**С. Б. Гашков, А. Б. Фролов**

# ДИСКРЕТНАЯ МАТЕМАТИКА

УЧЕБНИК И ПРАКТИКУМ ДЛЯ ВУЗОВ

3-е издание, исправленное и дополненное

*Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по естественнонаучным направлениям*

**Книга доступна в электронной библиотеке biblio-online.ru, а также в мобильном приложении «Юрайт.Библиотека»**

**Москва ▪ Юрайт ▪ 2019**

УДК 51(075.8)
ББК 22.176я73
Г24

***Авторы*:**

**Гашков Сергей Борисович** — доктор физико-математических наук, профессор кафедры дискретной математики отделения математики механико-математического факультета Московского государственного университета имени М. В. Ломоносова;

**Фролов Александр Борисович** — профессор, доктор технических наук, профессор кафедры математического моделирования Института автоматики и вычислительной техники Национального исследовательского университета «Московский энергетический институт».

***Рецензенты*:**

*Бабаш А. В.* — профессор, доктор физико-математических наук, профессор кафедры информационной безопасности Национального исследовательского университета «Высшая школа экономики»;

*Вагин В. Н.* — профессор, доктор технических наук, профессор кафедры прикладной математики Национального исследовательского университета «Московский энергетический институт».

**Гашков, С. Б.**

Г24 Дискретная математика : учебник и практикум для вузов / С. Б. Гашков, А. Б. Фролов. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 483 с. — (Высшее образование). — Текст : непосредственный.

ISBN 978-5-534-11613-7

В книге отражены разделы дискретной математики, предусматриваемые учебными программами классических, национальных исследовательских и технических университетов. При соблюдении необходимого уровня доказательности рассматриваются задачи, встречающиеся в инженерной практике, для формализации которых необходимы математические модели дискретной математики — теоретико-множественные, комбинаторно-логические, автоматные, графовые, функциональные, алгебраические и др. Существенное внимание уделено принципам построения алгоритмов решения задач дискретной математики на базе известных моделей вычислений (рекурсия, ветвления и ограничения и т. п.) и оценкам их сложности в контексте общей теории сложности алгоритмов. По каждой главе даны задачи и теоретические упражнения.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

*Для студентов, слушателей факультетов повышения квалификации, специалистов, преподавателей и программистов, использующих методы дискретной математики.*

УДК 51(075.8)
ББК 22.176я73



ISBN 978-5-534-11613-7

# Оглавление

# Предисловие

Книга основана на лекциях по дискретной математике, читавшихся авторами в течение многих лет соответственно в МГУ имени М. В. Ломоносова и НИУ «МЭИ». Курсы дискретной математики в классических, национальных исследовательских и технических университетах имеют свои особенности. В технических вузах в курсы дискретной математики включают обычно элементы общей алгебры, логики и теории чисел, а в классических университетах — нет, так как в них читаются отдельные курсы по этим темам. Мы хотели написать книгу, равно пригодную для изучения дискретной математики студентами и технических вузов, и университетов, поэтому первая глава посвящена элементам теории множеств, в третьей главе, наряду с алгеброй множеств, появляются высказывания и предикаты, в четвертой главе — частично-упорядоченные множества и их наиболее важный класс — решетки, и заканчивается она установлением тесной связи одного из видов решеток с булевыми алгебрами.

Мы старались сделать изложение максимально простым, поэтому не выдвигали на первый план абстрактное понятие булевой алгебры, а вместо него разбирали конкретные его разновидности, а именно алгебры высказываний, множеств, предикатов и один из видов решеток. Вторая глава посвящена функциям алгебры логики, технически она, по-видимому, сложнее третьей и четвертой, но поставлена она на второе место потому, что рассматриваемые в ней объекты более просты и менее абстрактны в сравнении с третьей и четвертой главами. Кроме того, обычно именно с функций алгебры логики начинаются курсы дискретной математики в университетах. Ввиду ограничения на объем книги эта глава не имеет продолжения, посвященного функциям многозначных логик, хотя в университетах их обычно изучают.

Пятая глава содержит элементы комбинаторики. Она является одной из наиболее технически трудных глав и ее объем превышает обычно отводимый комбинаторике в курсах дискретной математики. Шестая глава посвящена теории графов. В ней ощутим уклон в прикладную тематику, а некоторые затронутые в ней вопросы рассматриваются потом в десятой главе. В седьмой главе, довольно абстрактной по содержанию (чем и объясняется ее позиция в книге), излагаются элементы логики предикатов с кванторами по предметным переменным. Эта тема в университетах входит в курсы логики, но в технических вузах часто попадает в дискретную математику. Вопросы, связанные с аксиомати-

зацией исчисления предикатов и теорией логического вывода, в этой главе не рассматриваются.

Восьмая глава посвящена сложности булевых функций (в технической терминологии — синтезу логических схем и их тестированию). Ее изучение предполагает знание второй главы и знакомство с пятой и шестой. В ней приведены не самые сильные из известных результатов, а только те, которые имеют достаточно простые доказательства. В девятой главе излагаются элементы теории автоматов. Ее изучение предполагает знакомство в той или иной степени со всеми предыдущими главами книги, кроме седьмой.

В десятой главе дается краткое введение в теорию алгоритмов, которой в университетах обычно посвящаются отдельные курсы. Она продолжается одиннадцатой главой, посвященной теории *NP*-полных задач. Во многих учебниках дискретной математики эта тема почти не затрагивается, и мы посчитали уместным дать ее сравнительно развернутое изложение.

Двенадцатая глава содержит очень краткое введение в общую алгебру и сравнительно подробное — в теорию конечных полей (которой обычно в курсах алгебры уделяется мало внимания), также в ней излагаются простейшие факты об эллиптических кривых над конечными полями. Знакомство с конечными полями полезно при чтении тринадцатой главы, посвященной теории самокорректирующихся кодов, в которой подробно рассматриваются наиболее популярные в приложениях коды (Хемминга, Рида — Соломона и Боуза — Чоудхури — Хоквингема). Из-за ограничения объема за рамками книги осталось алфавитное кодирование (но оно подробно изложено во многих учебниках дискретной математики).

При изучении последней, четырнадцатой главы, посвященной криптографическим приложениям, читатель также может воспользоваться знаниями, полученными в двенадцатой главе. В ее первой половине разъясняются основные принципы работы автоматов, генерирующих линейные рекуррентные последовательности (эта тема продолжает линии, начатые в пятой и девятой главах). В заключительной части главы описаны системы цифровой подписи, основанные на использовании эллиптических кривых, принятые недавно в качестве стандарта в России.

Каждая из глав дает лишь краткое введение в соответствующую тематику. Все они могли бы иметь существенно бóльшие размеры, если бы не ограничение на объем книги (и на продолжительность реально читаемого курса). Некоторые из включаемых в курсы дискретной математики тем нам пришлось по упомянутой причине оставить за рамками изложения. Желающих глубже ознакомиться с вопросами, не затронутыми в книге, мы направляем к списку литературы в ее конце. Большинство книг из этого списка мы использовали, не указывая, как принято в учебной литературе, явно ссылок на них внутри текста. Наибольшее влияние на наше изложение оказали книги [13, 33] — на из-

ложение функций алгебры логики во второй главе; [20] — на изложение теоретических основ сложности таких функций в связи с анализом и синтезом логических схем в восьмой главе, а также на изложение логики высказываний и логики предикатов в седьмой главе; первое издание книги [17] — на изложение теории конечных автоматов в девятой главе. Первое издание учебника [3], развитием которого является настоящее издание, использовано при изложении теории отношений и теории графов. На изложение алгебраических вопросов в двенадцатой главе оказали влияние книги [9, 23], а комбинаторики — [27].

С целью облегчения понимания излагаемого материала и несмотря на ограничения на объем, в книгу помещено большое количество рисунков и иллюстрирующих примеров. В конце каждой главы имеется список задач (иногда короткий, а иногда и довольно длинный), среди которых есть как легкие, так и трудные. Желающих глубже изучить дискретную математику и потренироваться в решении задач мы направляем к соответствующим сборникам задач, один из которых [28] параллельно нашей книге вышел в издательстве «Юрайт».

В настоящем издании устранены замеченные авторами неточности первого издания. Для придания учебнику внутренней завершенности добавлены разделы по алгоритмам, упоминаемым в одиннадцатой главе в первом издании. Кроме того, данная глава дополнена примерами и упражнениями, как и пятая глава, в которую также включен параграф по теории перечисления Пойа. Добавлен ряд ссылок на используемые источники.

Авторы признательны А. В. Бабашу, В. Н. Вагину и П. А. Макарову за поддержку данного издания и полезные замечания, а также автору задачника [28] Ю. В. Таранникову, участвовавшему в формировании содержания книги и обсуждении путей изложения материала.

Данное издание подготовлено частично при финансовой поддержке РФФИ, проекты № 14-01-00671а, 17-01-00485а и 19-01-00294а.

# Глава 1
# МНОЖЕСТВА И ОТНОШЕНИЯ

Алфавиты стали более знакомыми, и теперь, кроме букв, стали попадаться и цифры — в порядках, которые я не сразу узнала.

*Т. Скарлетт*. «Наваждение Люмаса»

---

В результате освоения главы 1 студент должен:

***знать***

- основные понятия и простейшие результаты теории множеств;

***уметь***

- пользоваться языком множеств и отношений для формулировки математических утверждений;

***владеть***

- приемами работы с конечными и счетными множествами и отношениями.

---

## 1.1. Множества и булеаны

Понятие множества является исходным понятием, лежащим в основе большинства математических структур.

**Определение 1.1.** *Множество* — это совокупность объединенных общим свойством попарно различимых объектов.

Это определение интуитивно ясно и не требует уточнения понятий объекта и объединяющего их общего свойства.

Теорию множеств, основанную на этом определении, называют наивной теорией множеств. Ее создателем был уроженец Санкт-Петербурга немецкий математик Георг Кантор (1845—1918). Интуитивный характер этого определения привел к появлению парадоксов, самым известным из которых является парадокс Рассела. В занимательной форме он называется парадоксом брадобрея: он решил брить тех и только тех жителей города, которые не бреются самостоятельно. Брить ли ему самого себя? Если брить, то он бреется самостоятельно, значит, брить себя не должен, а если не брить, то он не бреется самостоятельно, значит, брить себя должен. Это обстоятельство вызвало неприятие наивной теории множеств многими математиками. Поэтому возникли аксиоматическая теория множеств, в которой аксиоматика построена так,

чтобы избежать всех известных парадоксов[1], и даже такие направления в математике, как интуиционизм[2] и конструктивизм[3], в которых вообще избегают употребления теоретико-множественных понятий. Но для изучения большинства математических понятий приведенное определение всех вполне устраивает. Упоминаемое в нем объединяющее свойство в самом общем понимании — это свойство объектов быть *элементом* данного множества (или принадлежать множеству): пишут $a \in A$, если объект $a$ является элементом множества $A$, и $a \notin A$, если не является.

Множества обычно обозначают прописными латинскими буквами, возможно, с индексами. При этом $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ являются стандартными обозначениями множеств натуральных, целых, рациональных, действительных и комплексных чисел.

*Конечные* множества содержат конечное число элементов. Как правило, они задаются перечислением (в фигурных скобках) обозначений элементов: $A = \{a_1, a_2, \ldots, a_k\}$. При этом порядок перечисления элементов не существенен: множества, являющиеся совокупностями одних и тех же элементов, считаются равными, данное отношение множеств обозначается знаком равенства: $\{a_1, a_2, \ldots, a_k\} = \{a_k, a_2, \ldots, a_1\}$. Прочие множества являются *бесконечными*, например бесконечны множества $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$. Элементами множеств могут быть элементы различных математических структур. Множество, не содержащее элементов, называется *пустым* множеством и обозначается $\varnothing$. Число элементов конечного множества $A$ обозначается $|A|$. Если $|A| = n$, то множество $A$ называется $n$-множеством. Ясно, что $|\varnothing| = 0$.

Если все элементы множества $A$ являются элементами множества $B$, то множество $A$ называется *подмножеством* множества $B$ (обозначение $A \subseteq B$). Таким образом, если $A \subseteq B$ и $B \supseteq A$, то $A = B$. Если $A \subseteq B$, $A \neq B$ и $A \neq \varnothing$, то $A$ называется *собственным* подмножеством множества $B$ (обозначение $A \subset B$), иначе оно называется *несобственным* подмножеством множества $B$. Всегда $\varnothing \subseteq A$ и если $A \neq \varnothing$, то $\varnothing \subset A$. Множество $B$ *доминирует* над подмножеством $A$, если $A \subset B$ и нет подмножества $C$ такого, что $A \subset C$ и $C \subset B$.

Множество всех подмножеств множества $A$ называется *булеаном* этого множества и обозначается $2^A$ или $\mathcal{B}(A)$.

***Утверждение 1.1.*** Число подмножеств $n$-множества $A$ равно $2^n$.

***Доказательство.*** (Индукцией по $n$). При $n = 1$ имеются только несобственные подмножества $\varnothing$ и $A = \{a\}$, $|2^A| = 2^1 = 2$. Пусть число подмножеств $(n-1)$-множества равно $2^{n-1}$. Исключим из $n$-множества $A$ один элемент $a$. Полученное $(n-1)$-множество по предположению индукции имеет $2^{n-1}$ подмножеств, являющихся также подмножествами исходного $n$-множества $A$. $2^{n-1}$ остальных его подмножеств получаются

---

[1] Наиболее известные варианты аксиоматики — теория ZF (Цермело — Френкеля) и теория NBG (Ноймана — Бернайса — Гёделя).

[2] Это направление было создано голландским математиком Л.-Э. Я. Брауэром (1881—1966).

[3] Его создателем был советский математик А. А. Марков (1903—1979).

из этих подмножеств добавлением элемента $a$. Таким образом, $n$-множество $A$ имеет $2 \times 2^{n-1} = 2^n$ подмножеств. □

Подмножества $A$ $n$-множества $B$ удобно описывать двоичными наборами $(i_1, \ldots, i_n)$ длиной $n$, элементы $i_j$ которых соответствуют элементам $b_j$ множества $B$ и имеет значение $i_j = 1$, если $b_j \in A$, или значение $i_j = 0$, если $b_j \notin A$. Такой бинарный набор называется *индикатором* подмножества $n$-множества [27]. Например, набор (1, 0, 1, 1) является индикатором подмножества $\{y_1, y_3, y_4\} \subset \{y_1, y_2, y_3, y_4\}$.

**Упражнение 1.1.** Найдите число двоичных наборов длиной $n$.

Булеан $n$-множества наглядно представляется *диаграммой Хассе*[1], на которой его элементы представляются малыми кружками, помеченными индикаторами. Индикаторы собственных подмножеств располагаются ниже индикаторов множеств и соединяются линиями с индикаторами доминирующих над ними множеств. По определению доминирования если множество $A$ доминирует над множеством $B$, то индикаторы этих множеств различаются точно в одной позиции. Такая диаграмма булеана называется также *двоичным n-мерным кубом* и обозначается $\mathcal{B}^n$. Его линии называются также *ребрами*. Двоичные $n$-мерные кубы $\mathcal{B}^n$, $n = 1, 2, 3, 4$, показаны на рис. 1.1. Таким образом, ребра двоичного $n$-мерного куба можно рассматривать как пары вершин

$$((\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n), (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n))$$

и считать их параллельными оси координат $x_i$, при этом число $i$ будем называть *направлением* ребра.

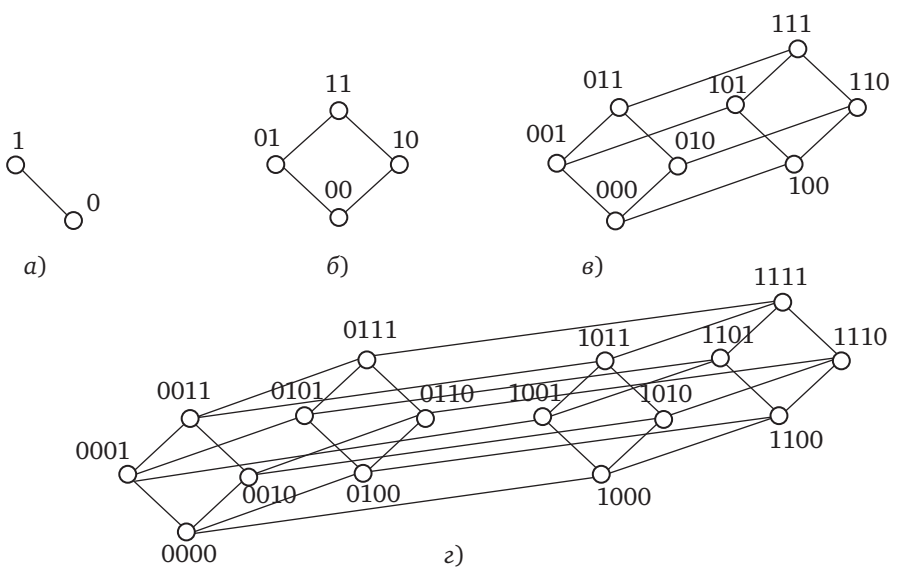


*Рис. 1.1.* **Одномерный (*а*), двумерный (*б*), трехмерный (*в*) и четырехмерный (*г*) кубы**

[1] Хельмут Хассе (Helmut Hasse, 1918—1979) — немецкий математик.

