

Таран Т. А.

ОСНОВЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Киев
«Просвіта»
2003

ББК ????? ?????

Т ??

Т ?? Таран Т. А.

Основы дискретной математики.— К.: Просвіта, 2003.— 288 с.

Аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация аннотация аннотация.

Аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация.

Ил. 103. Табл. 25. Список лит.: с. 287 (48 назв.)

Аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация.

Аннотация аннотация аннотация аннотация аннотация
аннотация аннотация аннотация.

Рецензенты: ? . ? . ??????????
? . ? . ??????????

Н а в ч а л ь н е в и д а н н я

Таран Тетяна Архипівна

Основи дискретної математики

(Російською мовою)

В авторській редакції
Комп'ютерна верстка М. Є. Пігурнов
Дизайн обкладинки ? . ? . ??????????

© Таран Т. А., 2003

© ПТФ «Просвіта», 2003

ISBN-966-7115-

Підп. до друку ???.2003. Формат 84x108/32. Папір офс. Спосіб друку — офсет.
Ум. друк. арк. ???, Обл.-вид. арк. ??,?. Зам. № . Наклад ??? пр.

Предисловие

Дискретная математика является базовым курсом при подготовке специалистов по информационным технологиям и искусственному интеллекту. Однако, несмотря на то, что вычислительная техника и программирование существуют уже более пятидесяти лет, до сих пор нет такого учебника, который стал бы «классическим» для этой дисциплины. Учебники по дискретной математике в значительной степени отражают область интересов и симпатии их авторов. Это во многом обусловлено разнообразием материала, который относят к курсу «Дискретная математика». Предлагаемый учебник не является исключением в этом отношении. Книга написана по материалам лекций, которые в течение нескольких лет читаются автором в Национальном техническом университете Украины «Киевский политехнический институт». Это второе издание учебника, первое издание вышло в 1998 г. в издательстве «Просвіта».

Целью учебника является изложение основных понятий и методов, необходимых для изучения последующих дисциплин специальностей «прикладная математика», «информационные технологии» и пр., формирование мировоззрения на дискретную математику и логику как на фундаментальную науку, используемую для формализации знаний. Поэтому в книгу включены основные разделы, используемые в новых информационных технологиях, таких как системы обработки данных, моделирование сложных систем, системы искусственного интеллекта.

Книга состоит из 15 глав. Условно ее можно разделить на две части. Первая часть содержит традиционные разделы дискретной математики: теорию множеств, теорию отношений и отображений, основы теории графов. В последнее время в теории искусственного интеллекта все чаще используются такие структуры, как решетки, поэтому в учебник включены основы теории решеток и их представлений. Вторая часть учебника посвящена математической логике.

При изложении основ математической логики основное внимание уделяется применению логических методов для формализации знаний и рассуждений. При изложении математической логики ведущими являются идеи, связанные с понятием аксиоматического метода, его использованием для построения формальных систем, отображением формальной системы на модели и применением этого математического аппарата для формализации и исследования проблемных областей. Поэтому при изложении логики приводится большое количество содержательных логических задач.

Несмотря на то, что учебник предназначен для инженеров, в книгу включены некоторые довольно абстрактные разделы осно-

ваний математики: исследование свойств исчисления предикатов, формализация арифметики и теорема Гёделя о неполноте. Значение теоремы Гёделя выходит за рамки формальной арифметики и имеет общематематический характер. Эта теорема говорит о невозможности полной формализации сколько-нибудь сложной математической теории и часто используется при обсуждении методологических проблем формализации, сравнительных возможностей человека и компьютера и т.д. Поэтому знакомство с теоремой Гёделя следует считать элементом математической культуры, необходимым не только для профессионалов-математиков, — подобно тому, как знание о невозможности вечного двигателя необходимо не только для профессионалов-физиков.

Последняя глава посвящена изложению основ теории алгоритмов. Основное внимание уделяется изучению проблемы вычислимости и связи ее с проблемами логического вывода.

Многие разделы, такие, как «Комбинаторика», «Абстрактные алгебры», «Теория автоматов», не вошли в данное издание. В основном это объясняется тем, что они читаются в других курсах, а также ограниченностью объема книги.

Автор выражает благодарность О. П. Кузнецову за совместную работу над главой «Теория графов», а также за ценные замечания, высказанные им при чтении рукописи. Автор также глубоко благодарен С. В. Сироте, главному редактору издательства «Просвіта», без которого эта книга не была бы издана, и М. Е. Пигурнову, взявшему на себя труд по подготовке макета книги, а также своим рецензентам

Глава 1.

МНОЖЕСТВА

1.1. Понятие множества

Создателем теории множеств был Георг Кантор¹. Основой этой теории является понятие множества.

↪ **Определение 1.1.** (по Кантору) *Множество S* есть любое собрание определенных и различимых между собой объектов нашей интуиции или интеллекта, мыслимое как единое целое. Эти объекты называются *элементами* множества.

Определение Кантора не является точным математическим определением, это интуитивное определение *понятия* множества. В дальнейшем мы увидим, что точное математическое определение множества вызывает серьезные затруднения.

Существенным пунктом канторовского понимания множества является то, что собрание объектов «мыслится как единое целое», т.е. само рассматривается как *один предмет*. Сами же «объекты нашей интуиции или интеллекта» могут быть совершенно произвольными: множество может состоять, например, из студентов данного курса, звезд на небе или простых чисел, — определение не накладывает никаких ограничений на природу предметов, входящих в множество. В математике в качестве элементов множеств обычно выступают такие объекты, как точки, кривые, числа, множества чисел и т. п. Канторовская формулировка позволяет также рассматривать множества, элементы которых по той или иной причине нельзя точно указать.

В канторовской концепции множества указывается, что элементы множества должны быть «различимыми» объектами, т.е. множество не может содержать двух одинаковых элементов. Эпитет «определенный» понимается в том смысле, что если дано какое-либо множество и некоторый предмет, то можно определить, является этот предмет элементом данного множества или нет. Отсюда вытекает, что множество *полностью определяется своими элементами*.

В дальнейшем будем использовать стандартные обозначения числовых множеств: \mathbf{N} — множество натуральных чисел; \mathbf{Z} — множество целых чисел; \mathbf{Q} — множество рациональных чисел; \mathbf{R} — множество вещественных чисел; \mathbf{C} — множество комплексных чисел.

Об элементах говорят, что они *принадлежат* множеству, и записывают это так: $x \in A$ (читается: « x принадлежит множеству A », или « x является элементом множества A »). Допускается запись: $x_1, x_2, \dots, x_n \in A$, если все эти элементы принадлежат множеству A . Запись $x \notin A$ означает, что x не принадлежит множеству A .

¹ Георг Кантор (**Cantor**) (1845—1918) — немецкий математик.

Однозначно определенное множество X , элементами которого являются предметы x_1, x_2, \dots, x_n , будем обозначать $X = \{x_1, x_2, \dots, x_n\}$. В частности, $\{x\}$ — так называемое *единичное* множество, — есть одноэлементное множество, единственным элементом которого является x . Если множество X конечное, то количество элементов в множестве обозначается $|X|$. Например, если $X = \{a, b, c\}$, то $|X| = 3$.

