями (13а) — (13в) (или (14а) — (14в)).

11.3. Все фигуры — многоугольные, черные, большие и округлые.

11.4. Эти условия непротиворечивы, но их можно упростить, они равносильны требованиям: «все *B* суть *A*» и «ни один *C* не есть *A*».

11.5. Прав был первый химик (его высказывание тождественно истинно).

11.6. Все девицы были либо благовоспитаны и молоды, но невеселы и некрасивы, либо веселы и красивы, но неблаговоспитаны и немолоды.

12.2. Мостиковая схема может включать семь контактов.

13.2. б) При $n=1$ формула (12) тривиальна и при $n=2$ была доказана [см. (9)]. Далее воспользуйтесь методом математической индукции.

13.3. Воспользуйтесь формулой включений и исключений (12).

13.5. а) При $(r-1)/n\leqslant\sigma\leqslant r/n$, где $r=1,2,\ldots,n$, ответ $[(r-1)/C_n^2]\times$ $\times[n\sigma-r/2]$; б) при $(r-1)/n\leqslant\sigma\leqslant r/n$ ответ $\left(C_{r-1}^{k-1}/C_n^k\right)\{n\sigma-[(k-1)/k]\,r\}$;

в) при $C_{r-1}^l/C_n^l\leqslant\sigma\leqslant C_r^l/C_n^l$ искомая величина равна $\left[C_{r-1}^{k-1}/\left(C_n^kC_{r-1}^{l-1}\right)\right]\times$ $\times\left\{C_n^l\sigma-[(k-l)/k]\,C_r^l\right\}$ (см. [35], решение задачи 60).

14.3. Полную систему функций образует лишь набор б).

14.4. а) Лишь операции $\mid$ и $\downarrow$ (см. с. 61—62).

14.7. а) «Функция большинства» 5 переменных имеет вид $f=p_0p_1p_2+$ $+p_0p_1p_3+p_0p_1p_4+\ldots+p_2p_3p_4=(p_0+p_1+p_2)(p_0+p_1+p_3)\ldots(p_2+$ $+p_3+p_4)$ (ср. упр. 1.4).

б) Соответствующая функция: $p_0(p_1p_2+p_1p_3+p_1p_4+p_2p_3+p_2p_4+$ $+p_3p_4)=p_0[(p_1+p_2+p_3)(p_1+p_2+p_4)(p_1+p_3+p_4)(p_2+p_3+p_4)]$.

15.2. Вероятность провала сессии равна 0,3439.

15.3. в) $p(\bar A\bar B)=p(\overline{A+B})=1-p(A+B)=1-[p(A)+p(B)-$ $-p(A)p(B)]=(1-p(A))(1-p(B))=p(\bar A)p(\bar B)$.

15.4. Воспользуйтесь формулой полной вероятности (16).

СПИСОК ЛИТЕРАТУРЫ

I. **Bool G.** An Investigation of the Laws of Thought, on which are Founded the Mathematical Theories of Logic and Probabilities. — London, 1854. Последнее издание. New York: Dover, 1958.

II. **Яглом И. М.** Математические структуры и математическое моделирование. — М.: Сов. радио, 1980.

ОБЩИЕ СОЧИНЕНИЯ ПО ТЕОРИИ БУЛЕВЫХ СТРУКТУР (БУЛЕВЫХ АЛГЕБР), МАТЕМАТИЧЕСКОЙ ЛОГИКЕ, ТЕОРИИ МНОЖЕСТВ И ТЕОРИИ ВЕРОЯТНОСТЕЙ

1 Книги для начинающих

1.1. **Яглом И. М.** Необыкновенная алгебра.— М.: Наука. 1968.

1.2. **Калужнин Л. А.** Что такое математическая логика.— М.: Наука, 1964; Элементы теории множеств и математической логики в школьном курсе математики.— М.: Просвещение, 1978.

1.3. **Гжегорчик А.** Популярная логика: Пер. с польск.— М.: Наука, 1979.

1.4. **Фрейденталь X.** Язык логики: Пер. с англ./Под ред. Ю. А. Гастева.— М.: Наука, 1969.

1.5 **Беркли Э.** Символическая логика и разумные машины: Пер. с англ./Под ред. Г Н Поворова.— М.: ИЛ, 1961.

1.6 **Столл Р. Р.** Множества. Логика. Аксиоматические теории: Пер. с англ./ Под ред. Ю. А. Шихановича.— М.: Просвещение, 1968.