Таким образом, двоичный $n$-мерный куб имеет $2^{n-1}$ ребер в каждом из направлений 1, …, $n$. Ребра одного направления называем *параллельными*.

*Весом* (нормой) вершины $\alpha$ назовем число $\|\alpha\| = \sum_{i=1}^{n} \alpha_i$, равное числу единиц в наборе $\alpha$. Множество всех вершин веса $k$ назовем $k$-м *слоем* двоичного $n$-мерного куба и обозначим $\mathcal{B}_k^n$.

**Определение 1.2.** *Декартовым*[1] *произведением* $A_1 \times A_2 \times \ldots \times A_n$ множеств $A_1, A_2, \ldots, A_n$ называется множество всех возможных наборов из $n$ элементов, по одному из каждого множества:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

При этом если $A_1 = A_2 = \ldots = A_n = A$, декартово произведение называется *декартовой степенью* множества $A$ и обозначается $A^n$.

Примером декартовой степени является $\{0, 1\}^n$ — множество всех двоичных наборов длиной $n$, оно же — множество индикаторов всех подмножеств $n$-множества.

Отображение $\psi : A^n \to A$ декартовой степени $A^n$ в множество $A$ называется *$n$-местной операцией* на множестве $A$.

**Определение 1.3.** *Алгеброй* называется пара $(A, \Omega)$, где $A$ — некоторое множество (*основное множество алгебры*), а $\Omega$ — множество операций на множестве $A$ (*сигнатура алгебры*).

Примером является алгебра множеств $(\mathcal{B}(U), \cap, \cup, \bar{\ })$. Ее основным множеством является булеан $\mathcal{B}(U)$ некоторого множества $U$, а операциями — пересечение $\cap$, объединение $\cup$ и дополнение $\bar{\ }$ множеств. Напомним, что *пересечением* множеств $A$ и $B$ называется множество $A \cap B$, элементы которого принадлежат как множеству $A$, так и множеству $B$. Если множества не имеют общих элементов, то их пересечение есть пустое множество $\varnothing$, такие множества называются *непересекающимися* множествами. *Объединение* множеств — множество $A \cup B$, элементы которого принадлежат множеству $A$ или множеству $B$. *Дополнение* $\overline{A}$ множества $A$ содержит все элементы множества $U$, не являющиеся элементами множества $A$.

Эти три основные операции алгебры множеств используются при описании производных операций.

*Разность множеств* обозначается и определяется как $A \setminus B = A \cap \overline{B}$.

*Симметрическая разность* множеств обозначается и определяется следующим образом (для нее используются и другие обозначения, например $\triangle$ или $\oplus$):

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

Используя операции пересечения и объединения, можно описать отношение вложения множеств: $A \subseteq B$ тогда и только тогда, когда $A \cap B = A$, а также тогда и только тогда, когда $A \cup B = B$.

---

[1] Рене Декарт (Rene Descartes, 1596—1650) — французский математик.

Операции над множествами, как и отношение включения множеств, принято пояснять *диаграммами Венна*[1], на которых множества изображаются геометрическими фигурами, а результаты операций — объединениями фрагментов этих фигур. Пересечение, объединение, разность, симметрическая разность и дополнение множеств показаны диаграммами Венна на рис. 1.2.

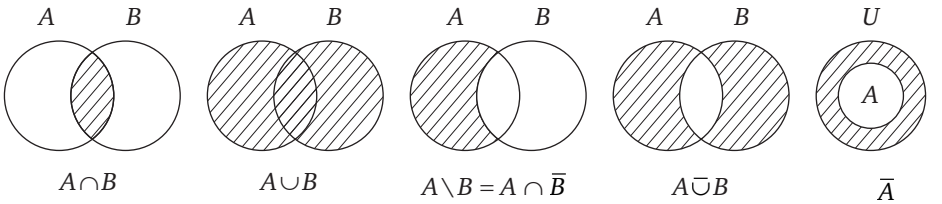


*Рис. 1.2.* **Теоретико-множественные операции и диаграммы Венна**

## 1.2. Отношения

> …Обломовского кучера он любил больше, нежели повара, скотницу Варвару больше их обоих, а Илью Ильича меньше их всех; но все-таки обломовский повар был для него лучше и выше всех поваров в мире, а Илья Ильич выше всех помещиков.
>
> *И. А. Гончаров*. «Обломов»

Взаимосвязь объектов отражается понятием отношения на их множестве. Теория отношений как один из разделов общей алгебры находит применение как в дискретной математике, так и в ее приложениях, в частности в теории баз данных.

Пусть $A_1, A_2, \ldots, A_n$ — произвольные множества.

**Определение 1.4.** *n-Арным* (т. е. *n-местным*) *отношением* $\rho^n$ на множествах $A_1, A_2, \ldots, A_n$ (или на множестве $A$, если $A_1 = A_2 = \ldots = A_n = A$) называется подмножество декартова произведения $A_1 \times A_2 \times \ldots \times A_n$, т. е. $\rho^n \subseteq A_1 \times A_2 \times \times \ldots \times A_n$. Наборы $(a_1, a_2, \ldots, a_n) \in \rho^n$ называются *элементами* отношения, они обозначаются также $\rho^n(a_1, a_2, \ldots, a_n)$.

Отношения, являющиеся конечными множествами, называются *конечными*, являющиеся пустыми множествами — *пустыми*, отношения, совпадающие с декартовой степенью множеств, на которых они рассматриваются, называются *универсальными*. Если эти множества одинаковы, то отношение называется *однородным*, в этом случае оно есть подмножество декартовой степени множества $A$: $\rho^n \subseteq A^n$.

При $n = 1$ отношение на множестве $A$ называется *унарным*, это просто подмножество множества $\rho^1 \subseteq A$.

[1] Джон Венн (John Venn, 1834—1923) — английский математик.

При $n = 2$ отношение на множествах $A$ и $B$ называется *бинарным*, это множество некоторых пар $(a, b)$ элементов из первого и второго множеств, например бинарным является отношение порядка на множестве натуральных чисел $\rho^2 = \{(a, b) : a \le b\} \subseteq \mathbb{N} \times \mathbb{N}$.

*Тернарные* отношения определяются на трех множествах, например $\rho^3 = \{(a, b, c) : a + b = c\} \subseteq \mathbb{N}^3$.

Отношения общего вида применяются, например, для описания и анализа операций в базах данных. В настоящем учебнике мы будем иметь дело в основном с унарными и бинарными отношениями.

### 1.2.1. Соответствия

**Определение 1.5.** Бинарные отношения $\rho \subseteq A_1 \times A_2$ называются также *соответствиями* между множествами $A_1$ и $A_2$.

Индекс 2 в обозначениях бинарных отношений будем опускать и наряду с обозначением $(a, b) \in \rho$ использовать обозначение $a\rho b$.

**Определение 1.6.** Множество $\mathrm{Im}(a) = \{b : (a, b) \in \rho\}$ называется *полным образом элемента* $a \in A_1$ при соответствии $\rho$, а множество $\mathrm{Im}^{-1}(b) = \{a : (a, b) \in \rho\}$ называется *полным прообразом элемента* $b \in A_2$ при соответствии $\rho$.

**Определение 1.7.** *Образом* $\mathrm{Im}(\rho)$ *соответствия* $\rho \subseteq A_1 \times A_2$ называется объединение полных образов всех элементов из $A_1$, а *прообразом* $\mathrm{Im}^{-1}(\rho)$ *соответствия* $\rho \subseteq A_1 \times A_2$ — объединение полных прообразов всех элементов множества $A_2$.

**Пример 1.1.** Соответствие $\rho \subseteq \{a, b, c, d\} \times \{A, B, C, D, E\}$ представлено на рис. 1.3 в виде двудольного графа (см. гл. 6); некоторые вершины $a, b, c, d$ его левой доли соединены дугами с некоторыми вершинами $A, B, C, D, E$ правой доли, чем и задано соответствие. При этом $\mathrm{Im}(a) = \mathrm{Im}(b) = \{B\}$; $\mathrm{Im}(c) = \{A, D\}$; $\mathrm{Im}(d) = \{C, E\}$; $\mathrm{Im}^{-1}(A) = \mathrm{Im}^{-1}(D) = \{c\}$; $\mathrm{Im}^{-1}(B) = \{a, b\}$; $\mathrm{Im}^{-1}(C) = \{a, d\}$; $\mathrm{Im}^{-1}(E) = \{d\}$; $\mathrm{Im}(\rho) = \{A, B, C, D, E\}$, $\mathrm{Im}^{-1}(\rho) = \{a, b, c, d\}$.

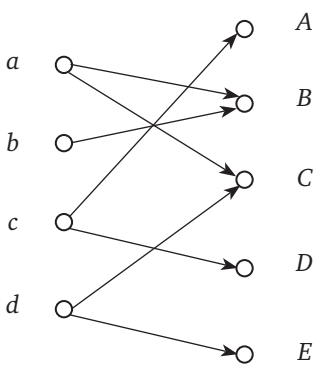


*Рис. 1.3.* **Изображение соответствия в виде графа [3]**

При изучении двудольных графов используются некоторые обобщения рассмотренных понятий. *Полным образом* $\mathrm{Im}(A)$ подмножества $A \subseteq A_1$ при соответствии $\rho$ называется объединение

$$\Gamma(A) = \mathrm{Im}(A) = \bigcup_{a \in A} \mathrm{Im}(a)$$

образов его элементов. При этом $\Gamma(A_1) = \mathrm{Im}(\rho)$. Например, на рис. 1.3 $\Gamma(\{a, d\}) = \{B, C, E\}$.

Аналогично *полным прообразом* подмножества $B \subseteq A_2$ при соответствии $\rho$ называется объединение прообразов его элементов: $\mathrm{Im}^{-1}(B) = \Gamma^{-1}(B)$. При этом $\Gamma^{-1}(A_2) = \mathrm{Im}^{-1}(\rho)$. Например, на рис. 1.3 $\Gamma^{-1}(\{B, C\}) = \{a, b, d\}$.

**Определение 1.8.** Соответствие $\varphi \subseteq X \times Y$, при котором полный образ $\mathrm{Im}(x)$ каждого элемента $x$ содержит единственный элемент, называется *отображением*.

Отображению $\varphi$ соответствует *функция* $\varphi(x)$ с областью определения $X$ и областью значений $\mathrm{Im}(X)$, *значением* функции на некотором элементе области значений является элемент его образа.

Для простоты не будем различать обозначения отображений и соответствующих функций: если $a\varphi y$, $\{y\} = \mathrm{Im}(x)$, то $y = \varphi(x)$.

Если $X = X_1 \times \ldots \times X_i \times \ldots \times X_n$, то функция $\varphi(x)$ называется функцией, зависящей от $n$ переменных, и обозначается $\varphi(x_1, \ldots, x_i, \ldots, x_n)$.

**Определение 1.9.** Отображение $\varphi : X \to Y$ называется *наложением*, или *сюръекцией*, если $\mathrm{Im}(\varphi) = Y$, т. е. каждый элемент $y$ множества $Y$ имеет прообраз. Такие отображения называют также *отображениями на*.

**Определение 1.10.** Отображение $\varphi : X \to Y$ называется *вложением*, или *инъекцией*, если элементы множества $X$ имеют различные полные образы: $x_1 \neq x_2 \Rightarrow \mathrm{Im}(x_1) \neq \mathrm{Im}(x_1)$. Такие отображения называют также *отображениями в*.

**Определение 1.11.** Отображение, являющееся одновременно сюръекцией и инъекцией, называется *биекцией*.

**Определение 1.12.** Соответствие $\psi^{-1} \subseteq Y \times X = \{(b, a) : (a, b) \in \psi \subseteq \subseteq X \times Y\}$ называется *обратным* к соответствию $\psi$.

**Теорема 1.1.** *Соответствие $\psi^{-1} \subseteq Y \times X$, обратное к отображению $\psi \subseteq X \times Y$, является отображением тогда и только тогда, когда отображение $\psi$ является биекцией.*

***Доказательство.*** Пусть соответствие $\psi^{-1}$ является отображением, следовательно, $\mathrm{Im}(\psi) = Y$ и $\psi$ есть сюръекция, при этом для любого $y \in Y$ имеем $|\mathrm{Im}(\mathrm{Im}^{-1}(y))| = 1$ и $\mathrm{Im}^{-1}(Y) = X$, так как $\psi$ есть отображение. Это возможно, только если $\psi$ есть инъекция, т. е. $x_1 \neq x_2 \Rightarrow \mathrm{Im}(x_1) \neq \mathrm{Im}(x_2)$. Таким образом, $\psi$ — сюръекция и инъекция, т. е. $\psi$ является биекцией.

Пусть отображение $\psi$ является биекцией, а обратное соответствие $\psi^{-1}$ отображением не является, т. е. существует такое $y \in Y$, что $|\mathrm{Im}(y)| \neq 1$. Если $|\mathrm{Im}^{-1}(y)| = 0$, то $\psi$ не является даже отображением, а если $|\mathrm{Im}^{-1}(y)| > 1$, то $\psi$ не является инъекцией. □

***Следствие 1.1.*** Отображение $\psi^{-1} \subseteq Y \times X$, обратное к биекции $\psi \subseteq \subseteq X \times Y$, является биекцией.

**Определение 1.13.** Отображение, являющееся биекцией, называется *взаимно однозначным соответствием*. Функция, соответствующая биекции, называется *взаимно однозначной* функцией.

**Определение 1.14.** Функция, соответствующая отображению $\psi^{-1}$, обратному к биекции $\psi$, называется функцией, *обратной* к функции, соответствующей отображению $\psi$.

Функцию, обратную к функции $\psi$, будем обозначать $\psi^{-1}$.

Такие функции, как и отвечающие им отображения, также называют биекциями.

**Пример 1.2.** Если $X = \left[\frac{\pi}{2}; \frac{\pi}{2}\right]$, $Y = [-1; 1]$, то cos$x$ не является ни наложением, ни вложением; sin$x$ — биекция, sin2$x$ — наложение, но не вложение.

**Пример 1.3 [3].** Обратной к функции $\varphi : \{1, 2, 3, 4\} \to \{a, b, c, d\}$ на рис. 1.4, *а* является функция $\varphi^{-1} : \{a, b, c, d\} \to \{1, 2, 3, 4\}$ на рис. 1.4, *б*.

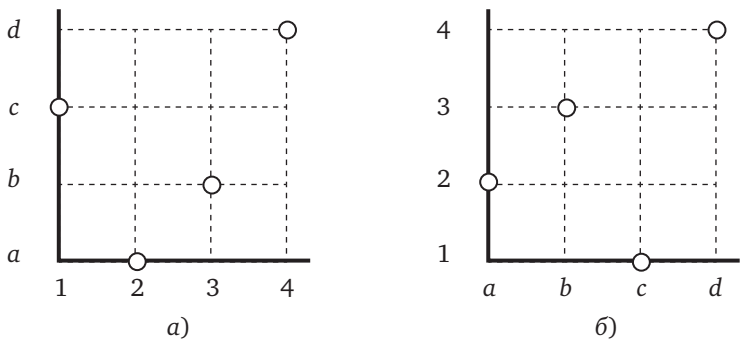


*Рис. 1.4.* **К примеру 1.3**

На множестве функций можно определить операцию *композиции функций*: пусть $f : A \to B$ и $\varphi : C \to D$ — две функции и $A' = \mathrm{Im}^{-1}(B \cap C)$. Определим функцию $\psi : A' \to D$ такую, что $\psi(a) = f(\varphi(a))$ (обозначение $\psi = \varphi * f$). Эта операция есть частный вариант операции *свертки* двух бинарных отношений.