Порядок следования элементов в множестве не имеет значения. Например, $\{a, b, c\}$ и $\{c, a, b\}$ — это одно и то же множество.

Элементы какого-либо множества сами могут быть множествами. Например, множество $A = \{\{1, 3\}, \{2, 4\}, \{5, 6\}\}$ есть множество из трех элементов ($|A| = 3$), а именно: $\{1, 3\}$, $\{2, 4\}$ и $\{5, 6\}$. Множества $B = \{\{1, 2\}, \{2, 3\}\}$ и $C = \{1, 2, 3\}$ — различные множества, так как элементами первого являются $\{1, 2\}$, $\{2, 3\}$, и $|B| = 2$, а элементами второго — $1, 2$ и 3 , $|C| = 3$. Множества $D = \{\{1, 2\}\}$ и $G = \{1, 2\}$ также различны, так как первое — одноэлементное множество, имеющее единственным своим элементом $\{1, 2\}$, а второе имеет своими элементами 1 и 2 .

На основании канторовского понимания множества можно дать определение множества через его свойства, которые постулируются как *интуитивные принципы*.

1.1.1. Интуитивный принцип объемности

Интуитивный принцип объемности формулируется следующим образом.

Два множества равны тогда и только тогда, когда они состоят из одних и тех же элементов.

Равенство множеств обозначается: $A = B$, неравенство — $A \neq B$.

Доказательство равенства каких-либо двух конкретных множеств A и B состоит из двух частей: необходимо доказать, что если $x \in A$, то $x \in B$, и обратное: если $x \in B$, то $x \in A$.

✱ **Пример 1.** Докажем, что множество A всех четных положительных целых чисел равно множеству B положительных целых чисел, представимых в виде суммы двух нечетных положительных целых чисел.

Допустим сначала, что $x \in A$, и докажем, что $x \in B$. Действительно, если $x \in A$, то $x = 2m$, так что $x = (2m - 1) + 1$. Это и означает, что $x \in B$.

Предположим теперь, что $x \in B$, и выведем отсюда, что $x \in A$. Если $x \in B$, то $x = (2p - 1) + (2q - 1)$, откуда $x = 2(p + q - 1)$, из чего следует, что $x \in A$.

Таким образом, мы доказали, что множества A и B состоят из одних и тех же элементов, следовательно, $A = B$.

1.1.2. Интуитивный принцип абстракции

Обозначение множества с помощью перечисления его элементов слишком громоздко, чтобы его использовать для задания множеств, имеющих, хотя и конечное, но большое число элементов, и вовсе неприменимо для бесконечных множеств.

⇨ **Определение 1.2.** Будем понимать под *высказыванием* повествовательное предложение, которое можно охарактеризовать как истинное или ложное. Тогда под *одноместным предикатом (формой)* от $x - P(x)$ будем понимать конечную последовательность, состоящую из слов и символа x , такую, что если каждое вхождение x в эту последовательность заменить одним и тем же именем некоторого предмета соответствующего рода, то в результате получится высказывание. Например, каждое из следующих выражений есть предикат от x :

$5 \text{ делит } x; x^2 + x + 1 > 0; x \text{ любит Джона}; x^2 = 2; 0 < x.$

Теперь можно сформулировать интуитивный принцип абстракции.

Любой одноместный предикат $P(x)$ определяет некоторое множество A таким образом, что элементами множества A являются те и только те предметы a , для которых $P(a)$ есть истинное высказывание.

Поскольку множества, состоящие из одних и тех же элементов, равны, то любой предикат $P(x)$ определяет в точности одно, вполне определенное, множество, обычно обозначаемое в математике через $\{x \mid P(x)\}$, что читается так: «множество всех таких x , что $P(x)$ ». Таким образом, $a \in \{x \mid P(x)\}$ в том и только том случае, если $P(a)$ — истинное высказывание. Можно сказать, что решение вопроса, является ли данный предмет a элементом множества $\{x \mid P(x)\}$, есть решение вопроса, обладает ли a некоторым определенным свойством (качеством). Поэтому, когда для определения некоторого множества A используют какой-нибудь предикат $P(x)$, его обычно называют *определяющим свойством множества A* . В таком случае принцип абстракции можно сформулировать в виде утверждения: «Каждое свойство определяет некоторое множество».

Введение в обращение бесконечных множеств с помощью определяющих их свойств — процедура, хорошо известная из аналитической геометрии. Например, окружность радиуса 2 на плоскости с центром в начале координат есть множество всех таких x , что x находится на расстоянии в две единицы от начала координат.

Следующие выражения представляют собой множества, определенные посредством некоторых свойств:

$A = \{x \mid x \in \mathbf{N}, x < 10\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\};$

$B = \{x \mid x \text{ есть функция, непрерывная на замкнутом отрезке действительных чисел от } 0 \text{ до } 1\}$.

Для обозначения множеств используются и различные видоизменения основной скобочной записи. Например, $C = \{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$ обозначает множество всех действительных чисел, лежащих в интервале $[0, 1]$, а $D = \{x \in \mathbf{Q}^+ \mid x^2 < 2\}$ — множество всех положительных рациональных чисел, квадраты которых меньше числа 2. Вместо того чтобы писать $\{y \mid y = 2x, \text{ где } x \text{ есть целое число}\}$, мы можем написать $\{2x \mid x \in \mathbf{Z}\}$. Аналогично через $\{x^2 \mid x \in \mathbf{Z}\}$ обозначается множество квадратов целых чисел.

Принцип объемности, принцип абстракции и принцип выбора (пока, за ненадобностью, не сформулированный) — это та основа, на которой строится канторовская теория множеств. Основное понятие, используемое при формулировке этих принципов, — это принадлежность элемента множеству.

1.1.3. Отношение включения

Введем еще два отношения между множествами.

↪ **Определение 1.3.** Если A и B есть множества, то говорят, что A *включено* в B , если каждый элемент множества A является также элементом множества B (символическая запись: $A \subseteq B$ или $B \supseteq A$). В этом случае говорят также, что множество A *есть подмножество* множества B .

Таким образом, $A \subseteq B$ означает, что для каждого x , если $x \in A$, то $x \in B$.

Множество A *строго включено* в B , или B *строго включает* A , или A *есть собственное подмножество* B , если $A \subseteq B$ и $A \neq B$ (символически: $A \subset B$).

Например, множество четных чисел строго включено в множество \mathbf{Z} целых чисел, а множество \mathbf{Q} рациональных чисел строго включает \mathbf{Z} .

Основные свойства отношения включения:

- $X \subseteq X$ — рефлексивность,
- $X \subseteq Y$ и $Y \subseteq Z$ влечет $X \subseteq Z$ — транзитивность,
- $X \subseteq Y$ и $Y \subseteq X$ влечет $X = Y$ — антисимметричность.

Последнее свойство выражает в терминах отношения включения два шага в доказательстве равенства двух множеств: для того, чтобы доказать, что $X = Y$, надо доказать, что $X \subseteq Y$, а затем, что $Y \subseteq X$.

Из принципа объемности следует, что может быть только одно множество, не имеющее элементов. Это множество называют *пустым множеством* и обозначают его символом \emptyset . Пустое множество есть подмножество любого множества.