1.7 **Хилтон А. М.** Логика и цепи переключения Пер. с англ./Под ред. Г. М. Уланова.— М.— Л.: Госэнергоиздат, 1962.

1.8. **Кэррол Льюис.** История с узелками: Пер.с англ. /Под ред. Я. А. Смородинского. — М.: Мир, 1973.

1.9. **Виленкин Н. Я.** Рассказы о множествах.— М.: Наука, 1969.

1.10. **Гнеденко Б. В., Хинчин А. Я.** Элементарное введение в теорию вероятностей.— М.: Наука, 1976.

1.11. **Мостеллер Ф., Рурке Р., Томас Дж.** Вероятность: Пер. с англ./Под ред. И. М. Яглома.— М.: Мир, 1969.

1.12. **Кофман А., Фор Р.** Займемся исследованием операций: Пер. с франц./ Под ред. А. А. Корбута.— М.: Мир, 1968.

1.13 **Кальбертсон Дж.** Математики и логика цифровых устройств. Пер. с англ./ Под ред. И. М. Яглома.— М.: Просвещение, 1965.

1.14. **Ивс Г., Нюсом К. В.** О математической логике и философии математики: Пер. с англ.— М.: Знание, 1968.

1.15. **Gardner M.** Logic Machines and Diagrams.— New York: McCraw-Hill, 1958.

1.16 **Rueff M., Jeger M.** Sets and Boolean Algebra.— London: George Allen and Unwin, 1970.

1.17. **Hohn F. E.** Applied Boolean Algebra.— New York: Macmillan, 1960.

1.18. **Flores I.** Logic of Computer Arithmetic.— Englewood Cliffs: Prentice-Hall, 1963.

1.19. **Strombach W., Emde H., Reyersbach W.** Mathematische Logik. — München: C. H. Beck, 1972.

2. Учебные пособия и книги, близкие к ним по уровню изложения

2.1. Дж. Кемени, Дж. Снелл, Дж. Томпсон. Введение в конечную математику: Пер. с англ./Под ред. И. М. Яглома.— М.: Мир, 1964.
2.2. Гиндикин С. Г. Алгебра логики в задачах.— М.: Наука, 1972.
2.3. Кузичев А. С. Диаграммы Венна.— М.: Наука, 1968.
2.4. Линдон Р. Заметки по логике.: Пер. с англ./Под ред. И. М. Яглома.— М.: Мир, 1968.
2.5. Манин Ю. И. Доказуемое и недоказуемое.— М.: Сов. радио, 1979.
2.6. Тарский А. Введение в логику и методологию дедуктивных наук: Пер. с англ./Под ред. С. А. Яновской.— М.: ИЛ, 1948.
2.7. Гильберт Д., Аккерман В. Основы теоретической логики: Пер. с нем./Под ред. С. А. Яновской.— М.: ИЛ, 1947.
2.8. Новиков П. С. Элементы математической логики.— М.: Наука, 1973.
2.9. Клини С. Математическая логика: Пер. с англ./Под ред. Г. Е. Минца.— М.: Мир, 1973.
2.10. Мендельсон Э. Введение в математическую логику: Пер. с англ./Под ред. С. И. Адена.— М.: Наука, 1976.
2.11. Карри X. Основания математической логики: Пер. с англ./Под ред. Ю. А. Гастева.— М.: Мир, 1969.
2.12. Гудстейн Р. Л. Математическая логика: Пер. с англ./Под ред. С. А. Яновской.— М:. ИЛ, 1961.
2.13. Колдуэлл С. Логический синтез релейных устройств: Пер. с англ./Под ред. М. А. Гаврилова.— М.: ИЛ, 1962.
2.14. Бурбаки Н. Теория множеств: Пер. с франц./Под ред. В. А. Успенского.— М.: Мир, 1965.
2.15. Шиханович Ю. А. Введение в современную математику.—М.: Наука, 1965.
2.16. Фор Р., Кофман А., Дени-Папен М. Современная математика: Пер. с франц./Под ред. А. Н. Колмогорова. — М.: Мир, 1966.
2.17. Феллер В. Введение в теорию вероятностей и ее приложения: Пер. с англ./Под ред. Е. Б. Дынкина.— М.: Наука, 1967.—Т.1.
2.18. Биркгоф Г. Теория структур: Пер. с англ.— М.: ИЛ, 1952.
2.19. Биркгоф Г., Барти Т. Современная прикладная алгебра: Пер. с англ.— М.: Мир, 1976.
2.20. Эдельман С. Л. Математическая логика.— М.: Высшая школа, 1975.
2.21. Сборник задач по математической логике и теории множеств./А.В. Гохман, М. А. Спивак, Г. И. Житомирский и др.— Саратов: СГУ, 1965.
2.22. Лавров И. А., Максимова Л. Л. Задачи по теории множеств математической логике и теории алгоритмов.— М.: Наука, 1975.
2.23. Mendelson E. Boolean Algebra and Switching Circuits.—New York: McGraw-Hill, 1970.
2.24. Flegg H. G. Boolean Algebra and its Applications.—New York: Wiley, 1964.
2.25. Hoernes G., Heilweil M. Introduction to Boolean Algebra and Logic Design.— New York: McGraw-Hill, 1964.
2.26. Whitesitt J. E. Boolesche Algebra und Anwendungen.— Braunschweig: Vieweg, 1969.