**Пример 1.4.** Пусть $\varphi$ — функция из примера 1.3, $f = \varphi^{-1}$. Тогда $\varphi * f = \varphi * \varphi^{-1}$ есть тождественная функция $\psi : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ такая, что $\psi(x) = x$.

### 1.2.2. Гомоморфизм и изоморфизм

**Гомоморфизм и изоморфизм отношений.** Напомним, что $n$-местное отношение $\rho^n \subseteq A^n$ на множестве $A$ называется однородным.

Пусть $\sigma^n$ — однородное $n$-местное отношение $\sigma^n \subseteq B^n$ на множестве $B$.

**Определение 1.15.** Отображение $\psi \subseteq A \times B$ множества $A$ *на* или *в* множество $B$, сохраняющее отношение, т. е. такое, что

$$(a_1, \ldots, a_n) \in \rho^n \Rightarrow (\psi(a_1), \ldots, \psi(a_n)) \in \sigma^n,$$

называется *гомоморфизмом отношений*, а отношение $\sigma^n$ — *гомоморфным образом* отношения $\rho^n$. Если это отображение является биекцией, то оно называется *изоморфизмом отношений*, а отношение $\sigma^n$ — *изоморфным образом* отношения $\rho^n$. При этом отношения $\sigma^n$ и $\rho^n$ называются *изоморфными* отношениями.

**Пример 1.5.** Пусть $A$ есть множество $\{1, 2, 3, 7, 6, 14, 21, 42\}$ всех делителей числа 42 и $a\rho b$, если $a \mid b$ ($a$ делит $b$). Множество $B$ есть множество индикаторов булеана $2^{\{2,3,7\}}$ и $(i_1, i_2, i_3)\sigma(i'_1, i'_2, i'_3)$, если $i_1 \le i'_1, i_2 \le i'_2, i_3 \le i'_3$.

Тогда отображение $\psi$:

| $A$ | 1 | 2 | 3 | 7 | 6 | 14 | 21 | 42 |
|---|---|---|---|---|---|---|---|---|
| $B$ | (0, 0, 0) | (0, 0, 0) | (0, 1, 0) | (0, 0, 1) | (0, 1, 0) | (0, 0, 1) | (0, 1, 1) | (0, 1, 1) |

есть гомоморфизм отношений $\rho$ и $\sigma$, не являющийся изоморфизмом, а биекция $\psi'$:

| $A$ | 1 | 2 | 3 | 7 | 6 | 14 | 21 | 42 |
|---|---|---|---|---|---|---|---|---|
| $B$ | (0, 0, 0) | (1, 0, 0) | (0, 1, 0) | (0, 0, 1) | (1, 1, 0) | (1, 0, 1) | (0, 1, 1) | (1, 1, 1) |

является изоморфизмом этих отношений, а сами отношения изоморфны.

**Алгебраические гомоморфизм и изоморфизм.** Аналогичные понятия гомоморфизма и изоморфизма определяются и для алгебр.

Напомним, что алгебра $(A, \Omega)$ задается основным множеством $A$ и сигнатурой $\Omega$ с операциями различной местности.

Пусть $(B, \Omega')$ — другая алгебра с основным множеством $B$, сигнатура $\Omega'$ которой состоит из такого же количества операций, что и сигнатура $\Omega$, причем местности соответствующих одна другой операций одинаковы.

**Определение 1.16.** Отображение $\psi \subseteq A \times B$ множества $A$ *на* или *в* множество $B$, сохраняющее операции, т. е. такое, что для любой пары соответствующих одна другой операций $\varphi$ и $\varphi'$

$$\varphi(a_1, \ldots, a_n) = a \Rightarrow \varphi'(\psi(a_1), \ldots, \psi(a_n)) = \psi(a),$$

называется *алгебраическим гомоморфизмом*, а алгебра $(B, \Omega')$ — *гомоморфным образом* алгебры $(A, \Omega)$.

**Определение 1.17.** Биекция $\psi \subseteq A \times B$ множества $A$ *на* множество $B$, сохраняющая операции, т. е. такая, что для любой пары соответствующих одна другой операций $\varphi$ и $\varphi'$

$$\varphi(a_1, \ldots, a_n) = a \Rightarrow \varphi'(\psi(a_1), \ldots, \psi(a_n) = \psi(a),$$

называется *алгебраическим изоморфизмом*, а алгебра $(B, \Omega')$ — *изоморфным образом* алгебры $(A, \Omega)$.

**Пример 1.6.** Пусть $A$ есть множество целочисленных степеней двойки $A = \{a : a = 2^n, n \in \mathbb{N}\}$ с операцией умножения, а множество $B = \mathbb{N}$ с операцией сложения. Тогда отображение $\psi : A \to B$ такое, что $\psi(a) = \log_2 a$, есть изоморфизм. При этом отображение $\psi^{-1} : B \to A$ таково, что $\psi^{-1}(b) = 2^b$, и оно также является изоморфизмом. Таким образом, алгебры $(A, \{\times\})$ и $(B, \{+\})$ изоморфны.

**Пример 1.7.** Алгебра $(Z_{\mathrm{mod}\ m}, \times_{\mathrm{mod}\ m})$, где $Z_{\mathrm{mod}\ m}$ есть множество остатков от деления целых чисел на положительное число $m$, а $\times_{\mathrm{mod}\ m}$ — операция умножения по модулю $m$ (умножение с последующим взятием остатка от деления на $m$), является гомоморфным образом алгебры $(\mathbb{Z}, \times)$. Отображение $\psi : \mathbb{Z} \to \to Z_{\mathrm{mod}\ m}$ такое, что $\psi(a) = a \bmod m$, где $a \bmod m$ есть остаток от деления числа $a$ на число $m$, является алгебраическим гомоморфизмом.

### 1.2.3. Однородные бинарные отношения

Рассмотрим некоторые свойства однородных бинарных отношений, по которым они классифицируются.

Отношение $\rho$ называется *транзитивным*, если оно имеет свойство *транзитивности* (Т): для любых $a, b, c$ справедливо утверждение «если выполняются одновременно $a\rho b$ и $b\rho c$, то выполняется и $a\rho c$».

*Рефлексивное* отношение характеризуется свойством *рефлексивности* (Р): для любого $a$ справедливо $a\rho a$, а *симметричное* отношение — свойством *симметричности* (С): для любых $a, b$ справедливо утверждение «если выполняются $a\rho b$, то выполняется и $b\rho a$».

Определяющие свойства *антитранзитивных*, *антирефлексивных* и *антисимметричных* отношений выражаются следующим образом: *антитранзитивность* (АТ) — для любых $a, b, c$ справедливо утверждение «если выполняются одновременно $a\rho b$ и $b\rho c$, то выполняется и $a\overline{\rho}c$ (т. е. не выполняется $a\rho c$)»; *антирефлексивность* (АР) — для любого $a$ справедливо $a\overline{\rho}a$; *антисимметричность* (АС) — для любых $a, b$ справедливо утверждение «если выполняются одновременно $a\rho b$ и $b\rho c$, то выполняется $a = b$».

Для упрощения изложения будем использовать указанные выше аббревиатуры наименований свойств однородных бинарных отношений. Однородное бинарное отношение $\rho \subseteq A^2$ на конечном множестве из $n$ элементов удобно задавать бинарной матрицей размером $n \times n$:

$$\rho = (\rho_{i,j}),\ i, j = 1, 2, \ldots, n,\ \rho_{i,j} = \begin{cases} 1, \text{если } a_i \rho a_j, \\ 0, \text{в противном случае.} \end{cases}$$

Такая матрица называется матрицей *инцидентности* однородного бинарного отношения.

В частности, отношение равенства на $n$-множестве $A$ представляется единичной матрицей $\delta_A = (\delta_{i,j})$ размером $n \times n$, где

$$\delta_{i,j} = \begin{cases} 1, \text{если } i = j, \\ 0, \text{в противном случае.} \end{cases}$$

**Пример 1.8.** Отношения, обладающие свойствами Т, АС, АР; Т, Р, АС; С, АР; АТ, АР, АС; Т, Р, С, имеют следующие матричные представления:

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

Последнее из этих отношений — пример *универсального* отношения.

Кроме матричного представления однородных бинарных отношений используют наглядные графические представления в виде *ориентированных псевдографов* — геометрических фигур на плоскости, состоящих из кружков, обозначающих элементы множества, и соединяющих их линий со стрелками, обозначающих элементы отношения.

**Определение 1.18.** Однородные бинарные отношения, являющиеся отображениями, называются *преобразованиями*.

## Задачи

**1.1.** Сформулируйте правило, как, используя рисунок куба $\mathcal{B}^n$, получить рисунок куба $\mathcal{B}^{n+1}$, сохраняя следующие особенности рисунков:

а) вершины изображаются различными точками на плоскости;

б) ребра изображаются отрезками прямых, соединяющих их вершины;

в) параллельные ребра изображаются равными и параллельными отрезками (а непараллельные, т. е. скрещивающиеся, ребра — непараллельными отрезками);

г) вершины из одного слоя изображаются точками, лежащими на одной прямой; вершины в слое $\mathcal{B}^n_{n/2+1}$ (при четном $n$) и в слоях $\mathcal{B}^n_{(n+1)/2}$, $\mathcal{B}^n_{(n+1)/2+1}$ (при нечетном $n$) располагаются на равных расстояниях;

д) вершины меньшего веса располагаются ниже вершин большего веса;

е) прямые, на которых лежат слои, параллельны друг другу.

**1.2.** Определите число элементов декартова произведения $A_1 \times A_2 \times \ldots \times A_i \times \ldots \times A_n$, $|A_i| = n_i$, $i = 1, \ldots, n$.

**1.3.** Выразите свойства однородных бинарных отношений на множестве $A$ с использованием операций над отношениями и отношения теоретико-множественного включения.

*Указание*. Транзитивность: $\rho * \rho \subseteq \rho$; рефлексивность: $\delta_A \subseteq \rho$; симметричность: $\rho^{-1} = \rho$; антитранзитивность: $\rho * \rho \subseteq \overline{\rho}$; антирефлексивность: $\delta_A \cap \rho = \varnothing$; антисимметричность: $\rho \cap \rho^{-1} \subseteq \delta_A$.

**1.4.** Покажите, как описать операции алгебры конечных множеств с использованием индикаторов подмножеств и как представляются результаты этих операций над подмножествами $n$-множества в двоичном $n$-мерном кубе.

**1.5.** В $n$-множестве выбрано $2^{n-1}$ подмножеств, из которых любые три пересекаются. Докажите, что все они пересекаются.

*Указание.* Индикаторы всех $2^n$ подмножеств $n$-множества разбейте на $2^{n-1}$ пар взаимно дополнительных. Тогда наше семейство не содержит двух наборов ни из одной пары (почему?). Далее заметьте, что пересечение любых двух множеств принадлежит семейству (иначе ему принадлежало бы его дополнение, не пересекающееся одновременно с обоими этими множествами, что по условию задачи невозможно). Наконец, обратите внимание, что если пересечение любых двух множеств принадлежит семейству, то и пересечение всех множеств тоже, и оно не пусто, иначе оно не пересекалось бы ни с одним из других множеств.

# Глава 2
# ФУНКЦИИ АЛГЕБРЫ ЛОГИКИ

В результате освоения главы 2 студент должен:

***знать***

- основы теории функций алгебры логики;

***уметь***

- применять язык формул алгебры логики;
- выполнять эквивалентные преобразования формул;
- доказывать полноту систем функций алгебры логики;

***владеть***

- простейшими методами минимизации формул алгебры логики.

## 2.1. Основные определения

Джордж Буль установил истинную связь алгебры и логики.

*А. де Морган*

**Определение 2.1.** *Функцией алгебры логики, зависящей от n переменных*, (а также *булевой функцией*[1]) называется функция $f(x_1, \ldots, x_n)$, переменные которой, как и сама функция, могут принимать значения из множества $\{0, 1\}$.

Множество всех функций алгебры логики, зависящих от $n$ переменных, обозначается $P_2(n)$, а их число $|P_2(n)|$ — $p_2(n)$. Функция алгебры логики является отображением $f : \{0, 1\}^n \to \{0, 1\}$ множества наборов $(a_1, \ldots, a_n)$ значений $a_i$, $i = 1, \ldots, n$, ее переменных $x_1, \ldots, x_n$ в множество $\{0, 1\}$. Это отображение представляется таблицей, в левом столбце которой размещаются бинарные наборы значений переменных, упорядоченные по возрастанию числовых эквивалентов, а в правом — соответствующие им значения функции. Разные такие отображения являются разными функциями и каждая функция не может быть представлена разными отображениями. При одном и том же порядке переменных таблицы, представляющие разные функции, различаются столбцами их значений, т. е. при определенном порядке переменных соответствие функций и отображений является биекцией.

[1] Джордж Буль (George Boole, 1815—1864) — английский математик и логик.

***Утверждение 2.1.*** Число двоичных наборов длины $n$ равно $2^n$.

***Доказательство.*** Доказательство данного утверждения предлагалось выше в учебнике в качестве упражнения 1.1. □

***Утверждение 2.2.*** Число $p_2(n)$ функций алгебры логики, зависящих от $n$ переменных, равно $2^{2^n}$.

***Доказательство.*** Число $p_2(n)$ — это одновременно и число таблиц отображений. Эти таблицы различаются столбцами значений функций. Высота этих столбцов равна $2^n$ — числу различных бинарных наборов длины $n$. Число различных возможных столбцов равно $2^{2^n}$. □

Это число с ростом $n$ быстро растет, так как с увеличением $n$ на единицу очередное число возводится в квадрат: $p_2(n + 1) = (p_2(n))^2$.

Таким образом, булеву функцию, зависящую от $n$ переменных, можно однозначно представить бинарным вектором длины $2^n$ ее значений на перечисляемых в указанном выше порядке бинарных наборах значений ее переменных (это перечисление принимается по умолчанию). Эквивалентными способами задания функции алгебры логики является задание ее перечислением десятичных эквивалентов двоичных наборов значений переменных, на которых функция принимает значение 1 или 0 (перечислением прообразов единичных или нулевых значений).

Булевы функции, зависящие от одной переменной, вместе с их обозначениями и названиями представлены в табл. 2.1.

*Таблица 2.1*

**Булевы функции, зависящие от одной переменной**

| $x$ | **Константа 0** | **Константа 1** | **Тождественная функция** | **Отрицание** |
|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 |
| Обозначение: | 0 | 1 | $x$ | $\overline{x}$ |

Отрицание обозначают также $\neg x$. В табл. 2.2 представлены пять функций, зависящих от двух переменных и их обозначения, а в табл. 2.3 — еще пять функций, являющихся отрицаниями функций из табл. 2.2.

*Таблица 2.2*

**Булевы функции, зависящие от двух переменных**

| $x_1$ | $x_2$ | **Конъюнкция** | **Дизъюнкция** | **Сумма по модулю два** | **Импликация** | **Обратная импликация** |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| Обозначение: | | $x_1 \wedge x_2$ | $x_1 \vee x_2$ | $x_1 \oplus x_2$ | $x_1 \rightarrow x_2$ | $x_1 \leftarrow x_2$ |

*Таблица 2.3*

**Отрицания булевых функций, зависящих от двух переменных**

| $x_1$ | $x_2$ | **Штрих Шеффера** | **Стрелка Пирса** | **Равнозначность** | **Отрицание импликации** | **Отрицание обратной импликации** |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| Обозначение: | | $x_1 \mid x_2$ | $x_1 \downarrow x_2$ | $x_1 \equiv x_2$ | $\overline{x_1 \to x_2}$ | $\overline{x_1 \leftarrow x_2}$ |

Для обозначения конъюнкции используют также знак & или, по аналогии с операцией умножения, обозначение вообще опускают: $x_1 \wedge x_2 = x_1 \,\&\, x_2 = x_1 x_2$. Далее в книге могут использоваться различные способы обозначения конъюнкции. Для сокращения записей формул с логическими операциями принимают соглашение об опускании скобок, полагая, что по силе связывания логические операции располагаются в таком порядке: $\neg, \downarrow, \mid, \wedge, \vee, \to$.

Функции табл. 2.3 могут быть выражены через функции табл. 2.2. Например, штрих Шеффера[1] $x_1 \mid x_2 = \overline{x_1 \wedge x_2} = \bar{x}_1 \vee \bar{x}_2$, а стрелка Пирса[2] $x_1 \downarrow x_2 = \overline{x_1 \vee x_2} = \bar{x}_1 \wedge \bar{x}_2$.