Каждое множество $A \neq \emptyset$ имеет, по крайней мере, два различных подмножества: само A и \emptyset , т.е. $A \subseteq A$ и $\emptyset \subseteq A$. Кроме того, каждый элемент множества A определяет некоторое подмножество множества A : если $a \in A$, то $\{a\} \subseteq A$. Подмножествами множества A будут также множества, составленные из двух элементов множества A , трех элементов, и так далее. В результате мы получим множество всех подмножеств множества A .

↪ **Определение 1.4.** Множество всех подмножеств множества A называется *множеством-степенью* множества A и обозначается $\wp(A)$.

Например, если $A = \{1, 2, 3\}$, то $\wp(A) = \{\{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1\}, \{2\}, \{3\}, \emptyset\}$.

Подчеркнем различие между отношениями принадлежности и включения: если $B \subseteq A$, то $B \in \wp(A)$, а если $a \in A$, то $\{a\} \subseteq A$ и $\{a\} \in \wp(A)$.

Термин «множество-степень множества A » принят в качестве наименования множества всех подмножеств множества A оттого, что для конечного множества A , состоящего из n элементов, $\wp(A)$ имеет 2^n элементов.

Докажем это утверждение.

Будем обозначать C_n^k количество всевозможных перестановок из n по k , определяемое формулой: $\frac{n!}{k!(n-k)!}$. В конечном множестве A , состоящем из n элементов, содержатся: пустое подмножество \emptyset , C_n^1 одноэлементных подмножеств, C_n^2 двухэлементных подмножеств, ..., C_n^k k -элементных подмножеств, ..., $1 = C_n^n$ — само множество A . Итого: $C_n^0 + C_n^1 + C_n^2 + \dots + C_n^k + \dots + C_n^n = (1 + 1)^n = 2^n$ подмножеств.

1.2. Операции над множествами

Продолжая описание методов получения новых множеств из уже существующих, мы введем две операции, при помощи которых из двух множеств строится новое множество.

↪ **Определение 1.5.** *Объединение* множеств A и B (обозначается через $A \cup B$ и читается как «объединение A и B ») есть множество всех предметов, которые являются элементами множества A или B , т.е. $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.

Здесь подразумевается не исключающий смысл слова «или».

Таким образом, по определению, $x \in A \cup B$ тогда и только тогда, когда x есть элемент хотя бы одного из множеств A и B .

Например: $\{1, 2, 3\} \cup \{1, 3, 4\} = \{1, 2, 3, 4\}$.

↪ **Определение 1.6.** *Пересечение* множеств A и B (обозначается через $A \cap B$ и читается как «пересечение A и B ») есть множество всех предметов, которые являются элементами обоих множеств A и B , т.е. $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.

Таким образом, по определению, $x \in A \cap B$ тогда и только тогда, когда x является одновременно элементом множества A и элементом множества B .

Например: $\{1, 2, 3\} \cap \{1, 3, 4\} = \{1, 3\}$.

Для всякой пары множеств A и B имеют место следующие включения:

$$\emptyset \subseteq A \cap B \subseteq A \subseteq A \cup B.$$

↪ **Определение 1.7.** Два множества A и B называются *непересекающимися* (или дизъюнктными), если $A \cap B = \emptyset$, и *пересекающимися*, если $A \cap B \neq \emptyset$. Система множеств называется *расчлененной*, если любая пара ее различных элементов является непересекающейся.

↪ **Определение 1.8.** *Разбиением* множества X будем называть такую расчлененную систему U непустых и различных подмножеств множества X , где каждый элемент множества X является в то же время элементом некоторого (следовательно, в точности одного) элемента системы U .

Например, $\{\{1, 2\}, \{3\}, \{4, 5\}\}$ есть разбиение множества $\{1, 2, 3, 4, 5\}$.

↪ **Определение 1.9.** *Абсолютное дополнение* множества A (обозначается через A' или $\neg A$) — это множество всех элементов, не являющихся элементами множества A : $\{x \mid x \notin A\}$.

↪ **Определение 1.10.** *Относительное дополнение* множества B до множества A — это множество $A \cap B'$; оно обычно обозначается через $A \setminus B$ (иногда $A - B$), что читается как « A минус B ».

Таким образом $A \setminus B = A \cap B'$ есть сокращение для $\{x \in A \mid x \notin B\}$, т.е. это множество тех элементов множества A , которые не являются элементами множества B .

↪ **Определение 1.11.** *Симметрическая разность* множеств A и B , обозначаемая через $A \div B$ (иногда используются обозначения $A \Delta B$ или $A + B$), определяется следующим образом: $x \in A \div B$ тогда и только тогда, когда x принадлежит ровно одному из множеств A и B :

$$A \div B = \{x \mid (x \in A \text{ и } x \notin B) \text{ или } (x \notin A \text{ и } x \in B)\}.$$

Из определения следует, что $A \div B = (A \setminus B) \cup (B \setminus A)$.

Нетрудно показать, что эта операция коммутативна: $A \div B = B \div A$, ассоциативна: $(A \div B) \div C = A \div (B \div C)$ и дистрибутивна

относительно пересечения: $(A \div B) \cap C = (A \cap C) \div (B \cap C)$. Кроме того, $A \div A = \emptyset$ и $A \div \emptyset = A$.

Если все рассматриваемые в ходе какого-либо рассуждения множества являются подмножествами некоторого множества U , то это множество U называют *универсальным множеством* (для этого рассуждения). Например, для элементарной арифметики универсальным множеством служит \mathbf{Z} , а для аналитической геометрии плоскости — множество всех упорядоченных пар действительных чисел.

Для графической иллюстрации отношений, которые могут иметь место между подмножествами какого-либо универсального множества U , часто используют так называемые диаграммы Венна — по имени английского священника Джона Венна (1834–1923)¹, применявшего их в своих исследованиях по логике. Диаграмма Венна представляет собой схематическое изображение множеств в виде точечных множеств: универсальное множество U изображается множеством точек некоторого прямоугольника, а его подмножество A — в виде круга или какой-нибудь другой простой области внутри этого прямоугольника. Правильнее, однако, было бы назвать их диаграммами Эйлера, поскольку задолго до Венна их употреблял знаменитый швейцарский математик Леонард Эйлер (1707–1783)². Ниже на рис. 1.1. показаны основные операции над множествами.

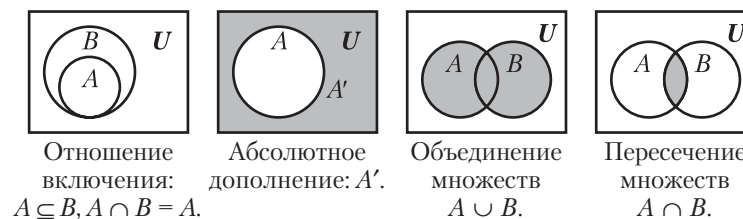


Рис. 1.1. Диаграммы Венна и круги Эйлера.

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

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

1.3. Алгебра множеств

1.3.1. Определение алгебры множеств

↪ **Определение 1.12.** Алгебра — это множество объектов с определенными на нем операциями, отвечающими некоторым свойствам. Обычно *абстрактная алгебра* задается как двойка $A = \langle M, \Sigma \rangle$, где M — множество объектов алгебры (*носитель алгебры*), Σ — множество операций (*сигнатура алгебры*). Множество операций описывается своими свойствами, которые задаются *системой аксиом* данной алгебры.