3. Монографии и учебники повышенной трудности

3.1. Владимиров Д. А. Булевы алгебры.— М.: Наука, 1969.
3.2. Сикорский Р. Булевы алгебры: Пер. с англ.— М.: Мир, 1969.
3.3. Клини С. Введение в метаматематику: Пер. с англ./Под ред. В. А. Успенского.— М.: ИЛ, 1957.
3.4. Расёва Е., Сикорский Р. Математика метаматематики: Пер. с англ.— М.: Наука, 1972.
3.5. Чёрч А. Введение в математическую логику: Пер. с англ./Под ред. В. А. Успенского.— М.: ИЛ, 1960. — Т.1.
3.6. Шенфилд Дж. Математическая логика: Пер. с англ./Под ред. Ю.Л. Ершова. — М.: Наука, 1975.

3.7. **Слупецкий Е., Борковский Л.** Элементы математической логики и теории множеств Пер. с польск./Под ред. И. Н. Коваленко.—М.: Прогресс, 1965.
3.8. **Куратовский К., Мостовский А.** Теория множеств: Пер. с англ./Под ред. А. Д. Тайманова.— М.: Мир, 1970.
3.9. **Halmos P. R.** Lectures on Boolean Algebras. — Toronto — New York — London: van Nostrand, 1963.
3.10. **Goodstein P. L.** Boolean Algebra.— Oxford: Pergamon, 1963.
3.11. **Halmos P. R.** Algebraic Logic. — New York: Chelsea, 1962.
3.12. **Manin Y. I.** A Curse in Mathematical Logic.— New York — Heidelberg — Berlin: Springer, 1977.
3.13. **Henkin L.** La structure algebrique des theories mathematiques.— Paris: Gauthier-Villars, 1956.