В некоторых случаях одно и то же отображение может представлять функции, различающиеся порядком следования переменных, например $f(x_1, x_2) = x_1 \vee x_2$ и $\varphi(x_1, x_2) = f(x_2, x_1) = x_2 \vee x_1$, но существуют функции, при разном порядке следования переменных являющиеся различными отображениями, например $f(x_1, x_2) = x_1 \to x_2$ и $\psi(x_1, x_2) = f(x_2, x_1) = x_2 \to x_1$.

Функции, являющиеся одинаковыми отображениями при любом порядке следования переменных, называются *симметричными*.

Такие функции при любой перестановке (т. е. однородной биекции) $\pi$ на множестве номеров переменных сохраняются:

$$f(x_{\pi(1)}, \ldots, x_{\pi(i)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_i, \ldots, x_n).$$

Переменная $x_i$ булевой функции $f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)$ называется *существенной*, если при некотором наборе $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ значений остальных переменных

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

Переменная, не являющаяся существенной, называется *фиктивной*.

---

[1] Генри Морис Шеффер (Henry Maurice Sheffer, 1882—1964) — американский логик.

[2] Чарльз Сандерс Пирс (Charles Sanders Peirce, 1839—1914) — американский философ и логик. О нем можно прочитать в книге: *Кирющенко В. В.* Чарльз Сандерс Пирс, или Оса в бутылке. Введение в интеллектуальную историю Америки. М. : Территория будущего, 2008.

**Пример 2.1.** Рассмотрим табличное представление функции $f(x_1, x_2, x_3)$:

| $x_1$ | $x_2$ | $x_3$ | $f(x_1, x_2, x_3)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |

В данном случае переменная $x_2$ — фиктивная, а переменные $x_1$ и $x_3$ — существенные.

Таблицу булевой функции можно упростить, исключив фиктивные переменные. Для этого достаточно вычеркнуть столбец значений этой переменной и удалить по одной строке из образовавшихся при этом пар одинаковых строк:

| $x_1$ | $x_2$ | $x_3$ | $f(x_1, x_2, x_3)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |

$\Leftrightarrow$

| $x_1$ | $x_3$ | $f(x_1, x_2, x_3)$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

$\Leftrightarrow$

| $x_1$ | $x_3$ | $f(x_1, x_2, x_3)$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Обратному преобразованию соответствует введение фиктивной переменной.

**Определение 2.2.** Две булевы функции называются *равными*, если они одинаковы или если одна из них может быть получена из другой посредством описанных преобразований удаления или введения фиктивных переменных.

Табличные представления булевых функций при большом числе переменных громоздки. Поэтому, как правило, используются представления функций формулами над некоторой системой функций.

Пусть задана некоторая система $\mathcal{A}$ функций алгебры логики[1].

$$\mathcal{A} = \{f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)\}. \qquad (2.1)$$

Дадим индуктивное определение формулы над системой $\mathcal{A}$.

[1] С учетом возможности введения и исключения фиктивных переменных можно считать, что все функции являются функциями, зависящими от $n$ переменных $x_1, \ldots, x_n$.

**Определение 2.3.** 1. Отдельная запись $f_i(x_1, \ldots, x_n)$ является *формулой* над системой функций (2.1). 2. Запись вида $f_i(A_1, \ldots, A_j, \ldots, A_n)$, где $A_j$, $j = 1, \ldots, n$, — формулы над системой (2.1) или переменные, есть *формула* над этой системой.

При этом если $A_j$ является формулой над системой (2.1), то $A_j$ называется *подформулой* формулы $f_i(A_1, \ldots, A_j, \ldots, A_n)$, в которую она входит. Таким образом, формула имеет иерархическую структуру вложенных одна в другую подформул. Наибольшая длина цепочки вложенных формул называется *глубиной* формулы.

Формула определяет (вычисляет, реализует) булеву функцию: по ней вычисляются значения функции на любом наборе $(a_1, \ldots, a_n)$ значений переменных. При этом в порядке неубывания глубины подформул вычисляются их значения как значения переменных (если $A_j$ — переменная) или как значения $f_i(\dot{A}_1, \ldots, \dot{A}_n)$ функций $f_i$ на вычисленных к этому моменту наборах значений $(\dot{A}_1, \ldots, \dot{A}_n)$.

Такие вычисления значений функции, заданной формулой, соответствуют следующему индуктивному определению функции, реализуемой формулой над системой функций.

**Определение 2.4.** 1. Формула вида $f_i(x_1, \ldots, x_n)$ *реализует функцию* $f_i(x_1, \ldots, x_n)$. 2. Формула вида $f_i(A_1, \ldots, A_j, \ldots, A_n)$, где $A_j$ — формулы или переменные $x_{i_j}$, *реализует функции* $f_i(f_{i_1}, \ldots, f_{i_j}, \ldots, f_{i_n})$, где $f_{i_j}$ — функции, реализуемые формулами $A_j$, или тождественные функции $f_{i_j}(x_{i_j}) = x_{i_j}$.

Функция, реализуемая формулой над системой функций (2.1), называется *суперпозицией* функций этой системы. В частности, формулы $f(x_{\pi(1)}, \ldots, x_{\pi(n)})$, $f(x, \ldots, x)$, где $\pi$ есть перестановка на множестве номеров переменных, а $f(x, \ldots, x)$ получена подстановкой тождественной функции $x$ вместо каждой переменной функции $f(x_1, \ldots, x_i, \ldots, x_n)$, реализуют суперпозиции функций любой системы, содержащей эту функцию.

Таким образом, функциями системы (2.1) могут порождаться другие функции в результате подстановки в них функций этой системы или переменных, в частности просто перестановкой или заменой переменных.

Множество всех функций, которые можно получить таким образом из функций некоторой системы $M$, т. е. множество всех суперпозиций этой системы, называется ее *замыканием* и обозначается $[M]$.

Одну и ту же функцию можно реализовать разными формулами над той или иной системой функций. Две формулы называются *эквивалентными*, если они реализуют равные булевы функции. Эквивалентность формул обозначают знаком равенства. Эквивалентные формулы, соединенные знаком равенства, называют также *тождеством*. Простейшие (базисные) тождества собраны в табл. 2.4.

Из индуктивного определения формулы над системой функций алгебры логики вытекает следующее утверждение.

***Утверждение 2.3.*** Справедливы следующие правила эквивалентных преобразований формул: (Э1) замена в двух эквивалентных формулах всех вхождений некоторой переменной одной и той же подформулой приводит к эквивалентным формулам; (Э2) при замене любой подформулы эквивалентной ей подформулой получается формула, эквивалентная исходной формуле.

*Таблица 2.4*

**Простейшие тождества**

| Обозначение | Формулы | Название |
|---|---|---|
| АЛ1 | $x \wedge x = x;\ x \vee x = x$ | Идемпотентность |
| АЛ2 | $x_1 \wedge x_2 = x_2 \wedge x_1;\ x_1 \vee x_2 = x_2 \vee x_1$ | Коммутативность |
| АЛ3 | $x_1 \wedge (x_2 \wedge x_3) = (x_1 \wedge x_2) \wedge x_3;$<br>$x_1 \vee (x_2 \vee x_3) = (x_1 \vee x_2) \vee x_3$ | Ассоциативность |
| АЛ4 | $x_1 \wedge (x_1 \vee x_2) = x_1;$<br>$x_1 \vee (x_1 \wedge x_2) = x_1$ | Тождества поглощения |
| АЛ5 | $x_1 \wedge (x_2 \vee (x_1 \wedge x_3)) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3);$<br>$x_1 \vee (x_2 \wedge (x_1 \vee x_3)) = (x_1 \vee x_2) \wedge (x_1 \vee x_2)$ | Модулярность |
| АЛ6 | $x_1 \wedge (x_2 \vee x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3);$<br>$x_1 \vee (x_2 \wedge x_3) = (x_1 \vee x_2) \wedge (x_1 \vee x_3)$ | Дистрибутивность |
| АЛ7 | $x_1 \wedge\ 1 = x_1;\ x_1 \vee 0 = x_1;\ x_1 \wedge 0 = 0;\ x_1 \vee 1 = 1$ | Свойства констант |
| АЛ8 | $x_1 \wedge \bar{x}_1 = 0; x_1 \vee \bar{x}_1 = 1$ | Свойства отрицания |
| АЛ9 | $\bar{\bar{x}} = x$ | Снятие двойного отрицания |
| АЛ10 | $\overline{x_1 \wedge x_2} = \bar{x}_1 \vee \bar{x}_2;\ \overline{x_1 \vee x_2} = \bar{x}_1 \wedge \bar{x}_2$ | Тождества Де Моргана[1] |

Согласно правилам Э1 и Э2 из тождеств АЛ1—АЛ10 можно вывести более общие тождества, заменив переменные $x_1$, $x_2$, $x_3$ произвольными формулами $\Phi_1$, $\Phi_2$ и $\Phi_3$, например $\Phi_1 \vee (\Phi_1 \wedge \Phi_2) = \Phi_1$.

Булева функция $f^*(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n)$ называется *двойственной* к функции $f(x_1, \ldots, x_n)$. Справедливо свойство взаимной двойственности: $(f^*)^* = f$.

Например, $x_1 \wedge x_2 = \overline{\bar{x}_1 \vee \bar{x}_2}$, т. е. функция $x_1 \wedge x_2$ двойственна к функции $x_1 \vee x_2$, функция $x_1 \vee x_2$ двойственна к функции $x_1 \wedge x_2$, взаимно двойственны константы 0 и 1.

Если $f(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n)$, то функция $f(x_1, \ldots, x_n)$ называется *самодвойственной*.

Например, самодвойственны функции $\bar{x}$, $x_1x_2 \vee x_1x_3 \vee x_2x_3$.

[1] Август де Морган (Augustus de Morgan, 1806—1871) — шотландский математик.

**Упражнение 2.1.** Как распознать свойство самодвойственности по таблице булевой функции? Перечислите самодвойственные функции, зависящие от двух переменных.

*Указание*. Самодвойственные функции имеют противоположные значения на противоположных наборах значений переменных. Из 16 элементарных (т. е. зависящих от одной или от двух переменных) функций самодвойственными являются две тождественные функции и их отрицания.

***Утверждение 2.4.*** Если

$$f(x_1, \ldots, x_n) = \varphi(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

то

$$f^*(x_1, \ldots, x_n) = \varphi^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)).$$

***Доказательство.*** Используя определение двойственной функции и свойство АЛ9, получаем

$$f^*(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n) = \overline{\varphi}(f_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, f_m(\overline{x}_1, \ldots, \overline{x}_n)) =$$
$$= \overline{\varphi}(\overline{f}_1(\overline{x}_1, \ldots, \overline{x}_n), \ldots, \overline{f}_m(\overline{x}_1, \ldots, \overline{x}_n)) = \overline{\varphi}(\overline{f}_1^*(x_1, \ldots, x_n), \ldots, \overline{f}_m^*(x_1, \ldots, x_n)) =$$
$$= \varphi^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)). \qquad \square$$

С помощью этого утверждения индукцией по глубине формулы легко доказывается следующее утверждение

***Утверждение 2.5*** (принцип двойственности). Если в некоторой формуле Ф заменить все обозначения функций обозначениями двойственных функций, то получится формула $\Phi^*$, представляющая двойственную функцию (т. е. суперпозиция двойственных функций двойственна суперпозиции функций).

Сформулируем следствия принципа двойственности.

***Следствие 2.1.*** Если в двух эквивалентных формулах заменить все функции на двойственные, то получатся две эквивалентные формулы.

***Следствие 2.2.*** Для любой булевой функции справедливо тождество

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

## 2.2. Разложение булевых функций по переменным

> Если остановить любого из этих прохожих, то вряд ли даже один из пятидесяти сможет внятно объяснить, что такое электричество, не говоря уже о каком-нибудь булевом логическом выражении.
>
> *Т. Фишер.*
> «Идиотам просьба не беспокоиться»

Булевы функции $f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n)$, получающиеся при подстановке констант $\sigma_1, \ldots, \sigma_k$ вместо переменных $x_1, \ldots, x_k$ функции $f(x_1, \ldots, x_n)$, называются $(\sigma_1, \ldots, \sigma_k)$-*компонентой* этой функции. Число $k$ называется *рангом* этой компоненты функции.

Замещаться константами могут любые переменные функции, не только первые по порядку их следования. Например, функция $f(x_1, x_2, 0) = x_1x_2$ есть $(\sigma_3)$-компонента при $\sigma_3 = 0$ функции $f(x_1, x_2, x_3) = x_1x_2 \vee \vee x_1x_3 \vee x_2x_3$.

Для сравнения всех $(\sigma_1, \ldots, \sigma_k)$-компонент функции удобно использовать прямоугольные таблицы, в которых столбцы соответствуют наборам значений переменных $x_1, \ldots, x_k$, а строки — наборам значений остальных переменных функции $f(x_1, \ldots, x_k, \ldots, x_n)$. Тогда столбцы представляют все возможные такие компоненты.

**Пример 2.2.** Функция $f(x_1, x_2, x_3, x_4)$ представлена таблицей

| | | $(x_1, x_2)$ | | | |
|---|---|---|---|---|---|
| | $f(x_1, x_2, x_3, x_4)$ | 00 | 01 | 10 | 11 |
| $(x_3, x_4)$ | 00 | 1 | 0 | 0 | 1 |
| | 01 | 0 | 1 | 0 | 0 |
| | 10 | 0 | 0 | 1 | 1 |
| | 11 | 0 | 1 | 1 | 1 |

Столбцы представляют $(\sigma_1, \sigma_2)$-компоненты, например $f(0, 1, x_3, x_4) = x_4$, а строки являются $(\sigma_3, \sigma_4)$-компонентами, например $f(x_1, x_2, 1, 1) = x_1 \vee x_2$. Для представления строками или столбцами других $(\sigma_i, \sigma_j)$-компонент таблицу следует перестроить перестановкой некоторых подтаблиц. Например, перестановкой нижней левой и верхней правой квадратных частей таблицы, содержащих по четыре элемента, столбцы становятся $(\sigma_3, \sigma_2)$-компонентами, а строки — $(\sigma_1, \sigma_4)$-компонентами:

| | | $(x_3, x_2)$ | | | |
|---|---|---|---|---|---|
| | $f(x_1, x_2, x_3, x_4)$ | 00 | 01 | 10 | 11 |
| $(x_1, x_4)$ | 00 | 1 | 0 | 0 | 0 |
| | 01 | 0 | 1 | 0 | 1 |
| | 10 | 0 | 1 | 1 | 1 |
| | 11 | 0 | 0 | 1 | 1 |

**Упражнение 2.2.** Какие части таблицы следует переставить, чтобы в строках получить $(x_2, x_4)$-компоненты функции $f(x_1, x_2, x_3, x_4)$?

*Указание.* Таблицу разбейте на две части, в одной — два первых столбца, во второй — третий и четвертый. В этих двух таблицах переставьте две нижние клетки левого столбца и две верхние клетки правого столбца. Например, для функции из последнего примера получится таблица

| | | $(x_1, x_3)$ | | | |
|---|---|---|---|---|---|
| | $f(x_1, x_2, x_3, x_4)$ | 00 | 01 | 10 | 11 |
| $(x_2, x_4)$ | 00 | 1 | 0 | 0 | 1 |
| | 01 | 0 | 0 | 0 | 1 |
| | 10 | 0 | 0 | 1 | 1 |
| | 11 | 1 | 1 | 0 | 1 |

Таблицы можно строить при любом разбиении множеств переменных.

**Пример 2.3.** Функцию $f(x_1, x_2, x_3, x_4)$ из примера 2.2 можно представить таблицей

| | | $(x_1, x_2, x_3)$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | $f(x_1, x_2, x_3, x_4)$ | 000 | 010 | 100 | 110 | 001 | 011 | 101 | 111 |
| $(x_4)$ | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |

Строками представлены $\sigma_4$-компоненты, а столбцами — $(\sigma_1, \sigma_2, \sigma_3)$-компоненты функции $f(x_1, x_2, x_3, x_4)$ из примера 2.2.

Введем понятия элементарной конъюнкции и элементарной дизъюнкции. При этом запись $x^\sigma$, $\sigma \in \{0, 1\}$, будем понимать как обозначение переменной $x$ (при $\sigma = 1$) или ее отрицания $\overline{x}$ (если $\sigma = 0$). Ясно, что $\sigma^\sigma = 1$.