Мы будем рассматривать алгебру подмножеств некоторого универсального множества U . Для краткости в дальнейшем будем называть ее просто *алгеброй множеств*.

↪ **Определение 1.13.** Определим *алгебру множеств* как четверку: $\langle M, \cup, \cap, ' \rangle$, где M — множество-степень универсального множества U , а множество операций состоит из операций объединения (\cup), пересечения (\cap) и дополнения ($'$) множества до множества U .

В содержательной теории множеств с помощью отношения принадлежности элементов множеству можно доказать следующую теорему.

Теорема 1.1. Для любых подмножеств A, B и C некоторого универсума U следующие равенства являются тождествами:

- 1) $A \cup (B \cap C) = (A \cup B) \cap C$,
 $A \cap (B \cup C) = (A \cap B) \cup C$ (ассоциативность);
- 2) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (коммутативность);
- 3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность);
- 4) $A \cup \emptyset = A$, $A \cap U = A$;
- 5) $A \cup A' = U$, $A \cap A' = \emptyset$.

Из этих тождеств, принятых как аксиомы, может быть выведена любая теорема алгебры множеств без использования понятия принадлежности. Из приведенных выше десяти тождеств видно, что каждое правое тождество получено из левого заменой символа \cup на \cap и наоборот, а также заменой \emptyset на U и наоборот.

↪ **Определение 1.14.** Равенство, полученное из исходного заменой всех символов U на \emptyset , \emptyset на U , \cup на \cap , \cap на \cup , называется *двойственным* исходному.

В приведенном выше списке тождеств 1–5 каждое тождество имеет двойственное ему тождество. Таким образом, мы приходим

к **принципу двойственности**: для любой теоремы алгебры множеств двойственное ей утверждение также является теоремой.

1.3.2. Теоремы алгебры множеств

Теорема 1.2. Для произвольных подмножеств A и B некоторого универсального множества U справедливы следующие утверждения:

- 6) если для всякого A $A \cup B = A$, то $B = \emptyset$,
 если для всякого A $A \cap B = A$, то $B = U$;
- 7) если $A \cup B = U$ и $A \cap B = \emptyset$, то $B = A'$;
- 8) $A'' = A$;
- 9) $\emptyset' = U$, $U' = \emptyset$;
- 10) $A \cup A = A$, $A \cap A = A$ (законы идемпотентности);
- 11) $A \cup U = U$, $A \cap \emptyset = \emptyset$;
- 12) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ (законы поглощения);
- 13) $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$ (законы де Моргана)¹.

Докажем некоторые утверждения, используя только тождества 1–5.

Утверждение 6.

Доказательство. Поскольку по условию $A \cup B = A$ для всех A , то это верно и для $A = \emptyset$, т.е. $\emptyset \cup B = \emptyset$. Тогда из 2) следует: $\emptyset \cup B = B \cup \emptyset$, т.е. $B \cup \emptyset = \emptyset$. С другой стороны, согласно 4), $B \cup \emptyset = B$. Отсюда следует, что $B = \emptyset$. ∞

Утверждение 7.

Доказательство (в скобках указаны номера применяемых аксиом и утверждений).

$B = (4) = B \cup \emptyset = (5) = B \cup (A \cap A') = (3) = (B \cup A) \cap (B \cup A') =$
 $= (2) = (A \cup B) \cap (B \cup A') = (\text{по усл.}) = U \cap (B \cup A') = (5) =$
 $= (A \cup A') \cap (B \cup A') = (2) = (A' \cup A) \cap (A' \cup B) = (3) =$
 $= A' \cup (A \cap B) = (\text{по усл.}) = A' \cup \emptyset = (4) = A'$. ∞

Доказательство **утверждения 8** следует из утверждения 7: аксиомы 5 можно переписать в виде: $A' \cup A = U$, $A \cap A' = \emptyset$ в силу коммутативности операций \cup и \cap (аксиомы 2). Тогда, по утверждению 7, $A = A''$.

Доказательство остальных утверждений предлагается читателю провести самостоятельно.

¹ **Огастес де Морган (De Morgan)** (1806–1871) — шотландский математик и логик. Занимался алгеброй, теорией рядов. Независимо от Дж. Буля пришел к основным идеям математической логики.

1.4. Парадокс Бертрانا Рассела

Неограниченное применение принципа абстракции вызывает возникновение парадоксов в канторовской теории множеств. В 1902 г. Бертран Рассел¹ открыл парадокс, основанный на одном лишь определении множества.

Множества либо являются элементами самих себя, либо не являются. Так, множество абстрактных понятий само является абстрактным понятием, а множество всех звезд на небе не является звездой. Множество звуков также является звуком. Аналогично, множество всех множеств само есть множество.

Рассмотрим M — множество всех множеств, являющихся элементами самих себя, и N — множество всех множеств, не являющихся элементами самих себя. К какому же из этих двух множеств отнести множество N ? Иными словами, является ли N элементом самого себя? Если N является элементом себя, т. е. $N \in N$, значит N является элементом M , т. е. $N \in M$, но тогда, по определению множества M , $N \notin N$, т. е. N не является элементом самого себя. Получили противоречие. С другой стороны, если N не является элементом самого себя, то N есть элемент N , а не M , и N является элементом самого себя, что опять является противоречием.

Парадокс Бертрانا Рассела известен в популярной форме как парадокс брадоброя (парикмахера). В одной деревне брадобрей обязуется брить всех тех и только тех жителей, которые не бреются сами. Как быть самому брадобрю: должен ли он брить самого себя? Очевидно, что любой ответ приводит к противоречию.

Поскольку большинство разделов математики использует теоретико-множественные понятия и сама теория множеств может считаться основой этих разделов, то обнаруженные парадоксы в начале 20-го века поставили под сомнение достоверность всей математической науки в целом. Выходом из создавшегося положения была аксиоматизация теории множеств. Один из вариантов такой аксиоматизации, система аксиом Цермело–Френкеля, будет приведен в главе 4.

¹ **Бертран Рассел (Russel)** (1872–1970) — выдающийся английский математик и философ, логик, общественный деятель. Основоположник английского неореализма и неопозитивизма. Один из классиков математической логики, лауреат Нобелевской премии по литературе (1950). (На русский язык переведена «История западной философии» Б. Рассела и некоторые другие его философские и литературно-философские произведения, а также научно-фантастические рассказы). Опубликованные в 1910–1913 гг. двухтомные «Основания математики» Бертрانا Рассела и Альфреда Норта Уайтхеда (1861–1947) содержат одну из наиболее известных и продуманных систем логического обоснования математики, оказавшую большое влияние на Д. Гильберта (1862–1947).

Глава 2.