ЛИТЕРАТУРА К ОТДЕЛЬНЫМ ГЛАВАМ КНИГИ

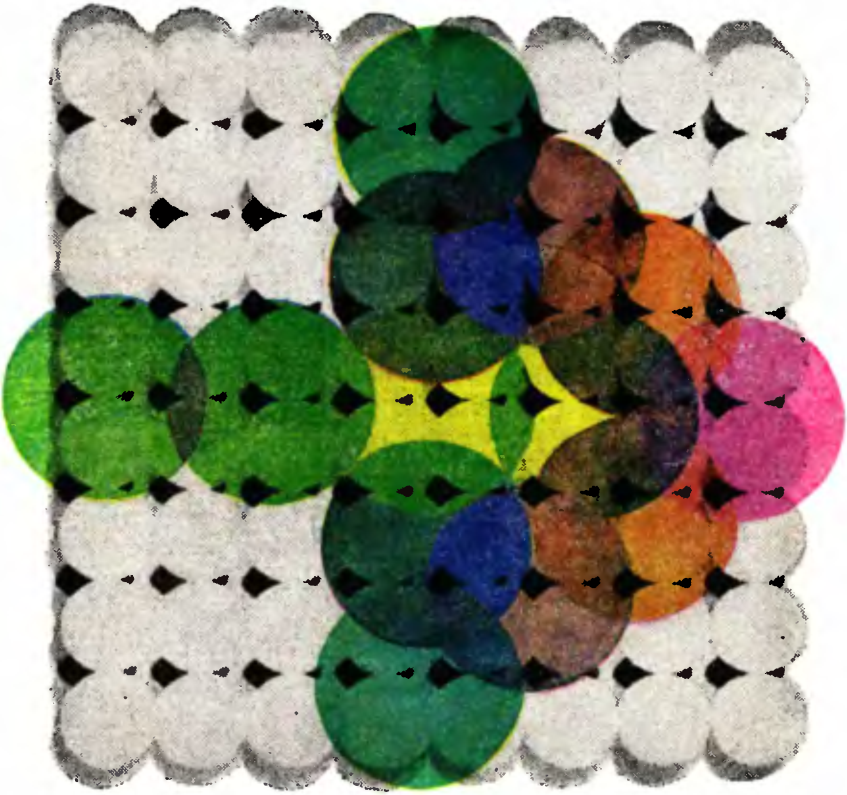
1. **Яглом И. М.** Комплексные числа и их применение в геометрии.— М.: Физматгиз, 1963.
2. **Арнольд И. В.** Теоретическая арифметика.— М.: Учпедгиз, 1939; **Кантор И. Л., Солодовников А. С.** Гиперкомплексные числа.— М.: Наука, 1973.
3. **Курош А. Г.** Лекции по общей алгебре.— М.: Наука, 1973; **Калужнин Л. А.** Введение в общую алгебру.— М.: Наука, 1973; **Кострикин А. И.** Введение в алгебру.— М.: Наука, 1977; **ван дер Варден Б. Л.** Алгебра: Пер. с нем./Под ред. Ю. И. Мерзлякова.— М.: Наука, 1976; **Ленг С.** Алгебра: Пер. с англ./Под ред. А. И. Кострикина.— М.: Мир, 1968.
4. **Скорняков Л. А.** Элементы теории структур.— М.: Наука: 1970; **Hermes H.** Einführung in die Verbandtheorie.— Berlin: Springer, 1955; **Szasz G.** Introduction to Lattice Theory. — New York: Academic Press, 1963.
5. **Бурбаки Н.** Алгебра (алгебраические структуры; линейная и полилинейная алгебра): Пер. с франц.— М.: Физматгиз, 1962; **Бурбаки Н.** Очерки по истории математики: Пер. с франц./Под ред. К. А. Рыбникова.— М.: ИЛ, 1963.— Архитектура математики, с. 245—259.
6. **Маркушевич А. И.** Деление с остатком в арифметике и алгебре. — М.: Изд. Акад. пед. наук РСФСР, 1942; **Калужнин Л. А.** Основная теорема арифметики.— М.: Наука, 1969; **Бельский А. А., Калужнин Л. А.** Деление с остатком.— Киев: Вища школа, 1977.
7. **Головина Л. И.** Линейная алгебра и некоторые ее приложения. — М.: Наука, 1975; **Шилов Г. Е.** Математический анализ (конечномерные векторные пространства).— М.: Наука, 1969; **Халмош П.** Конечномерные векторные пространства: Пер. с англ.— М.: Физматгиз, 1963.
8. **Бахман Ф., Шмидт Э.** n-угольники: Пер. с нем./Под ред. И. М. Яглома. — М.: Мир, 1973.
9. **Лопшиц А. М.** Вычисление площадей ориентированных фигур.— М.: Гостехиздат, 1956.
10. **Пойа Д.** Математика и правдоподобные рассуждения: Пер. с англ./Под ред. С. А. Яновской.— М.: Наука, 1975.
11. **Блехман И. И., Мышкис А. Д., Пановко А. Г.** Прикладная математика: предмет, логика, особенности подходов.— Киев: Наукова думка, 1976.
12. **Аристотель.** Сочинения в 4-х т.: Пер. с древнегреч./Под ред. З. Н. Микеладзе.— М.: Мысль, 1978.— Т.2.
13. **Лукасевич Я.** Аристотелевская силлогистика с точки зрения современной формальной логики: Пер. с англ./Под ред. П. С. Попова.— М.: ИЛ, 1959.
14. **Эренфест П. С.** Рецензия на книгу Л. Кутюра «Алгебра логики». — Журнал русского физ.-хим. общ-ва, физ. отдел., 42, отд. 2, вып. 10, 1910, с. 382—387.
15. **Шеннон К.** Символический анализ релейных и переключательных цепей.— В кн.: Работы по теории информации и кибернетике: Пер. с англ./Под. ред. Р. Л. Добрулина и О. В. Лупанова.— М.: ИЛ, 1943, с. 9—45: **Шестаков В. И.**

Некоторые математические методы конструирования и упрощения двухполюсных электрических схем класса А. Канд. дисс. МГУ.— М.: 1938; Алгебра двухполюсных схем, построенных исключительно из двухполюсников (алгебра А-схем). — Журнал технич. физики, 1941, т. 11, № 6, с. 532—549; Представление характеристических функций предложений посредством выражений, реализуемых релейно-контактными схемами.— Изв. АН СССР. Сер. мат. 1946, 10, с. 529—565; Математическая логика и автоматика.— Математика в школе, 1958, № 6, с. 4—20; 1959, № 1, с. 19—39.