Константу 1 назовем *элементарной конъюнкцией нулевого ранга*, а формулу вида $x_{i_1}^{\sigma_{i_1}} \wedge \ldots \wedge x_{i_k}^{\sigma_{i_k}}$, где все переменные различны, — *элементарной конъюнкцией ранга k*.

Используем сокращенные обозначения $x_{i_1}^{\sigma_{i_1}} \wedge \ldots \wedge x_{i_k}^{\sigma_{i_k}} = x_{i_1}^{\sigma_{i_1}} \cdots x_{i_k}^{\sigma_{i_k}}$, опуская знаки $\wedge$.

Аналогично константа 0 называется *элементарной дизъюнкцией нулевого ранга*, а формула вида $x_{i_1}^{\sigma_{i_1}} \vee \ldots \vee x_{i_k}^{\sigma_{i_k}}$, где все переменные различны, — *элементарной дизъюнкцией ранга k*.

Эти функции обладают следующими очевидными свойствами:

$$a_{i_1}^{\sigma_{i_1}} \cdots a_{i_k}^{\sigma_{i_k}} = \begin{cases} 1, \text{если } a_{i_j} = \sigma_{i_j} \text{ для любых } j, \\ 0, \text{в остальных случаях;} \end{cases}$$

$$a_{i_1}^{\sigma_{i_1}} \vee \ldots \vee a_{i_k}^{\sigma_{i_k}} = \begin{cases} 0, \text{если } a_{i_j} \neq \sigma_{i_j} \text{ для любых } j, \\ 1, \text{в остальных случаях.} \end{cases}$$

Здесь $a_{i_j}$, $j = 1, \ldots, k$, — суть значения переменных элементарной конъюнкции или дизъюнкции.

Понятия $(\sigma_1, \ldots, \sigma_k)$-компонент, элементарных конъюнкций и элементарных дизъюнкций используются в теоремах о конъюнктивном и дизъюнктивном разложении функций алгебры логики.

**Теорема 2.1 (теорема Шеннона[1] о дизъюнктивном разложении).** *Всякая функция алгебры логики $f(x_1, \ldots, x_k, \ldots, x_n)$ представима формулой*

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_k) \in \{0,1\}^k} x_1^{\sigma_1} \cdots x_k^{\sigma_k} f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n).$$

[1] Клод Эльвуд Шеннон (Claude Elwood Shannon, 1916—2001) — американский инженер и математик.

***Доказательство.*** Рассмотрим значение этой формулы на произвольном двоичном наборе значений переменных $(a_1, \ldots, a_n)$. С учетом указанного свойства элементарных конъюнкций все слагаемые этой дизъюнктивной суммы, кроме одного, а именно $a_1^{a_1} \cdots a_k^{a_k} f(a_1, \ldots, a_n)$, заведомо будут равны нулю, а указанный выделенный член равен значению $f(a_1, \ldots, a_n)$. Такое равенство выполняется для всех таких двоичных наборов. □

**Пример 2.4.** Используя данные о компонентах функции $f(x_1, x_2, x_3, x_4)$ из примера 2.2, приведем несколько ее дизъюнктивных разложений:

$$f(x_1, x_2, x_3, x_4) = x_1^0 x_2^0 f(0,0, x_3, x_4) \vee x_1^0 x_2^1 f(0,1, x_3, x_4) \vee x_1^1 x_2^0 f(1,0, x_3, x_4) \vee$$
$$\vee x_1^1 x_2^1 f(1,1, x_3, x_4) = \bar{x}_1 \bar{x}_2 (\overline{x_3 \vee x_4}) \vee \bar{x}_1 x_2 (x_4) \vee x_1 \bar{x}_2 (x_3) \vee x_1 x_2 (x_4 \to x_3) =$$
$$= x_3^0 x_4^0 f(x_1, x_2, 0,0) \vee x_3^0 x_4^1 f(x_1, x_2, 0,1) \vee x_3^1 x_4^0 f(x_1, x_2, 1,0) \vee x_3^1 x_4^1 f(x_1, x_2, 1,1) =$$
$$= \bar{x}_3 \bar{x}_4 (\overline{x_1 \oplus x_2}) \vee \bar{x}_3 x_4 (\overline{x_2 \to x_1}) \vee x_3 \bar{x}_4 (x_1) \vee x_3 x_4 (x_1 \vee x_2).$$

***Следствие 2.3 (о дизъюнктивном разложении по одной переменной).*** Всякая функция алгебры логики $f(x_1, \ldots, x_n)$ реализуется формулой

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

***Следствие 2.4 (о дизъюнктивном разложении по всем переменным).*** Всякая функция алгебры логики $f(x_1, \ldots, x_n)$, не являющаяся константой 0, представима формулой

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n, f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \cdots x_n^{\sigma_n}.$$

Эта формула получается из разложения по теореме 2.1

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n} x_1^{\sigma_1} \cdots x_n^{\sigma_n} f(\sigma_1, \ldots, \sigma_n)$$

удалением слагаемых, для которых $f(\sigma_1, \ldots, \sigma_n) = 0$.

Формула, представляющая функцию по следствию 2.4, называется *совершенной дизъюнктивной нормальной формой* функции (сокращенно СДНФ). Это частный случай *дизъюнктивной нормальной формы* (ДНФ), формулы, представляющей функцию в виде дизъюнкции элементарных конъюнкций.

**Пример 2.5.** Функция $f(x_1, x_2, x_3, x_4)$ из примера 2.2 имеет следующую СДНФ:

$$\bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \vee x_1 x_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_1 x_2 \bar{x}_3 x_4 \vee x_1 \bar{x}_2 x_3 \bar{x}_4 \vee x_1 x_2 x_3 \bar{x}_4 \vee \bar{x}_1 x_2 x_3 x_4 \vee$$
$$\vee x_1 \bar{x}_2 x_3 x_4 \vee x_1 x_2 x_3 x_4.$$

**Теорема 2.2 (теорема Шеннона о конъюнктивном разложении).** *Всякая функция алгебры логики $f(x_1, \ldots, x_k, \ldots, x_n)$ представима формулой*

$$f(x_1, \ldots, x_n) = \bigwedge_{(\sigma_1, \ldots, \sigma_k) \in \{0,1\}^k} (\bar{x}_1^{\sigma_1} \vee \cdots \vee \bar{x}_k^{\sigma_k} \vee f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n)).$$

***Доказательство.*** Построим по теореме 2.1 дизъюнктивное разложение отрицания данной функции $f(x_1, \ldots, x_n)$:

$$\overline{f}(x_1,\ldots,x_n)=\bigvee_{(\sigma_1,\ldots,\sigma_k)\in\{0,1\}^k} x_1^{\sigma_1}\cdots x_k^{\sigma_k}\overline{f}(\sigma_1,\ldots,\sigma_k,x_{k+1},\ldots,x_n).$$

По следствию 2.2, заменив все входящие в эту формулу функции двойственными функциями, а переменные — их отрицаниями, получим формулу, представляющую функцию $f(x_1, \ldots, x_n)$:

$$f(x_1,\ldots,x_n)=\bigwedge_{(\sigma_1,\ldots,\sigma_k)\in\{0,1\}^k}(\overline{x}_1^{\sigma_1}\vee\cdots\overline{x}_k^{\sigma_k}\vee\overline{f}^*(\sigma_1^*,\ldots,\sigma_k^*,\overline{x}_{k+1},\ldots,\overline{x}_n)).$$

Преобразуем подформулы $\overline{f}^*(\sigma_1^*,\ldots,\sigma_k^*,\overline{x}_{k+1},\ldots,\overline{x}_n)$ по определению двойственной функции, учитывая,что $\sigma^*=\overline{\sigma}$:

$$\overline{\overline{f}}(\overline{\sigma}_1,\ldots,\overline{\sigma}_k,\overline{\overline{x}}_{k+1},\ldots,\overline{\overline{x}}_n)=f(\sigma_1,\ldots,\sigma_k,x_{k+1},\ldots,x_n). \qquad \square$$

***Следствие 2.5 (о конъюнктивном разложении по одной переменной).*** Всякая функция алгебры логики $f$ представима формулой

$$f(x_1,\ldots,x_n)=(\overline{x}_k\vee f(x_1,\ldots,x_{k-1},1,x_{k+1},\ldots,x_n))\wedge$$
$$\wedge(x_k\vee f(x_1,\ldots,x_{k-1},0,x_{k+1},\ldots,x_n)).$$

Такие разложения можно строить непосредственно по этой формуле, используя, например, соответствующие табличные представления функции, или путем преобразования дизъюнктивных разложений отрицания функции заменой в них переменных отрицаниями переменных, функций $\wedge$ — функциями $\vee$, а функций $\vee$ — функциями $\wedge$.

***Следствие 2.6 (о конъюнктивном разложении по всем переменным).*** Всякая функция алгебры логики $f(x_1, \ldots, x_k, \ldots, x_n)$, не равная константе 1, представима формулой

$$f(x_1,\ldots,x_k,\ldots,x_n)=\bigwedge_{(\sigma_1,\ldots,\sigma_n)\in\{0,1\}^n,\,f(\sigma_1,\ldots,\sigma_n)=0}(\overline{x}_1^{\sigma_1}\vee\ldots\vee\overline{x}_k^{\sigma_n}).$$

Представление булевой функции, получаемое по этому следствию, называется *совершенной конъюнктивной нормальной формой* функции (сокращенно СКНФ). Она является частным случаем *конъюнктивной нормальной формы* (КНФ) — представления функции в виде конъюнкции элементарных дизъюнкций.

Элементарная конъюнкция, не содержащая отрицаний переменных, называется *монотонной* конъюнкцией. В частности, монотонной конъюнкцией является константа 1.

**Определение 2.5.** *Полиномом Жегалкина*[1] называется формула, являющаяся монотонной конъюнкцией или суммой по модулю два различных монотонных конъюнкций, или константой 0.

**Теорема 2.3.** *Всякая функция алгебры логики представима полиномом Жегалкина, причем единственным образом.*

[1] Иван Иванович Жегалкин (1869—1947) — профессор Московского университета.

***Доказательство.*** Полином Жегалкина функции, являющейся константой, есть эта константа. Булева функция $f(x_1, \ldots, x_n)$, не равная константе 0, имеет СДНФ. По свойству элементарных конъюнкций на любом наборе значений переменных $(a_1, \ldots, a_n)$ не более чем одна элементарная конъюнкция в этой СДНФ имеет значение 1. Учитывая свойства $x \vee 0 = x$ и $x \oplus 0 = x$ функции сложения по модулю два, все функции $\vee$ (если они имеются) в СДНФ можно заменить функциями $\oplus$. Затем в полученной формуле все отрицания переменных $\overline{x}_i$ в элементарных конъюнкциях заменяются эквивалентными формулами $x_i \oplus 1$. Далее раскрытием скобок по дистрибутивному закону $x(y \oplus 1) = xy \oplus x$ и приведением подобных членов по закону $x \oplus x = 0$ завершается построение полинома. То, что каждая функция алгебры логики представима единственным полиномом Жегалкина, вытекает из того факта, что количество различных полиномов Жегалкина от $n$ переменных равно числу функций алгебры логики, зависящих от $n$ переменных. Действительно, число монотонных конъюнкций, зависящих от не более чем $n$ переменных (включая 1), равно $2^n$. Каждый полином Жегалкина включает определенный их набор, всего таких наборов $2^{2^n}$. □

**Пример 2.6.** Преобразуем СДНФ функции $f(x_1, x_2, x_3, x_4)$ из примера 2.5 в полином Жегалкина:

$$(x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus 1)(x_4 \oplus 1) \oplus x_1x_2(x_3 \oplus 1)(x_4 \oplus 1) \oplus$$
$$\oplus (x_1 \oplus 1)x_2(x_3 \oplus 1)x_4 \oplus x_1(x_2 \oplus 1)x_3(x_4 \oplus 1) \oplus$$
$$\oplus x_1x_2x_3(x_4 \oplus 1) \oplus (x_1 \oplus 1)x_2x_3x_4 \oplus x_1(x_2 \oplus 1)x_3x_4 \oplus x_1x_2x_3x_4 =$$
$$= 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_2x_3x_4.$$

Применим обозначение $x^{(\sigma)}$ (отличное от $x^{\sigma}$, $\sigma \in \{0, 1\}$):

$$x^{(\sigma)} = \begin{cases} x, \text{если } \sigma = 1, \\ 1, \text{если } \sigma = 0. \end{cases}$$

Это позволит представлять монотонные конъюнкции, содержащие переменные, которым в двоичном наборе $(\sigma_1, \ldots, \sigma_n)$ соответствуют 1, в виде $x_1^{(\sigma_1)} \wedge \ldots \wedge x_n^{(\sigma_n)}$ и записывать полином Жегалкина функции $f(x_1, \ldots, x_n)$, следующим образом:

$$f(x_1, \ldots, x_n) = \bigoplus_{(\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n} a_{(\sigma_1, \ldots, \sigma_n)} x_1^{(\sigma_1)} \wedge \ldots \wedge x_n^{(\sigma_n)}.$$

Здесь $a_{(\sigma_1, \ldots, \sigma_n)} \in \{0, 1\}$ — двоичные коэффициенты; $\bigoplus_{(\sigma_1, \ldots, \sigma_n) \in \{0,1\}^n}$ обозначает суммирование по модулю два по всем двоичным наборам.

Значения функции на конкретном наборе по этой формуле вычисляются как суммы коэффициентов:

$$f(a_1, \ldots, a_n) = \bigoplus_{(\sigma_1, \ldots, \sigma_n) \le (a_1, \ldots, a_n)} a_{(\sigma_1, \ldots, \sigma_n)}.$$

Здесь $\bigoplus_{(\sigma_1,\ldots,\sigma_n)\le(a_1,\ldots,a_n)}$ означает суммирование по всем наборам ($\sigma_1$, …, $\sigma_i$, …, $\sigma_n$), таким что $\sigma_i \le a_i$, $i = 1, \ldots, n$, т. е. по всем минорантам набора ($a_1$, …, $a_n$).

Используя эту формулу, коэффициенты полинома Жегалкина можно представить в виде

$$a_{(\sigma_1,\ldots,\sigma_n)} = f(a_1,\ldots,a_n) \oplus \bigoplus_{(\sigma_1,\ldots,\sigma_n)<(a_1,\ldots,a_n)} a_{(\sigma_1,\ldots,\sigma_n)}. \qquad (2.2)$$

Здесь $\bigoplus_{(\sigma_1,\ldots,\sigma_n)<(a_1,\ldots,a_n)}$ означает суммирование по всем минорантам набора ($a_1$, …, $a_n$), не равным этому набору.

Отсюда получаем способ вычисления коэффициентов полинома Жегалкина в лексикографическом порядке их индексов:

$$a_{(0,\,0,\,\ldots,\,0)} = f(0, \ldots, 0),$$

далее очередные коэффициенты вычисляются по формуле (2.2).

Вычисление рассмотренными выше способами трудоемко. Известен метод быстрого преобразования вектора значений функции в вектор коэффициентов полинома Жегалкина (см. работу [28]).

## 2.3. Теорема о полноте

Существуют системы функций алгебры логики, позволяющие представить формулой любую булеву функцию. Примерами таких систем являются: система

$$\{\overline{x}_1, x_1 \wedge x_2, x_1 \vee x_2\}, \qquad (2.3)$$

позволяющая каждую булеву функцию представить либо в СДНФ, либо в СКНФ, и система

$$\{0, 1, x_1 \wedge x_2, x_1 \oplus x_2\}, \qquad (2.4)$$

позволяющая представить любую булеву функцию полиномом Жегалкина.

Такие системы ($C$) называются *полными*. Их замыкания [$C$] совпадают с множеством $P_2$ всех функций алгебры логики: [$C$] = $P_2$.

*Проблема полноты* заключается в распознавании свойства полноты данной системы. Известны два подхода к этой проблеме.

Первый состоит в том, что формулами над исследуемой системой пытаются представить функции некоторой полной системы. Справедлива следующая теорема.

**Теорема 2.4.** *Если функции некоторой полной системы F представимы формулами над системой C, то система C также полная.*

Доказательство оставляется читателю.

**Пример 2.7.** Система $C = \{\overline{x}_1, x_1 \wedge x_2\}$ является полной, так как функции полной системы (2.3) можно представить формулами над ней.

При таком подходе для каждой новой системы приходится конструировать формулы, выражающие функции некоторой полной системы, с использованием функций из нее.