ТЕОРИЯ ОТНОШЕНИЙ

2.1. Основные понятия

Для обозначения какой-либо связи между объектами или понятиями в математике часто пользуются понятием «отношение». Например, свойство элемента принадлежать или не принадлежать множеству является отношением « $x \in X$ », причем, если элемент принадлежит множеству, то отношение выполнено, а если не принадлежит, то не выполнено. Включение множества в другое множество « $X \subseteq Y$ » также является отношением. На множестве людей задано отношение родства, например, « x — отец y ». Если взять конкретных людей и подставить их имена вместо x и y , то мы получим истинное или ложное высказывание, например: «Лайй — отец Эдипа» — истинное высказывание, «Полиб — отец Эдипа»¹ — ложное. В этом смысле отношение также является предикатом, который обращается в истинное или ложное высказывание при подстановке в него конкретных элементов из области определения.

Рассмотрим еще одну операцию над множествами.

➤ **Определение 2.1.** *Декартовым произведением множеств X и Y называется множество всех упорядоченных пар $\langle x, y \rangle$, таких, что $x \in X$ и $y \in Y$.*

Это обозначается как $X \times Y = \{\langle x, y \rangle \mid x \in X, y \in Y\}$.

Упорядоченная пара элементов $\langle x, y \rangle$ однозначно определяется через x и y . Кроме того, если $\langle x, y \rangle = \langle u, v \rangle$, то $x = u$ и $y = v$. Принято называть x *первой*, а y — *второй координатой* упорядоченной пары $\langle x, y \rangle$.

✱ **Пример.** Пусть даны множества $X = \{1, 2\}$ и $Y = \{2, 3, 4\}$. Декартово произведение этих двух множеств: $X \times Y = \{\langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 1, 4 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle, \langle 2, 4 \rangle\}$. Рассмотрим подмножество этого декартового произведения $A = \{\langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 1, 4 \rangle, \langle 2, 3 \rangle, \langle 2, 4 \rangle\}$. Это не что иное, как отношение $\rho_1: x < y$ — « x меньше y ». На том же множестве упорядоченных пар можно выделить еще одно отношение $\rho_2: y = x + 1$ — это подмножество $\{\langle 1, 2 \rangle, \langle 2, 3 \rangle\}$. Другое отношение $\rho_3: x = y$ — это подмножество $\{\langle 2, 2 \rangle\}$. Множество упорядоченных пар образует *бинарное отношение*.

➤ **Определение 2.2.** *Бинарное отношение есть подмножество декартового произведения двух множеств.*

¹ **Эдип, Полиб и Лайй** — герои трагедии Софокла «Царь Эдип». Эдип был не родным сыном Полиба и потому второе высказывание ложно. Родным же отцом Эдипа был Лайй, и потому первое высказывание истинно.

Бинарное отношение обозначается так: $\langle x, y \rangle \in \rho$ или $x\rho y$. Эти выражения эквивалентны и читаются как « x находится в отношении ρ к y ».

Естественным обобщением понятия *бинарного* отношения является понятие *n -арного* (n -местного) отношения, определяемого как подмножество декартова произведения n множеств:

$$X_1 \times X_2 \times \dots \times X_n = \{\langle x_1^i, x_2^i, \dots, x_n^i \rangle \mid x_1^i \in X_1, x_2^i \in X_2, \dots, x_n^i \in X_n\}.$$

n -арное отношение представляет собой множество упорядоченных n -ок (читается: «энка»). Упорядоченную n -ку называют иначе *кортежем*. Подмножество кортежей из n элементов образует *n -арное отношение*. При $n = 2$ имеет место бинарное отношение, при $n = 3$ используется термин *тернарное* отношение.

* Примеры.

1. Для некоторых отношений приняты специальные обозначения:

равенство: $x = y$;

тождество: $x \equiv y$;

неравенства: $x \geq y, x \leq y, x < y, x > y$;

принадлежность: $x \in Y, x \notin Y$;

включение: $X \subseteq Y, X \subset Y$;

конгруэнтность: $x \cong y$.

2. Множество $\{\langle 2, 4 \rangle, \langle 7, 3 \rangle, \langle 3, 3 \rangle, \langle 2, 1 \rangle\}$, будучи множеством упорядоченных пар, есть бинарное отношение. Не имея никакого конкретного значения, это отношение, естественно, не имеет и специального названия.

3. Если m обозначает отношение материнства, то $\langle \text{Джейн}, \text{Джон} \rangle \in m$ означает, что Джейн является матерью Джона.

4. « x и y — родители z » — тернарное отношение.

5. Примером n -арного отношения, где $n = 4$, может служить таблица:

	Фамилия	Год рожд.	Место жительства	Образование
1	Иванов	1958	Киев	высшее
2

↪ **Определение 2.3.** Областью определения бинарного отношения ρ (обозначение: D_ρ) называют множество первых координат элементов из ρ , областью значений отношения ρ (обозначение: R_ρ) — множество вторых координат элементов из ρ .

Например, как областью определения, так и областью значений отношения включения для подмножеств множества U является множество $\wp(U)$; областью определения для отношения материнства служит множество всех матерей, в то время, как область значений этого отношения — множество всех людей.

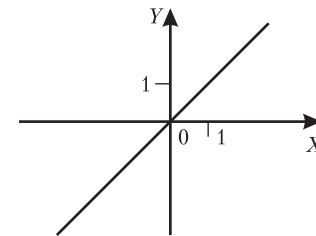
2.2. Способы задания отношений

2.2.1. График отношения

Аналитическая геометрия плоскости основывается на допущении о том, что между точками евклидовой плоскости и декартовым произведением $\mathbf{R} \times \mathbf{R}$ существует взаимно однозначное соответствие. Каждой точке на плоскости соответствуют ее координаты — упорядоченная пара $\langle x, y \rangle$. Поэтому отношение на множестве \mathbf{R} можно изображать на плоскости некоторой конфигурацией или множеством точек. Например, отношение равенства можно изобразить в виде прямой $y = x$ в декартовой системе координат.

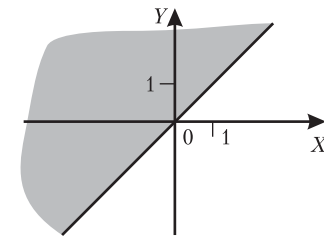
↪ **Определение 2.4.** Если основным предметом изучения служат отношения на множестве действительных чисел \mathbf{R} , то множество точек, соответствующих элементам отношения, называют *графиком* этого отношения.

Ниже на рис. 2.1—2.4 приводятся четыре примера отношений, для каждого из которых схематически представлен его график. В тех случаях, когда график является частью плоскости, эта часть плоскости на чертеже заштриховывается.



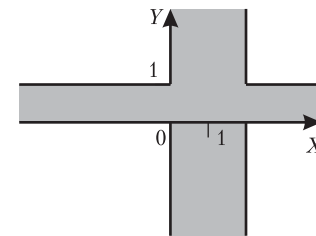
$$\{\langle x, y \rangle \in \mathbf{R} \times \mathbf{R} \mid y = x\}$$

Рис. 2.1.



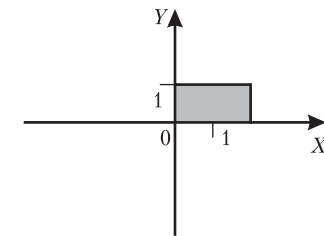
$$\{\langle x, y \rangle \in \mathbf{R} \times \mathbf{R} \mid y \geq x\}$$

Рис. 2.2.



$$\{\langle x, y \rangle \in \mathbf{R} \times \mathbf{R} \mid 0 \leq x \leq 2 \text{ или } 0 \leq y \leq 1\}$$

Рис. 2.3.