16. **Лузин Н. Н.** Теория функций действительного переменного.— М.: Учпедгиз 1940.
17. **Лебег А.** Об измерении величин: Пер. с франц./Под ред. И.М. Яглома. — М.: Учпедгиз, 1960; **Рохлин В. А.** Площадь и объем.— Энциклопедия элементарной математики./Под ред. В. Г. Болтянского и И. М. Яглома.— М.: Наука, 1966. — Кн V: Геометрия, с 5—87.
18. **Виленкин Н. Я.** Комбинаторика.— М.: Наука, 1960; Популярная комбинаторика— М.: Наука, 1975.
19. **Яглом И. М., Болтянский В. Г.** Выпуклые фигуры.— М.— Л.: Гостехиздат, 1951.
20. **Штейнгауз Г.** Сто задач: Пер. с польск. — М.: Наука 1976.
21. **Яглом И. М., Файнберг Е. И.** Оценки для вероятностей сложных событий. — Труды VI Всесоюзного совещания по теории вероятностей и математической статистике.— Вильнюс, 1962, с. 297 — 303; **Пирогов С. А.** Вероятности сложных событийи линейное программирование.— Теория вероятностей и ее применения, 1968 13, № 2, с. 344—348.
22. **Виноградов И. М.** Основы теории чисел.— М.: Наука, 1972.
23. **Яглом А. М., Яглом И. М.** Вероятность и информация.— М.: Наука, 1973.
24. **Яблонский С. В., Гаврилов Г. П., Кудрявцев В. В.** Функции алгебры логики и классы Поста:— М.: Наука, 1966; **Яблонский С. В.** Функциональные построения в k-значной логике.— Труды Математического Института им. В. А. Стеклова АН СССР, 1958, т. 51, с. 5—142.
25. **Полетаев И. А.** Сигнал— М.: Сов. радио, 1958.
26. **Бернштейн С. Н.** Опыт аксиоматического обоснования теории вероятностей. — Записки матем. товарищества. Харьков, 1917, (2) 15, с. 209—274.
27. **Колмогоров А. Н** Основные понятия теории вероятностей. —М.: Наука, 1974.
28. **Борель Э.** Случай: Пер. с франц./Под ред. В. А. Костицина.— М.:— Пг.: Гиз, 1923.
29. **Заде Л.** Понятие лингвистической переменной и его применение к принятию приближенных решений: Пер. с англ./Под ред. Н. Н. Моисеева и С. А. Орловского. — М.: Мир, 1976.
30. **Kaufmann A.** Introduction á la theorie des sous-ensembles flous: Tomes 1—3 — Paris: Masson; 1974—75; **Kaufmann A., Dubois T., Cools M.** — Exercices avec solutions sur la theorie des sous-ensembles flous — Paris: Masson, 1975.
31. **Розенфельд В. А., Яглом И. М.** Многомерные пространства.— Энциклопедия элементарной математики./Под ред. В. Г. Болтянского и И. М. Яглома. М.. Наука, 1966. — Кн. V: Геометрия, с. 349—392.
32. **Мизес Р.** Вероятность и статистика: Пер. с нем./Под ред. А. Я Хинчина.—М. — Л.. Гиз, 1930.
33. **Маркушевич А. И.** Ряды.— М.: Наука, 1979; **Шерватов В. Г.** Гиперболические функции.— М., Физматгиз 1958.
34. **Мостеллер Ф.** Пятьдесят занимательных вероятностных задач с решениями: Пер. с англ. /Под ред. Ю.В. Линника.— М.: Наука, 1975; **Мешалкин Л. Л.** Сборник задач по теории вероятностей. — М.. МГУ, 1963; **Яглом А. М., Яглом И. М.** Неэлементарные задачи в элементарном изложении.— М.: Гостехиздат, 1954.
35. **Шклярский Д. О., Ченцов Н. Н., Яглом И. М.** Геометрические оценки и задачи из комбинаторной геометрии.— М.: Наука, 1974.

ОГЛАВЛЕНИЕ

КИБЕРНЕТИКА



И. М. ЯГЛОМ

БУЛЕВА СТРУКТУРА И ЕЕ МОДЕЛИ