Второй подход, называемый *критериальным*, позволяет любую систему исследовать универсальным методом. При этом используется понятие замкнутого класса.

*Замкнутым классом* называется система функций $F$, совпадающая со своим замыканием: $F = [F]$.

Введем обозначения:

- $T_0$ — множество функций, сохраняющих константу 0:

$$T_0 = \{f(x_1, \ldots, x_n) : f(0, \ldots, 0) = 0\};$$

- $T_1$ — множество функций, сохраняющих константу 1:

$$T_1 = \{f(x_1, \ldots, x_n) : f(1, \ldots, 1) = 1\};$$

- $S$ — множество самодвойственых функций:

$$S = \{f(x_1, \ldots, x_n) : f(x_1, \ldots, x_n) = f^*(x_1, \ldots, x_n)\};$$

- $M$ — множество монотонных функций, т. е. функций $f(x_1, \ldots, x_n)$, таких что по всем наборам $(a_1, \ldots, a_i, \ldots, a_n)$, таким что $a_i \le b_i$, $i = 1, \ldots, n$, выполняется неравенство $f(a_1, \ldots, a_n) \le f(b_1, \ldots, b_n)$:

$$M = \{f(x_1, \ldots, x_n) : (a_1, \ldots, a_n) \le (b_1, \ldots, b_n) \Rightarrow f(a_1, \ldots, a_n) \le f(b_1, \ldots, b_n)\};$$

- $L$ — множество линейных функций:

$$L = \{f(x_1, \ldots, x_n) : f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n, a_i \in \{0, 1\}\}.$$

**Упражнение 2.3.** Проверьте, что каждое из пяти множеств $T_0$, $T_1$, $S$, $M$, $L$ является замкнутым классом.

*Указание.* Рассмотрите суперпозицию $\varphi(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$ функций $\varphi, f_1, \ldots, f_m$ из данного множества и докажите, что она принадлежит этому множеству. Например, если функции $\varphi, f_1, \ldots, f_m$ линейные, то линейной окажется и их суперпозиция.

**Пример 2.8.** Функция $x_1 \wedge x_2$ принадлежит классам $T_0$, $T_1$ и $M$, но не принадлежит классам $S$ и $L$. Стрелка Пирса $x_1 \downarrow x_2$ не принадлежит ни одному из этих классов. Сумма по модулю два принадлежит классам $T_0$ и $L$ и не принадлежит классам $T_1$, $S$ и $M$.

С целью краткости произвольные функции, не принадлежащие этим замкнутым классам, будем обозначать следующим образом: $f_{\overline{0}}$ — функции, не сохраняющие константу 0, $f_{\overline{1}}$ — функции, не сохраняющие

константу 1, $f_{\overline{S}}$ — несамодвойственные функции, $f_{\overline{M}}$ — немонотонные функции, $f_{\overline{L}}$ — нелинейные функции.

Рассмотрим некоторые свойства функций $f_{\overline{S}}, f_{\overline{M}}, f_{\overline{L}}$.

***Лемма 2.1* (*о несамодвойственной функции*).** Из несамодвойственной функции подстановками вместо переменных тождественной функции или ее отрицания можно получить некоторую константу.

***Доказательство.*** Пусть $f(x_1, \ldots, x_n)$ — несамодвойственная функция. Рассмотрим наборы $(a_1, \ldots, a_n)$ и $(\overline{a}_1, \ldots, \overline{a}_n)$ значений переменных, на которых нарушается самодвойственность: $f(a_1, \ldots, a_n) = f(\overline{a}_1, \ldots, \overline{a}_n)$. Рассмотрим функцию $\varphi(x) = f(x^{a_1}, \ldots, x^{a_n})$. Ясно, что

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

Таким образом, $\varphi(0) = \varphi(1) = c \in \{0, 1\}$, т. е. $\varphi(x)$ — константа. □

**Пример 2.9.** Подставим тождественную функцию $x$ вместо переменных функции импликации $x_1 \to x_2$: $x \to x = \overline{x} \vee x = 1$.

***Лемма 2.2* (*о немонотонной функции*).** Из немонотонной функции подстановками переменной $x$ и констант 0 и 1 вместо переменных можно получить отрицание $\overline{x}$.

***Доказательство.*** Пусть $f(x_1, \ldots, x_n)$ — немонотонная функция. Тогда найдутся два набора значений переменных $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$, на которых нарушается свойство монотонности, т. е. такие, что $(a_1, \ldots, a_n) < (b_1, \ldots, b_n)$, а $f(a_1, \ldots, a_n) > f(b_1, \ldots, b_n)$ (при этом $f(a_1, \ldots, a_n) = 1$, $f(b_1, \ldots, b_n) = 0$).

Образуем функцию $\psi(x) = f(\chi_1(x), \ldots, \chi_n(x))$, где

$$\chi_i(x) = \begin{cases} a_i, \text{если } a_i = b_i, \\ x, \text{если } a_i \neq b_i, \end{cases} i = 1, \ldots, n.$$

Тогда $\psi(0) = f(a_1, \ldots, a_n) = 1$; $\psi(1) = f(b_1, \ldots, b_n) = 0$, так как $\chi_i(0) = a_i$, $\chi_i(1) = b_i$, т. е. $\psi(x) = \overline{x}$. □

***Лемма 2.3* (*о нелинейной функции*).** Из нелинейной функции подстановками констант 0 и 1 вместо переменных можно получить элементарную конъюнкцию $x_1^{\sigma_1} \wedge x_2^{\sigma_2}$ или элементарную дизъюнкцию $x_1^{\sigma_1} \vee x_2^{\sigma_2}$.

***Доказательство.*** Пусть $f(x_1, \ldots, x_n)$ — нелинейная функция. Рассмотрим ее полином Жегалкина. В нем есть хотя бы одно слагаемое, содержащее две или более переменных. Не ограничивая общности, будем считать, что в него входят переменные $x_1$ и $x_2$. Рассмотрим такое слагаемое, содержащее наименьшее число $k$ переменных, $2 \le k \le n$. Также не ограничивая общности, положим, что оно совпадает с $x_1 \cdots x_k$. Тогда полином Жегалкина функции $f(x_1, x_2, \sigma_3, \ldots, \sigma_n)$, где $\sigma_3 = \ldots = \sigma_k = 1$, $\sigma_{k+1} = \ldots = \sigma_n = 0$, имеет вид $\varphi(x_1, x_2) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus x_1 x_2$.

Эквивалентными преобразованиями получим

$$\varphi(x_1, x_2) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus x_1 x_2 = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus x_1 x_2 \oplus a_1 a_2 \oplus a_1 a_2 =$$
$$= a_0 \oplus a_1 a_2 \oplus x_1 (x_2 \oplus a_1) \oplus a_2 (x_2 \oplus a_1) = a_0 \oplus a_1 a_2 \oplus (x_2 \oplus a_1)(x_1 \oplus a_2) =$$
$$= \sigma \oplus (x_1 \oplus \sigma_1)(x_2 \oplus \sigma_2),$$

где $\sigma = a_0 \oplus a_1 a_2$, $\sigma_1 = a_2$, $\sigma_2 = a_1$. Учитывая, что $x \oplus \sigma = \overline{x^{\sigma}} = x^{\bar{\sigma}}$, находим:

$$\varphi(x_1, x_2) = \overline{\overline{(\overline{x_1^{\sigma_1}} \wedge \overline{x_2^{\sigma_2}})^{\sigma}}} = \begin{cases} x_1^{\sigma_1} \vee x_2^{\sigma_2}, \text{если } \sigma = 1, \\ x_1^{\bar{\sigma}_1} \wedge x_2^{\bar{\sigma}_2}, \text{если } \sigma = 0. \end{cases}$$ □

***Следствие 2.7.*** Из нелинейной функции подстановками констант и возможными отрицаниями переменных и самой функции можно получить конъюнкцию.

Действительно, $x_1 x_2 = \left( \overline{\varphi(\overline{x_1^{\sigma_1}}, \overline{x_2^{\sigma_2}})} \right)^{\sigma}$.

**Теорема 2.5 (теорема Поста[1] о функциональной полноте).** *Система функций алгебры логики $F$ является полной тогда и только тогда, когда она не содержится ни в одном из замкнутых классов $T_0$, $T_1$, $S$, $M$ и $L$.*

***Доказательство.*** *Необходимость* следует из очевидного свойства замыкания: если $F_1 \subseteq F_2$, то $[F_1] \subseteq [F_2]$. Поэтому полная система $F$ не может содержаться в замкнутом классе, не являющемся полным, а каждый из перечисленных классов полным не является, например функция стрелка Пирса $x_1 \downarrow x_2$ не принадлежит ни одному из этих классов.

*Достаточность*. Пусть система $F$ не содержится ни в одном из классов $K \in \{T_0, T_1, S, M, L\}$. Тогда в $F$ найдутся не обязательно различные функции $f_{\bar{0}}, f_{\bar{1}}, f_{\bar{S}}, f_{\bar{M}}$ и $f_{\bar{L}}$, не принадлежащие классам $T_0$, $T_1$, $S$, $M$ и $L$ соответственно.

Подстановкой переменной $x$ в функции $f_{\bar{0}}, f_{\bar{1}}$ можно получить отрицание

$$\bar{x} = \begin{cases} f_{\bar{0}}(x, \ldots, x), \text{если } f_{\bar{0}}(1, \ldots, 1) = 0, \\ f_{\bar{1}}(x, \ldots, x), \text{если } f_{\bar{1}}(0, \ldots, 0) = 1 \end{cases}$$

или обе константы

$$c = \begin{cases} 1 = f_{\bar{0}}(x, \ldots, x), \text{если } f_{\bar{0}}(1, \ldots, 1) = 1, \\ 0 = f_{\bar{1}}(x, \ldots, x), \text{если } f_{\bar{1}}(0, \ldots, 0) = 0. \end{cases}$$

В первом случае с помощью функции $f_{\bar{S}}$ по лемме 2.1 получим константу $c$ и следом — ее отрицание $\bar{c}$.

Во втором случае с помощью функции $f_{\bar{M}}$ по лемме 2.2 получим отрицание и следом — вторую константу.

Далее с помощью нелинейной функции $f_{\bar{L}}$ по лемме 2.3 и следствию 2.7 получим конъюнкцию.

[1] Эмиль Леон Пост (Emil Leon Post, 1897—1954) — американский математик.

Таким образом,через функции $f_{\overline{0}}, f_{\overline{1}}, f_{\overline{S}}, f_{\overline{M}}$ и $f_{\overline{L}}$ можно выразить отрицание и конъюнкцию, образующие полную систему, и по теореме 2.4 эти функции составляют полную систему. □

**Пример 2.10.** Система функций $\{x_1x_2, 0, x_1 \equiv x_2\}$ полная, так как $x_1 \equiv x_2 \notin T_0$, $0 \notin T_1, x_1 \equiv x_2 \notin S, x_1 \equiv x_2 \notin M, x_1x_2 \notin L$. Система функций $\{x_1 \oplus x_2, x_1x_2\}$ неполная, так как, например, обе функции содержатся в классе $T_0$.

Полная система называется *базисом*, если никакая ее собственная (т. е. не совпадающая с ней подсистема) не является полной.

***Следствие 2.8.*** Базис содержит не более четырех функций.

***Доказательство.*** Базис содержит функцию $f_{\overline{0}}$. При этом если $f_{\overline{0}}(1,\ldots,1) = 0$, то $f_{\overline{0}} \notin M$, а если $f_{\overline{0}}(1,\ldots,1) = 1$, то $f_{\overline{0}} \notin S$, т. е. функция $f_{\overline{0}}$ является одновременно либо функцией типа $f_{\overline{M}}$, либо функцией типа $f_{\overline{S}}$.

Базис из четырех функций существует. Это система функций $\{x_1x_2, 0, 1, x_1 \oplus x_2 \oplus x_3\}$.

Проверку полноты и базисности системы функций удобно выполнять с использованием таблицы. Ее столбцы соответствуют замкнутым классам $T_0$, $T_1$, $S$, $M$ и $L$, а строки — функциям данной системы. В полях таблицы ставится знак «минус», если функция не принадлежит классу, и знак «плюс», если принадлежит. Таблица для данного базиса из четырех функций имеет вид

| | $T_0$ | $T_1$ | $S$ | $M$ | $L$ |
|---|---|---|---|---|---|
| $x_1x_2$ | + | + | − | + | − |
| 0 | + | − | − | + | + |
| 1 | − | + | − | + | + |
| $x_1 \oplus x_2 \oplus x_3$ | + | + | + | − | + |

Ни одна строка не может быть удалена так, чтобы в каждом столбце остался знак «–». □

Замкнутый класс $F$ называется *предполным*, если он не совпадает с классом всех булевых функций $P_2$ и если добавление к нему любой не принадлежащей ему функции приводит к образованию полной системы: $F \neq P_2$, но $[F \cup \{f\}] = P_2$, если $f \notin F$.

**Упражнение 2.4.** Покажите, что

$$T_0 \cup \{f_{\overline{0}}\} = P_2,\ T_1 \cup \{f_{\overline{1}}\} = P_2,\ S \cup \{f_{\overline{S}}\} = P_2,\ M \cup \{f_{\overline{M}}\} = P_2, L \cup \{f_{\overline{L}}\} = P_2.$$

**Упражнение 2.5.** Укажите, когда система $\{f(x, y)\}$ из одной функции является полной.

***Следствие 2.9.*** Существует только пять предполных классов функций алгебры логики — $T_0$, $T_1$, $S$, $M$ и $L$.

***Доказательство.*** Каждый из этих классов не совпадает с $P_2$. Любой замкнутый класс, не содержащийся ни в одном из этих классов, — полная система. Любая другая замкнутая система либо совпадает с одним

из этих классов, либо является его собственной подсистемой, т. е. не является предполным классом. □

Э. Л. Пост доказал, что множество всех замкнутых классов булевых функций счетно и что каждый из них является конечно порожденным, т. е. имеет конечный базис — конечную систему функций, замыкание которой совпадает с данным классом, а замыкание любой ее собственной подсистемы с ним не совпадает[1].

## 2.4. Минимизация булевых функций

> При чтении популярных книг… наступает страшный миг, когда страница вдруг зарастает математическими формулами, немедля ослепляющими разум читателя.
>
> *В. В. Набоков*. «Ада, или радости страсти»

Каждая функция алгебры логики может быть представлена различными формулами. Поэтому естественно возникает задача нахождения наиболее простых формул, представляющих данную функцию. Ввиду ее практической неразрешимости в общем виде (вследствие лавинообразного возрастания с ростом числа переменных числа возможных вариантов) ограничивают класс формул, в частности, рассматривают представления функций алгебры логики только в дизъюнктивной (ДНФ) или только в конъюнктивной (КНФ) нормальной форме (см. выше). Булева функция, отличная от нуля, может иметь множество ДНФ, а функция, отличная от единицы, — множество КНФ. Минимизация функций в классах ДНФ и КНФ заключается в нахождении наиболее простых таких формул.

ДНФ, содержащие наименьшее число вхожений переменных (т. е. имеющие наименьшую сумму рангов элементарных конъюнкций), называются *минимальными* ДНФ, а ДНФ, содержащие наименьшее число элементарных конъюнкций — *кратчайшими* ДНФ. Аналогично определяются понятия минимальной и кратчайшей КНФ.

Функция $\varphi(x_1, \ldots, x_n)$ называется *импликантой* функции $f(x_1, \ldots, x_n)$, если $\varphi \to f = 1$, т. е. $\varphi(x_1, \ldots, x_n) = 1$ влечет $f(x_1, \ldots, x_n) = 1$.

Функция $\varphi(x_1, \ldots, x_n)$ называется *имплициентой*[2] *функции* $f(x_1, \ldots, x_n)$, если $f \to \varphi = 1$, т. е. $f(x_1, \ldots, x_n) = 1$ влечет $\varphi(x_1, \ldots, x_n) = 1$.

Легко проверить, что $\varphi \to f = 1$ тогда и только тогда, когда $\varphi \vee f = f$, и $f \to \varphi = 1$ тогда и только тогда, когда $\varphi \wedge f = \varphi$.

Импликанты (имплициенты) обладают следующими очевидными свойствами.

---

[1] Упрощенное изложение результатов Поста см. в книге: *Яблонский С. В.*, *Гаврилов Г. П.*, *Кудрявцев В. Б.* Функции алгебры логики и классы Поста. М. : Наука. 1966. Короткое доказательство впоследствии было получено А. Б. Угольниковым (*Угольников А. Б.* О замкнутых классах Поста // Известия вузов. Математика. 1988. № 7 (314). С. 79—88).