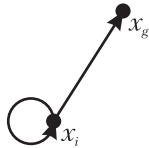
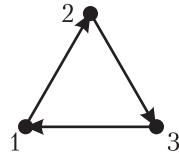
$$\{\langle x, y \rangle \in \mathbf{R} \times \mathbf{R} \mid 0 \leq x \leq 2 \text{ и } 0 \leq y \leq 1\}$$

Рис. 2.4.

2.2.2. Графический способ задания множества

Если задано отношение $xру, x \in X, y \in Y$, то элементы множеств X и Y можно изображать точками на плоскости, а упорядоченную пару — линией со стрелкой (дугой), направленной от x к y : $x \rightarrow y$. Тогда отношение на конечном множестве элементов может быть представлено в виде *графа*.

Например, отношение $\rho_1 = \{ \langle x_i, x_i \rangle, \langle x_i, x_g \rangle \}$ может быть представлено в виде графа, изображенного на рис. 2.5. Отношение $\rho_2 = \{ \langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle \}$ может быть представлено в виде ориентированного графа (см. рис. 2.6).

Рис. 2.5. Граф отношения ρ_1 .Рис. 2.6. Граф отношения ρ_2 .

2.2.3. Матричный способ задания отношений

Зададим отношение ρ : « x дружит с y » на множестве M , где $M = \{a_1, a_2, a_3, a_4\}$ — множество персонажей. Это отношение можно представить в виде таблицы (матрицы), элементы которой равны единице, если между соответствующими элементами есть отношение дружбы, и нулю в противном случае.

	a_1	a_2	a_3	a_4
a_1	1	0	1	0
a_2	0	1	0	0
a_3	1	0	1	1
a_4	0	0	1	1

Из этой таблицы видно, что a_1 дружит с a_3 , a_2 не дружит ни с кем, кроме как с самим собой, а a_3 дружит со всеми, кроме a_2 . Такой способ задания отношений называется матричным способом. В этом случае отношение $\rho \in X \times Y$ представляется в

виде матрицы $A = \| a_{ig} \|$ с элементами a_{ig} , где i — номер строки, g — номер столбца; $a_{ig} = 1$, если элементы x_i и y_g находятся в отношении ρ , и $a_{ig} = 0$ в противном случае.

Если $\| a_{ig} \| = 0$, т.е. для всех i и g $a_{ig} = 0$, то $\rho \equiv 0$ — пустое отношение; если $\| a_{ig} \| = 1$, т.е. для всех i и g $a_{ig} = 1$, то $\rho \equiv 1$ — полное отношение.

2.3. Операции над отношениями

Так как каждое отношение есть множество, то над отношениями можно выполнять все операции, определенные для множеств. В результате формируются новые, более сложные отношения.

2.3.1. Теоретико-множественные операции

→ **Определение 2.5.** Пересечением отношений α и β называется отношение, определяемое пересечением соответствующих множеств.

* **Пример.** Пусть α : « $x \geq y$ », β : « $x > y$ ». Тогда пересечение $\alpha \cap \beta$ есть отношение « $x > y$ ».

→ **Определение 2.6.** Объединением отношений α и β образуется объединением соответствующих множеств.

Пример. Пусть α : « $x > y$ », β : « $x = y$ », тогда их объединение есть отношение $\alpha \cup \beta$: « $x \geq y$ ».

→ **Определение 2.7.** Включение отношений: α включено в β , если множество всех пар $\langle x, y \rangle \in \alpha$ содержится и в отношении β , т.е. $\alpha \subseteq \beta$, если для каждого $\langle x, y \rangle \in \alpha$, $\langle x, y \rangle \in \beta$.

→ **Определение 2.8.** Если α — отношение, заданное на M , то обратное отношение α^{-1} определяется как $x\alpha^{-1}y = y\alpha x$.

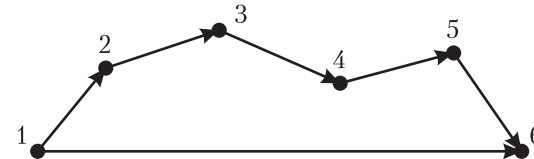
Например, если α : « $x > y$ », где $x, y \in \mathbf{R}$, то обратное ему отношение α^{-1} : « $y > x$ », или « $x < y$ ». Если α : « x сестра y », где $x \in \{\text{женщины}\}$, $y \in \{\text{мужчины}\}$, то обратное отношение α^{-1} — « y сестра x ».

→ **Определение 2.9.** Дополнением бинарного отношения ρ между элементами $x \in A$ и $y \in B$, считается множество $\rho' = (A \times B) \setminus \rho$, которое тоже является отношением.

→ **Определение 2.10.** Отношения α и β могут образовывать произведение отношений $\alpha\beta$, которое само является отношением, т.е. $x\alpha\beta y$, $x, y \in M$, если существует такой элемент $z \in M$, что $x\alpha z$ и $z\beta y$.

Например, пусть α : « x — мать y », β : « x отец y ». Тогда существует такое b , что $a\alpha b$ и $b\beta c$, т.е. « a — мать b » и « b — отец c ». Тогда произведение этих отношений: « a — бабушка c ».

→ **Определение 2.11.** Отношение α , называется транзитивным замыканием отношения α , определенного на множестве M , тогда и только тогда, когда существуют такие $a\alpha_1 b$, что $a\alpha z_1$, $z_1\alpha z_2$, $z_2\alpha z_3$, ..., $z_{n-1}\alpha b$.

Рис. 2.7. Транзитивное замыкание отношения $x < y$.

✱ **Примеры.**

- На множестве N определено отношение α : $x < y$. Тогда транзитивным замыканием этого отношения для значений $1 < 2 < \dots < 6$ будет отношение $1 < 6$ (см. рис. 2.7).
- Транзитивным замыканием отношения «быть сыном» является отношение «быть прямым потомком».
- Транзитивным замыканием отношения «иметь общую стену» для жильцов одного дома является отношение «жить на одном этаже».

2.3.2. Основные свойства отношений

Будем рассматривать отношения, заданные на множестве X , т.е. $x, y, u \in X$.

↪ **Определение 2.12.** Отношение ρ на множестве X называется *рефлексивным*, если для любых $x \in X$ выполняется $x\rho x$. Если для всех $x \in X$ не выполняется $x\rho x$, то отношение называется *антирефлексивным*.

✱ **Примеры.** Отношение равенства рефлексивно. Отношение $x \geq y$, $x, y \in R$ рефлексивно, так как $x \geq x$. Отношение $x > y$, $x, y \in R$ антирефлексивно, так как ни для одного числа не выполнимо $x > x$.

↪ **Определение 2.13.** Отношение ρ на множестве X называется *симметричным*, если для любых $x \in X, y \in X$, из $x\rho y$ следует $y\rho x$.

Иными словами, отношение симметрично, если всякий раз, как выполняется $x\rho y$, выполняется и $y\rho x$.

✱ **Примеры.** Из того, что « x родственник y », следует, что « y родственник x », — отношение симметрично. Отношение « x — сестра y », определенное на множестве всех людей, несимметрично: возможно, что y является братом x . Однако то же отношение, определенное на множестве женщин, является симметричным.

↪ **Определение 2.14.** Отношение ρ на множестве X называется *антисимметричным*, если для любых $x, y \in X$, из того, что $x\rho y$ и $y\rho x$, следует $x = y$.

✱ **Примеры.** Отношение $x \leq y$ антисимметрично: из того, что $x \leq y$ и $y \leq x$, следует, что $x = y$, т.е. это один и тот же элемент.

Если для любых $x, y \in X$ из того, что $x\rho y$, следует, что не выполняется $y\rho x$, то отношение называется *асимметричным*.

Отношения « x предок y » и « y потомок x » асимметричны, причем второе является обратным к первому. Отношение строгого порядка $x < y$ является асимметричным: если выполняется $x < y$, то не выполняется $y < x$.

↪ **Определение 2.15.** Отношение ρ называется *транзитивным*, если из того, что $x\rho y$ и $y\rho z$, следует $x\rho z$.

✱ **Пример.** Отношение « x предок y » транзитивно: если « x предок y » и « y предок z », то « x предок z ». Отношение $x < y$, где $x, y \in R$, транзитивно: если $x < y$ и $y < z$, то $x < z$. Отношение « x любит y », в общем случае нетранзитивно: если « x любит y », а « y любит z », то из этого не следует, что « x любит z ».

2.4. Отношение эквивалентности

↪ **Определение 2.16.** Отношение, которое обладает свойствами рефлексивности, симметричности и транзитивности, называется отношением *эквивалентности*.

✱ **Примеры отношений эквивалентности.**

1. Отношение равенства на любом множестве является отношением эквивалентности, причем отношение равенства является в некотором смысле минимальным (предельным) случаем отношения эквивалентности.
2. Геометрическое отношение подобия треугольников на плоскости является отношением эквивалентности.
3. Отношения сравнимости по модулю n в Z : x сравнимо с y по модулю n , если разность $x - y$ делится на n (без остатка). Обозначается: $x \equiv y \pmod{n}$. Например: $3 \equiv 6 \pmod{3}$, $7 \equiv 13 \pmod{3}$.
4. Отношение параллельности прямых в евклидовом пространстве есть отношение эквивалентности.
5. Утверждения вида $\sin^2 x + \cos^2 x = 1$, $(a + b)(a - b) = a^2 - b^2$, состоящие их формул, соединенных знаком равенства, задают бинарное отношение на множестве формул, описывающих суперпозиции элементарных функций. Это отношение равносильности также является отношением эквивалентности: формулы равносильны, если они задают одну и ту же функцию.
6. Отношение «студенты x и y учатся в одной группе», где $x, y \in \{\text{«студенты первого курса»}\}$, есть отношение эквивалентности.
7. Отношение «жить в одном районе», определенное на множестве людей, живущих в г. Киеве, является отношением эквивалентности.

Множество всех жителей Киева разбивается последним отношением эквивалентности на ряд непересекающихся подмножеств, в данном случае на множества людей, живущих в одном и том же районе. Два жителя считаются эквивалентными по данному отношению, если они живут в одном и том же районе, и в этом смысле они неразличимы, т.е. они обладают одним и тем же свойством: «жить в районе «XXX». Это свойство является определяющим свойством (предикатом) множества всех жителей района «XXX». С другой стороны, нельзя жить в двух (и более) районах сразу (во всяком случае, согласно прописке), поэтому множества жителей различных районов не пересекаются. Таким образом, отношение

«жить в одном районе» разбивает все множество жителей города на ряд непересекающихся подмножеств, таких, что внутри каждого подмножества все жители эквивалентны по данному отношению, и никакие два жителя разных подмножеств не находятся в отношении эквивалентности друг с другом. Такие подмножества называются *классами эквивалентности*.

Дадим более строгое определение.

↪ **Определение 2.17.** Пусть на множестве X задано отношение эквивалентности ρ . Тогда подмножество $A \subseteq X$ называется *классом эквивалентности по отношению ρ* , если A состоит из всех тех элементов $x \in X$, что для некоторого $a \in X, a \in A$ и $x \rho a$.

Можно построить классы эквивалентности следующим образом. Выберем элемент a_1 , принадлежащий X , и образуем подмножество $A_1 \subseteq X$ из a_1 и всех элементов, эквивалентных a_1 . Это будет класс эквивалентности A_1 . Далее выберем элемент $a_2 \in X, a_2 \notin A_1$, и образуем класс A_2 , состоящий из всех элементов, эквивалентных a_2 , и т. д. Получим систему классов A_1, A_2, \dots , такую, что любой элемент $a_i \in X$ входит только в один класс, объединение всех классов $A_1 \cup A_2 \cup \dots$ образует множество X , и для любых i, j $A_i \cap A_j = \emptyset$, т.е. *множество классов эквивалентности образует разбиение множества X* .

Полученная система классов эквивалентности обладает следующими свойствами.

Теорема 2.1.

1. Пусть ρ есть отношение эквивалентности на X . Тогда множество классов эквивалентности по отношению ρ есть разбиение множества X . Обратно, если есть некоторое разбиение \mathfrak{R} множества X , а отношение ρ таково, что $a \rho b$ тогда и только тогда, когда $a \in A, b \in A, A \in \mathfrak{R}$, то ρ есть отношение эквивалентности на X .

2. Если отношение эквивалентности ρ определяет разбиение \mathfrak{R} множества X , то отношение эквивалентности, определяемое этим разбиением \mathfrak{R} , совпадает с ρ . Обратно, если некоторое разбиение \mathfrak{B} множества X определяет некоторое отношение эквивалентности ρ , то разбиение \mathfrak{R} множества X , определяемое этим отношением ρ , совпадает с \mathfrak{B} .

Доказательство. Доказательство первой части теоремы следует из свойств отношения эквивалентности. Каждый элемент X войдет хотя бы в один класс эквивалентности. Предположим, что некоторый элемент b входит одновременно в два класса эквивалентности A_i и A_j . Тогда существует $a_i \in A_i$ такое, что $a_i \rho b$, и существует $a_j \in A_j$ такое, что $b \rho a_j$. Но тогда, в силу свойства транзитивности, $a_i \rho a_j$ и, следовательно, классы A_i и A_j есть один и тот же класс.

Пусть теперь \mathfrak{R} есть разбиение множества X . Отношение ρ симметрично по определению. Если $a \in X$, то в \mathfrak{R} найдется такое множество A , что $a \in A$, так что ρ рефлексивно. Покажем, что оно транзитивно. Пусть $a \rho b$ и $b \rho c$. Тогда в \mathfrak{R} найдется такое A , что $a, b \in A$, и такое B , что $b, c \in B$. Поскольку $b \in B$ и $b \in A$, то $A = B$. Следовательно $a \rho c$. \bowtie

На основании этой теоремы можно дать конструктивное определение отношения эквивалентности: отношение ρ на множестве X называется эквивалентностью, если существует разбиение X на подмножества $\{A_1, A_2, \dots, A_n\}$ такое, что отношение $x \rho y$ выполняется тогда и только тогда, если x и y принадлежат одному и тому же подмножеству.

Будем обозначать класс эквивалентности, порожденный элементом $a \in X$ через $[a]$. Тогда, если $a \rho b$, то $[a] = [b]$.