[2] Это понятие двойственно импликанте.

1. а) Дизъюнкция импликант функции $f$ является импликантой функции $f$;

б) конъюнкция имплициент функции $f$ является имплициентой функции $f$.

2. а) Если $\varphi$ — импликанта функции $f$ и $\psi$ — любая функция алгебры логики, то $\varphi \wedge \psi$ является импликантой функции $f$;

б) если $\varphi$ — имплициента функции $f$ и $\psi$ — любая функция алгебры логики, то $\varphi \vee \psi$ является имплициентой функции $f$.

3. Любая функция является импликантой (имплициентой) самой себя.

Ясно, что элементарные конъюнкции СДНФ функции $f$ являются ее импликантами, а элементарные дизъюнкции СКНФ этой функции — ее имплициентами.

Будем использовать операцию *склеивания* двух элементарных конъюнкций $K_1 = x_i K_1'$ и $K_2 = \overline{x}_i K_2'$, где элементарные конъюнкции $K_1'$ и $K_2'$ не имеют переменных, входящих в одну из них с отрицанием, а в другую без отрицания. Такие элементарные конъюнкции будем называть *соседними*. Результатом склеивания является элементарная конъюнкция $K_{1,2} = K_1 \circ K_2 = K_1' K_2'$.

***Утверждение 2.6.*** Если элементарные конъюнкции $K_1 = x_i K_1'$ и $K_2 = \overline{x}_i K_2'$ являются импликантами функции $f$, то элементарная конъюнкция $K_1 \circ K_2 = K_1' K_2'$ также является ее импликантой.

Доказательство утверждения оставляется читателю.

В соответствии с тождеством поглощения $K_1 = K_1 \vee K_1 K_2$ будем говорить, что элементарная конъюнкция $K_1$ *поглощает* элементарную конъюнкцию $K = K_1 K_2$.

В соответствии со свойствами импликант используем два правила эквивалентных преобразований ДНФ.

Э1. *Неполное склеивание*: нахождение двух соседних элементарных конъюнкций $K_1 = x_i K_1'$ и $K_2 = \overline{x}_i K_2'$ и добавление в ДНФ результата $K_1 \circ K_2 = K_1' K_2'$ их склеивания.

Э2. *Поглощение*: нахождение в ДНФ двух элементарных конъюнкций, одна их которых поглощает другую, и удаление поглощаемой конъюнкции, т. е. замена $K_1 K_2 \vee K_1$ на $K_1$ (более короткая элементарная конъюнкциям $K_1$ поглощает более длинную $K_1 K_2$).

Результат применения каждого из этих правил зависит от выбора упомянутых в них пар конъюнкций.

Элементарная конъюнкция $K$ из ДНФ (элементарная дизъюнкция $D$ из КНФ) функции алгебры логики называется *простой импликантой* (*простой имплициентой*) этой функции, если из нее нельзя удалить ни одной переменной, сохраняя свойство быть импликантой (имплициентой).

***Утверждение 2.7.*** Пусть $K_1 \vee K_2 \vee \ldots \vee K_p$ — минимальная ДНФ функции $f(x_1, \ldots, x_n)$. Тогда $K_i$ — простые импликанты.

***Доказательство.*** Если это не так, то найдется импликанта $K_i$, которая удалением одной или нескольких переменных преобразуется в про-

стую импликанту $K'$. Тогда по свойствам импликант $f(x_1, \ldots, x_n) = K_1 \vee \vee \ldots \vee K_{i-1} \vee \vee K_i \vee K_{i+1} \vee \ldots \vee K_p = K_1 \vee \ldots \vee K_{i-1} \vee K_i \vee K' \vee K_{i+1} \vee \ldots \vee K_p = = K_1 \vee \ldots \vee K_{i-1} \vee K' \vee K_{i+1} \ldots \vee K_p$. Последнее преобразование по правилу Э2 эквивалентных преобразований ДНФ (элементарная конъюнкция $K_i$ поглощается более простой элементарной конъюнкцией $K'$), т. е. существует ДНФ данной функции, содержащая меньшее число вхождений символов переменных, чем ДНФ $K_1 \vee K_2 \vee \ldots \vee K_p$, так как в конъюнкции $K_i$ больше символов переменных, чем в $K'$. □

Для минимальной КНФ верно двойственное утверждение.

***Утверждение 2.8.*** Минимальная ДНФ (КНФ) представляет собой дизъюнкцию (конъюнкцию) простых импликант (простых имплициент).

***Утверждение 2.9.*** Дизъюнкция (конъюнкция) всех простых импликант (имплициент) булевой функции равна этой функции.

Дизъюнкция (конъюнкция) всех простых импликант (имплициент) булевой функции называется *сокращенной дизъюнктивной нормальной формой* — сокр. ДНФ (*сокращенной конъюнктивной нормальной формой* — сокр. КНФ) этой функции.

**Пример 2.11.** Сокращенной ДНФ функции $f(x_1, x_2, x_3) = \Sigma_1(0, 2, 3, 4, 5, 7)$ (здесь перечислены десятичные эквиваленты двоичных наборов, на которых функция принимает значение 1) является ДНФ

$$\bar{x}_1\bar{x}_3 \vee \bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2 \vee x_1\bar{x}_2 \vee x_1x_3 \vee x_2x_3.$$

Ее минимальные ДНФ следующие:

$$\bar{x}_1\bar{x}_3 \vee x_1\bar{x}_2 \vee x_2x_3, \ \bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2 \vee x_1x_3.$$

Дизъюнкция (конъюнкция) простых импликант (имплициент) булевой функции, равная этой функции, называется *тупиковой ДНФ* (*тупиковой КНФ*) данной функции, если из нее нельзя удалить ни одной простой импликанты (имплициенты), не нарушая этого ее свойства.

Ясно, что минимальные ДНФ (КНФ) являются тупиковыми.

**Пример 2.12.** Кроме указанных в предыдущем примере имеется еще три тупиковые ДНФ той же функции:

$$\bar{x}_1\bar{x}_3 \vee \bar{x}_2\bar{x}_3 \vee x_1x_3 \vee x_2x_3, \ \bar{x}_1\bar{x}_3 \vee \bar{x}_1x_2 \vee x_1\bar{x}_2 \vee x_1x_3, \ \bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2 \vee x_1\bar{x}_2 \vee x_2x_3.$$

Таким образом, минимизация в классе ДНФ (КНФ) сводится к нахождению всех простых импликант (имплициент) и выбору некоторых из них для образования минимальных форм.

Ниже представлен алгоритм Блейка[1] — Порецкого[2] вычисления сокращенной ДНФ булевой функции, заданной ее произвольной ДНФ.

---

[1] *Blake A.* Canonical expression in Boolean algebra : Dissertation. Chicago, 1937.

[2] Платон Сергеевич Порецкий (1846—1907) — доцент Казанского университета, астроном. Первым в России стал заниматься математической логикой.

**Алгоритм Блейка — Порецкого**

Вход: ДНФ булевой функции $f(x_1, \ldots, x_n)$.

Выход: сокращенная ДНФ этой функции.

1. Удалить элементарные конъюнкции, поглощаемые хотя бы одной из остающихся элементарных конъюнкций.

2. Пока возможно: выполнять операцию неполного склеивания, включать ее результат в ДНФ, если он не поглощается ни одной из ее элементарных конъюнкций, и затем выполнять операции поглощения с использованием новой элементарной конъюнкции (если она образовалась).

3. Вернуть полученную ДНФ.

**Теорема 2.6.** *Алгоритм Блейка — Порецкого строит сокращенную ДНФ функции, заданной произвольной ДНФ.*

***Доказательство*** основано на леммах 2.4, 2.5, из которых следует, что алгоритм остановится после того, как в ДНФ будут включены все простые импликанты и в ней не будет иных элементарных конъюнкций. □

***Лемма 2.4.*** Если $K = K_1 \circ K_2 = x_i K_1' \circ \overline{x}_i K_2'$, то $K = x_i K' \circ \overline{x}_i K'$, где $K'$ есть имплициента как $K_1'$, так и $K_2'$.

***Доказательство.*** Такой имплициентой является элементарная конъюнкция

$$K' = K_1' K_2' = x_i K' \circ \overline{x}_i K'. \square$$

***Лемма 2.5.*** Если ДНФ данной функции $f(x_1, \ldots, x_n)$ не является сокращенной, то в ней найдутся две элементарные конъюнкции, склеиванием которых получится элементарная конъюнкция, не поглощаемая ни одной из имеющихся в ДНФ.

***Доказательство.*** Поскольку ДНФ не является сокращенной, найдется не входящая в нее простая импликанта $K$. Ее ранг меньше, чем $n$, так как простые импликанты ранга $n$ либо поглощаются некоторой конъюнкцией в любой ДНФ, либо входят в сокращенную ДНФ. Поэтому некоторая переменная $x_i$ в простой импликанте $K$ не представлена (непосредственно или в виде ее отрицания). Следовательно, $K = x_i K \vee \overline{x}_i K = x_i K \circ \overline{x}_i K = K_0 \circ K_1$. Если в ДНФ имеются элементарные конъюнкции $K_0'$ и $K_1'$, являющиеся имплициентами конъюнкций $K_0$ и $K_1$, то по лемме 2.4 их склеиванием и получается элементарная конъюнкция $K = K_0' \circ K_1'$. Если же хотя бы одна элементарная конъюнкция $K_0$ или $K_1$ не имеет имплициенты в ДНФ, то описанная процедура рекурсивно применяется к ней как к конъюнкции, не входящей в сокращенную ДНФ. В итоге будет получена элементарная конъюнкция, являющаяся импликантой функции $f(x_1, \ldots, x_n)$, не входящая в текущую ДНФ. □

Таким образом, после каждой итерации второго шага алгоритма Блейка — Порецкого получается ДНФ, не имеющая элементарных конъюнкций, поглощаемых некоторой из имеющихся в ней элементарных конъюнкций.

**Пример 2.13.** Построим сокращенную ДНФ функции $f(x_1, x_2, x_3, x_4)$, заданной ДНФ $\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_1\bar{x}_2x_3\bar{x}_4 \vee x_2x_3x_4 \vee \bar{x}_1x_2\bar{x}_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4$.

Элементарных конъюнкций, поглощаемых другими элементарными конъюнкциями этой ДНФ, нет. В пяти последовательных итерациях будут получены следующие ДНФ (в каждой добавляется одна элементарная конъюнкция и одна или две, возможно, удаляются):

$$\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_2x_3x_4 \vee \bar{x}_1x_2\bar{x}_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4 \vee x_1\bar{x}_2\bar{x}_4,$$

$$\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_2x_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4 \vee x_1\bar{x}_2\bar{x}_4 \vee \bar{x}_1x_2x_4,$$

$$\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_2x_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4 \vee x_1\bar{x}_2\bar{x}_4 \vee \bar{x}_1x_2x_4 \vee x_1x_3\bar{x}_4,$$

$$\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_2x_3x_4 \vee x_1x_2x_3 \vee x_1x_3x_4 \vee x_1\bar{x}_2\bar{x}_4 \vee \bar{x}_1x_2x_4 \vee x_1x_3\bar{x}_4 \vee x_1\bar{x}_2x_3,$$

$$\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_2x_3x_4 \vee x_1\bar{x}_2\bar{x}_4 \vee \bar{x}_1x_2x_4 \vee x_1x_3.$$

Последняя полученная ДНФ и есть сокращенная ДНФ заданной функции.

Получаемая таким алгоритмом ДНФ хотя и называется сокращенной, может содержать большое число элементарных конъюнкций и в общем случае может упрощаться удалением некоторых из них. Дело в том, что отдельные элементарные конъюнкции могут быть импликантами дизъюнкций некоторых других элементарных конъюнкций и могут быть удалены по соответствующему свойству импликант.

Таким образом, тупиковые (а среди них и минимальные) ДНФ получаются из сокращенной ДНФ удалением некоторых элементарных конъюнкций.

Варианты такого удаления должны отвечать условию равенства получаемой после удаления некоторых элементарных конъюнкций ДНФ исходной функции $f(x_1, \ldots, x_n)$: на каждом двоичном наборе $(a_1, \ldots, a_n)$ таком, что $f(a_1, \ldots, a_n) = 1$, хотя бы одна из остающихся элементарных конъюнкций должна иметь значение 1. Такое логическое условие можно составить в виде булевой функции $\varphi(y_1, \ldots, y_m)$, где бинарные переменные $y_i$, $i = 1, \ldots, m$, соответствуют элементарным конъюнкциям сокращенной ДНФ $K_1 \vee K_2 \vee \ldots \vee K_m$ и имеют следующий смысл: при $y_i = 1$ элементарная конъюнкция $K_i$ входит в тупиковую ДНФ.

Такое условие можно составить по так называемой импликантной таблице $T$. Это двоичная таблица размером $m \times s$, где $s$ — число наборов из области единичных значений функции. Столбцы соответствуют таким элементам, а строки — простым импликантам $K_i$ сокращенной ДНФ и в то же время — соответствующим логическим переменным $y_i$. Элемент $T(i, j)$ таблицы равен 1, если на $j$-м наборе $i$-я импликанта имеет значение 1.

В таблице могут быть столбцы, имеющие единицу только в одной строке. Очевидно, что соответствующие таким строкам элементарные конъюнкции обязаны быть в любой тупиковой ДНФ. Дизъюнкция таких элементарных конъюнкций образует *ядро* сокращенной ДНФ (его может и не быть). Тупиковые ДНФ образуются пополнением ядра.

Перед составлением упомянутого логического условия таблицу $T$ следует упростить, удалив столбцы, поглощаемые хотя бы одним из ос-

тающихся, т. е. имеющие 1 в тех же строках, что и в одном из остающихся столбцов (этим как бы предвосхитим упрощение составляемого логического условия с помощью тождества поглощения АЛ4). В частности, будут удалены столбцы, имеющие единицу в строке, соответствующей некоторой элементарной конъюнкции ядра. Теперь можно составить логическое условие упрощения ДНФ. Составляется конъюнкция элементарных дизъюнкций переменных, соответствующих единичным элементам столбцов. Приведением полученной КНФ к дизъюнктивному виду получим в виде элементарных конъюнкций варианты тупиковых ДНФ в виде дизъюнкции простых импликант, соответствующих переменным таких элементарных конъюнкций. Далее можно определить сложность каждого варианта и выбрать минимальные ДНФ.

**Пример 2.14.** Рассмотрим сокращенную ДНФ $\bar{x}_1\bar{x}_3 \vee \bar{x}_2\bar{x}_3 \vee x_1\bar{x}_2 \vee x_1x_3$ функции $f(x_1, x_2, x_3) = \Sigma_1(0, 2, 4, 5, 7)$.

Составим импликантную таблицу:

| | | (0,0,0) | (0,1,0) | (1,0,0) | (1,0,1) | (1,1,1) |
|---|---|---|---|---|---|---|
| $y_1$ | $\bar{x}_1\bar{x}_3$ | 1 | 1 | 0 | 0 | 0 |
| $y_2$ | $\bar{x}_2\bar{x}_3$ | 1 | 0 | 1 | 0 | 0 |
| $y_3$ | $x_1\bar{x}_2$ | 0 | 0 | 1 | 1 | 0 |
| $y_4$ | $x_1x_3$ | 0 | 0 | 0 | 1 | 1 |

Ядро сокращенной ДНФ образуют элементарные конъюнкции $\bar{x}_1\bar{x}_3$, $x_1x_3$. Они имеют значение 1 на двоичных наборах (0, 1, 0) и (1, 1, 1). После упрощения имеем таблицу

| | | (0,1,0) | (1,0,0) | (1,1,1) |
|---|---|---|---|---|
| $y_1$ | $\bar{x}_1\bar{x}_3$ | 1 | 0 | 0 |
| $y_2$ | $\bar{x}_2\bar{x}_3$ | 0 | 1 | 0 |
| $y_3$ | $x_1\bar{x}_2$ | 0 | 1 | 0 |
| $y_4$ | $x_1x_3$ | 0 | 0 | 1 |

Логическое условие имеет вид $y_1(y_2 \vee y_3)y_4$. Приведением к дизъюнктивному виду получим $y_1y_2y_4 \vee y_1y_3y_4$, отсюда имеем две тупиковые ДНФ $\bar{x}_1\bar{x}_3 \vee \bar{x}_2\bar{x}_3 \vee x_1x_3$ и $\bar{x}_1\bar{x}_3 \vee x_1\bar{x}_2 \vee x_1x_3$.

## 2.5. Геометрическая интерпретация дизъюнктивной нормальной формы

Миром правит геометрия, ибо геометрия —
земное отражение божественного промысла.

*Дж. Бэнвилл*. «Кеплер»

Рассмотренные в предыдущем параграфе понятия имеют наглядную и удобную для анализа и компьютерной реализации геометрическую интерпретацию с использованием двоичного многомерного куба $\mathcal{B}^n$

(см. параграф 1.1). *Интервалом* $I(\mathbf{a}, \mathbf{b})$ двоичного $n$-мерного куба с *верхней границей* $\mathbf{a} = (a_1, \ldots, a_n)$ и *нижней границей* $\mathbf{b} = (b_1, \ldots, b_n)$ называется множество двоичных наборов $\mathbf{c} = (c_1, \ldots, c_i, \ldots, c_n)$, $b_i \le c_i \le a_i$, $i = 1, \ldots, n$.

Интервалы $I(\mathbf{a}, \mathbf{b})$ удобно представлять троичными векторами $(\alpha_1, \ldots, \alpha_n)$, где

$$\alpha_i = \begin{cases} a_i, \text{если } a_i = b_i, \\ *, \text{если } a_i \ne b_i. \end{cases}$$

Здесь символ $*$ обозначает, что половина двоичных наборов данного интервала в соответствующей позиции имеет значение 0, а в остальных наборах имеется значение 1, т. е. двоичные наборы интервалов $(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ и $(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$ попарно различаются в этой позиции. Поэтому $*$ интерпретируется как двухэлементное множество $\{0, 1\}$ возможных значений в соответствующей позиции. Тогда значения 0 и 1 интерпретируются как одноэлементные множества $\{0\}$ и $\{1\}$. Соответственно такой интерпретации ниже при описании операций над интервалами применяются теоретико-множественные поэлементные операции $0 \cup 1 = *$, $0 \cap * = 0$, $1 \cap * = 1$, $* \cap * = *$ (иные сочетания значений операндов не используются).

*Размерностью* $\dim I(\mathbf{a}, \mathbf{b})$ интервала $I(\mathbf{a}, \mathbf{b})$ двоичного $n$-мерного куба называется число символов $*$ в его обозначении, а число $k = n - \dim I(\mathbf{a}, \mathbf{b})$ называется его *рангом* ($\mathrm{rk} I(\mathbf{a}, \mathbf{b})$). Нульмерными интервалами являются вершины двоичного $n$-мерного куба, а одномерными — его ребра. Сам двоичный $n$-мерный куб можно рассматривать как $n$-мерный интервал нулевого ранга.

Два интервала $(\alpha_1, \ldots, \alpha_n)$ и $(\beta_1, \ldots, \beta_n)$ называются *смежными*, если имеется ровно одна так называемая *контрарная* пара значений $\{\alpha_i, \beta_i\} = \{0, 1\}$. В векторной нотации удобно описывать две операции над интервалами. *Пересечение* ($\cap$) двух интервалов, не имеющих контрарных пар, образуется покомпонентным пересечением элементов их векторных представлений:

$$(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) \cap (\beta_1, \ldots, \beta_i, \ldots, \beta_n) = (\alpha_1 \cap \beta_1, \ldots, \alpha_i \cap \beta_i, \ldots, \alpha_n \cap \beta_n).$$

*Сопряжение* (обозначение $\circ$) соседних интервалов отличается от этой операции тем, что элементы контрарной пары объединяются (т. е. в соответствующей позиции ставится значение $*$), а элементы в остальных позициях пересекаются. Пересечение соответствует пересечению интервалов как множеств двоичных наборов, а сопряжение — объединению интервалов, являющихся подмножествами сопрягаемых интервалов.

**Пример 2.15.** $(1, *, 0, *, 1) \cap (*, 1, 0, *, 1) = (1, 1, 0, *, 1)$;
$(1, *, 0, *, 1) \circ (*, 1, 1, *, 1) = (1, 1, *, *, 1)$.

Функцию алгебры логики удобно представлять отметками вершин куба $\mathcal{B}^n$, на которых она принимает значение 1. Это множество называют *носителем* этой функции и обозначают $\mathcal{N}_f^n$.

**Упражнение 2.6.** Докажите, что носитель $\mathcal{N}_K^n$ любой конъюнкции $K = x_{i_1}^{\sigma_1} \dots x_{i_r}^{\sigma_r}$, рассматриваемой как функция, зависящая от $n$ переменных $x_1$, …, $x_n$, есть $(n - r)$-мерный интервал куба $\mathcal{B}^n$.

**Упражнение 2.7.** Докажите, что для любых двух функций $f$, $g$, зависящих от одних и тех же $n$ переменных, справедливы тождества

$$\mathcal{N}_{f \vee g} = \mathcal{N}_f \cup \mathcal{N}_g,\ \mathcal{N}_{f\&g} = \mathcal{N}_f \cap \mathcal{N}_g, \mathcal{N}_{\overline{f}} = \mathcal{B}^n \setminus \mathcal{N}_f,$$

$$\mathcal{N}_{f \oplus g} = \mathcal{N}_f \,\overline{\cup}\, \mathcal{N}_g = (\mathcal{N}_f \setminus \mathcal{N}_g) \cap (\mathcal{N}_g \setminus \mathcal{N}_f).$$

**Определение 2.6.** Множество интервалов, объединение которых равно носителю функции, называется *покрытием носителя функции интервалами* (коротко — *покрытием*).

Покрытие, из которого нельзя удалить ни один из интервалов, называется *тупиковым*. *Сложностью* покрытия называется сумма рангов входящих в него интервалов. Покрытие минимальной сложности называется *минимальным*. Интервал, являющийся подмножеством носителя функции, называется ее *единичным интервалом*. Единичный интервал, не являющийся собственным подмножеством никакого другого единичного интервала, называется *максимальным единичным интервалом*. Покрытие носителя функции $n$ переменных, образованное интервалами ранга $n$, называется *совершенным*. Покрытие, содержащее все единичные максимальные интервалы, называется *сокращенным*.

Носитель простой импликанты есть максимальный единичный интервал. Совершенной, сокращенной, минимальным и тупиковым ДНФ соответствуют одноименные покрытия. Пересечению элементарных конъюнкций соответствует пересечение интервалов, а склеиванию элементарных конъюнкций — сопряжение интервалов.

Таким образом, всем действиям с ДНФ соответствуют действия с интервалами.

Тупиковые и минимальные ДНФ можно строить с помощью импликантных таблиц, строки которых соответствуют максимальным единичным интервалам, а единицы в клетках означают вхождение соответствующего столбцу элемента в интервал. Логические переменные $y_i$ имеют следующий смысл: $i$-й интервал входит в покрытие.

**Пример 2.16.** Рассмотрим сокращенное покрытие

$$\{I_1, I_2, I_3, I_4, I_5, I_6\} = \{(0, *, 0), (*, 0, 0), (0, 1, *), (1, 0, *), (*, 1, 1), (1, *, 1)\}$$

множества {(0, 0, 0), (0, 1, 0), (1, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0), (1, 1, 1)} вершин трехмерного двоичного куба. Импликантная таблица имеет вид

| | | (0,0,0) | (0,1,0) | (1,0,0) | (0,1,1) | (1,0,1) | (1,1,1) |
|---|---|---|---|---|---|---|---|
| $y_1$ | (0,*,0) | 1 | 1 | 0 | 0 | 0 | 0 |
| $y_2$ | (*,0,0) | 1 | 0 | 1 | 0 | 0 | 0 |
| $y_3$ | (0,1,*) | 0 | 1 | 0 | 1 | 0 | 0 |
| $y_4$ | (1,0,*) | 0 | 0 | 1 | 0 | 1 | 0 |
| $y_5$ | (*,1,1) | 0 | 0 | 0 | 1 | 0 | 1 |
| $y_6$ | (1,*,1) | 0 | 0 | 0 | 0 | 1 | 1 |

Ядра в данном случае нет, таблицу упростить нельзя. Каждый элемент множества входит в два интервала, и логическое условие покрытия содержит шесть элементарных дизъюнкций:

$$(y_1 \vee y_2)(y_1 \vee y_3)(y_2 \vee y_4)(y_3 \vee y_5)(y_4 \vee y_6)(y_5 \vee y_6).$$

Приведением к ДНФ получим пять вариантов тупиковых покрытий, соответсвующих элементарным конъюнкциям этой ДНФ:

$$y_1y_4y_5 \vee y_2y_3y_6 \vee y_1y_2y_5y_6 \vee y_2y_3y_4y_5 \vee y_1y_3y_4y_6.$$

В том числе имеем два минимальных покрытия (соответствуют двум первым элементарным конъюнкциям построенной ДНФ):

$$\{I_1, I_4, I_5\} = \{(0, *, 0), (1, 0, *), (*, 1, 1)\}; \{I_2, I_3, I_6\} = \{(*, 0, 0), (0, 1, *), (1, * 1)\}.$$

Пусть заданы покрытиями $\Pi_1$ и $\Pi_2$ два множества $M_1$ и $M_2$ двоичных наборов длины $n$. Следующий алгоритм, получаемый некоторым дополнением алгоритма Блейка — Порецкого, определяет, верно ли, что $M_2 \subseteq M_1$.

---

**Алгоритм сравнения двух покрытий**

Вход: Произвольные покрытия $\Pi_1$ и $\Pi_2$ подмножеств $M_1$ и $M_2$ единичного $n$-мерного куба.

Выход: $M_2 \subseteq M_1$?

1. Принять $\Pi_1' = \Pi_1, \Pi_2' = \Pi_2$.

2. Пока возможно, удалять все интервалы из $\Pi_1'$ и $\Pi_2'$, покрываемые отдельными остающимися в $\Pi_1'$ интервалами, находить в $\Pi_1'$ два интервала, порождающие сопряжением интервал, не покрываемый ни одним из имеющихся в покрытии $\Pi_1'$ интервалов, и включать его в покрытие $\Pi_1'$.

3. Если $\Pi_2' = \varnothing$ , вернуть *true*.

4. Вернуть *false*.

---

Применяя этот алгоритм сначала к покрытиям $\Pi_1$, $\Pi_2$, а затем к ним же, но в обратном порядке, можно установить, в каком из отношений ($M_1 \subset M_2$, $M_2 \subset M_1$, $M_1 = M_2$ или $M_1$ и $M_2$ не сравнимы) находится пара множеств.

Исходное покрытие может быть произвольным набором интервалов, таким что каждый элемент покрываемого множества является элементом хотя бы одного интервала и, напротив, элементы дополнения этого множества не входят ни в один из интервалов. Например, исходное покрытие может быть совершенным, т. е. состоять из одноэлементных

интервалов. Но предпочтительнее использовать по возможности более «крупные» интервалы. Их можно находить, например, в двоичном $n$-мерном кубе, на котором выделены элементы покрываемого множества, или по картам Карно[1]. *Карта Карно* — это прямоугольная таблица, столбцы которой соответствуют переменным $x_1, \ldots, x_k$, а строки — переменным $x_{k+1}, \ldots, x_n$. Столбцы и строки карты помечаются наборами значений соответствующих переменных так, что метки соседних столбцов или строк (с учетом циклического замыкания от последнего столбца к первому и от последней строки к первой) различались в одной позиции. Такое размещение двоичных наборов называется *кодом Грея*. В клетки таблицы, соответствующие элементам покрываемого множества, заносятся значения 1. Правильным конфигурациям из клеток с единицами — образующим (с учетом замыкания по столбцам и строкам) заполненные единицами прямоугольники — и соответствуют интервалы, которые можно использовать в исходном покрытии.

Как правило, число $n$ не превышает четырех. При больших числах $n$ целесообразно использовать $2^{n-4}$ карт по числу наборов значений переменных $x_5, \ldots, x_n$. При внимательном анализе небольших таблиц можно сразу найти все максимальные интервалы, тогда исходное покрытие окажется сокращенным и алгоритм его не изменит. Но не всегда удается увидеть в таблице все максимальные интервалы, а при использовании нескольких таблиц, представляющих более сложные множества при $n > 6$, даже если взять максимальные интервалы этих таблиц, они могут в сочетании образовывать более крупные интервалы, но вполне подходят как кандидаты в начальное покрытие, к которому применяется описанный выше алгоритм.

**Упражнение 2.8.** Постройте исходное покрытие подмножества куба $\{0, 1\}^5$, заданного двумя картами Карно для $x_5 = 0$ и $x_5 = 1$:

$x_5 = 0$

| $(x_1, x_2)$ \ $(x_3, x_4)$ | (0,0) | (0,1) | (1,1) | (1,0) |
|---|---|---|---|---|
| (0,0) | 1 | 0 | 0 | 0 |
| (0,1) | 1 | 0 | 0 | 1 |
| (1,1) | 1 | 0 | 0 | 1 |
| (1,0) | 0 | 0 | 0 | 0 |

$x_5 = 1$

| $(x_1, x_2)$ \ $(x_3, x_4)$ | (0,0) | (0,1) | (1,1) | (1,0) |
|---|---|---|---|---|
| (0,0) | 1 | 0 | 0 | 0 |
| (0,1) | 0 | 0 | 0 | 0 |
| (1,1) | 1 | 0 | 0 | 1 |
| (1,0) | 0 | 0 | 0 | 1 |

и постройте сокращенное покрытие этого множества.

[1] Морис Карно (Maurice Karnaugh, род. 1924) — американский физик.

*Указание.* По первой карте находим интервалы (0, ∗, 0, 0, 0), (∗, 1, ∗, 0, 0). По второй карте обнаружим три интервала: (0, 0, 0, 0, 1), (1, 1, ∗, 0, 1), (1, ∗, 1, 0, 1).

Если использовать эти пять интервалов в качестве исходного покрытия, алгоритм обнаружит еще один максимальный интервал (0, 0, 0, 0, ∗). Таким образом, совершенное покрытие состоит из шести интервалов.

Используется также *алгоритм Куайна — МакКласки*[1]. Согласно этому алгоритму для построения сокращенного покрытия, пока возможно, выполняются циклически сначала так называемые *неполные склеивания*, т. е. сопряжения интервалов одного и того же ранга, различающихся только в одной позиции (контрарной паре), а затем все возможные поглощения. Такой алгоритм построит сокращенное покрытие, если он будет применен к совершенному покрытию. Если же исходное покрытие совершенным не является, потребуется сначала его усложнить, заменив элементарные конъюнкции меньшего ранга дизъюнкциями соответствующих конъюнкций большего ранга. Например, по покрытию (1, 1, 1), (1, ∗, 0), (0, 0, 0) по алгоритму Блейка — Порецкого сопряжением первого и второго интервалов с последующим поглощением первого получается покрытие (1, 1, ∗), (1, ∗, 0), (0, 0, 0), далее сопряжением двух последних интервалов с последующим поглощением получается сокращенное покрытие (1, 1, ∗), (1, ∗, 0), (∗, 0, 0). Для применения алгоритма Квайна — МакКласки сначала требуется преобразовать исходное покрытие в совершенное «расщеплением» второго интервала: (1, 1, 1), (1, 1, 0), (1, 0, 0), (0, 0, 0).

*О сложности нахождения минимального покрытия.* Описанный метод нахождения тупиковых и минимальных покрытий в общем случае может потребовать экспоненциально возрастающих с числом переменных объемов вычислений и практически оказывается неприемлемым. Поэтому используют приближенные алгоритмы, которые могут приводить к решению, отличающемуся от минимального. Такими алгоритмами являются, например, различные варианты градиентного алгоритма покрытия двоичной таблицы (см. гл. 11).

*О минимизации КНФ.* По заданной КНФ по принципу двойственности можно получить ДНФ отрицания той же функции. Построением сокращенных, тупиковых и минимальных ДНФ и последующим преобразованием их по тому же принципу двойственности получим сокращенную, тупиковые и минимальные КНФ этой же функции.

*О минимизации частичных функций алгебры логики.* Частичная функция алгебры логики $F(x_1, \ldots, x_n)$ принимает значение 1 на двоичных наборах из области единичных значений и значение 0 на двоичных наборах из области нулевых значений. На остальных наборах эта функция не определена. Функции $F(x_1, \ldots, x_n)$ соответствует множество функций

[1] Уиллард Ван Орман Куайн (Willard Van Orman Quine, 1908—2000) — американский логик и философ; Эдвард МакКласки (Edward McCluskey, род. 1929) — американский инженер и математик.