↪ **Определение 2.18.** Множество классов эквивалентности множества X по отношению ρ называется *фактор-множеством множества X по отношению ρ* и обозначается $[X/\rho]$.

* Примеры.

1. Все классы эквивалентности по отношению равенства состоят из одного элемента. Фактор-множество по отношению равенства состоит из элементов самого множества.

2. Свойство параллельности прямых на плоскости определяет отношение эквивалентности. Фактор-множество этого отношения – множество всех направлений на плоскости. Оно может быть описано, как множество всех углов наклона прямой к оси абсцисс, т.е. интервал $[0^\circ, 180^\circ)$.

3. Пусть $x, y \in \mathbf{Z}$. Рассмотрим отношение сравнимости по модулю 3: $x \rho y$ есть $x \equiv y \pmod{3}$. Запись $x \equiv y \pmod{3}$ означает, что разность $x - y$ делится на 3 без остатка. Будем обозначать это так: $x \rho y$ есть $(x - y)/3 = k \in \mathbf{Z}$. Докажем, что $x \equiv y \pmod{3}$ – отношение эквивалентности.

3.1. Проверим выполнение свойства рефлексивности: для всякого x $x \rho x$. Действительно, $(x - x)/3 = 0/3 = 0$; $0 \in \mathbf{Z}$, следовательно, отношение рефлексивно.

3.2. Проверим выполнение свойства симметричности: если $x \rho y$, то $y \rho x$. Пусть $(x - y)/3 = k \in \mathbf{Z}$. Тогда $(y - x)/3 = -(x - y)/3 = -k \in \mathbf{Z}$. Следовательно, условие симметричности выполняется.

3.3. Проверим выполнение свойства транзитивности: из $x \rho y$ и $y \rho z$ следует $x \rho z$. Пусть $(x - y)/3 = k_1 \in \mathbf{Z}$, т.е. $x - y = 3k_1$, и $(y - z)/3 = k_2 \in \mathbf{Z}$, т.е. $y - z = 3k_2$. Решим эту систему уравнений, сложив их: $x - y + y - z = 3(k_1 + k_2)$, т.е. $x - z = 3(k_1 + k_2) = k_3 \in \mathbf{Z}$. Условие транзитивности выполняется.

Следовательно, отношение $x \equiv y \pmod{3}$ является отношением эквивалентности. Найдем его фактор-множество $[\mathbf{Z}/\rho]$. Произвольное число $x \in \mathbf{Z}$ можно записать в виде $3q + r$, где $q, r \in \mathbf{Z}$, $0 \leq r < 3$. В один и тот же класс эквивалентности попадут все числа, дающие при делении на 3 одинаковое число r в остатке. Мы получим три класса эквивалентности: $[0] = \{0, 3, 6, 9, 12, \dots\}$; $[1] = \{1, 4, 7, 10, 13, \dots\}$; $[2] = \{2, 5, 8, 11, 14, \dots\}$. В класс $[0]$ попадают все числа, которые делятся на 3 без остатка, в класс $[1]$ — все числа, при делении на 3 дающие в остатке 1, и в класс $[2]$ — все числа, дающие в остатке 2. Каждый класс можно охарактеризовать одним представителем этого класса, и в данном случае таким представителем удобнее всего выбрать остаток r . Следовательно, фактор-множеством \mathbf{Z} по отношению $x \equiv y \pmod{3}$ будет $[\mathbf{Z}/x \equiv y \pmod{3}] = \{[0], [1], [2]\}$.

Глава 3.

ОТОБРАЖЕНИЯ. ФУНКЦИИ

3.1. Основные понятия

В предыдущей главе мы рассмотрели бинарные отношения, которые являются подмножествами декартова произведения двух множеств. Бинарные отношения, определенные на декартовом квадрате множества, представляют наибольший интерес, так как они обладают рядом свойств, которые позволяют выделять такие полезные отношения, как отношения равенства, эквивалентности, порядка. Для отношений, образованных различными множествами, когда $\rho \subseteq E \times F$, говорить о рефлексивности, симметричности и транзитивности уже не имеет смысла, так как первая и вторая координата ρ могут иметь различную природу. Например, отношение « x родился в году y » является подмножеством декартова произведения множества людей и множества лет (подмножества целых положительных чисел) и ставит в соответствие каждому человеку год его рождения. Для исследования подобных отношений вводятся понятия *соответствия*, *отображения*, *функции*.

↪ **Определение 3.1.** Говорят, что между множествами E и F определено *соответствие* Γ , если задано некоторое произвольное подмножество декартового произведения $E \times F$. Множество E называется *областью определения*, F — *областью значений* соответствия Γ .

Соответствие, обратное Γ , обозначим Γ^{-1} , где F — область определения, E — область значений Γ^{-1} .

↪ **Определение 3.2.** *Отображением* множества E на множество F называется такое соответствие, которое каждому элементу $x \in E$ сопоставляет по крайней мере один элемент $y \in F$. Тогда элемент y называется *образом* элемента x , а x — *прообразом* элемента y , или *переменной*, или *аргументом*. Отображение E в F будем обозначать $f: E \rightarrow F$, где f — имя отображения.

✱ **Пример.** На рис. 3.1 показано соответствие между множествами E и F , на рис. 3.2 — отображение множества E в множество F .

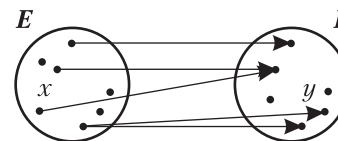


Рис. 3.1. Соответствие.

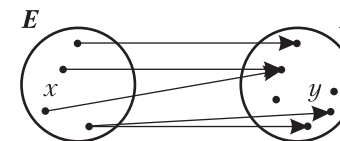


Рис. 3.2. Отображение.

3.1.1. Сюръекция

↪ **Определение 3.3.** Отображение E на F называется *сюръективным*, или *сюръекцией*, или *наложением*, если каждый элемент $y \in F$ есть образ по крайней мере одного элемента $x \in E$, т.е. $\forall y \in F \exists x \in E (y = \Gamma(x))$.

Условие $\forall y \in F |\Gamma^{-1}(y)| \geq 1$ характеризует сюръекцию. Это означает, что каждый элемент из F имеет не менее одного прообраза в E . На графе соответствия в каждый элемент y входит по крайней мере одна дуга (рис. 3.3) и обратное отображение $\Gamma^{-1}(y)$ не пусто.

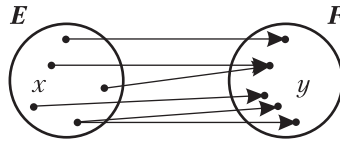


Рис. 3.3. Сюръекция.

3.1.2. Инъекция

↪ **Определение 3.4.** Отображение E в F называется *инъективным*, или *инъекцией*, или *вложением*, если каждый элемент $y \in F$ есть образ только одного элемента $x \in E$, либо вообще не имеет прообраза.

В этом случае E инъективно отображается в F . На графе соответствия в каждый элемент y входит самое большее одна дуга, т.е. условие $\forall y \in F |\Gamma^{-1}(y)| \leq 1$ характеризует инъекцию. На рис. 3.4. показана инъекция: в каждый элемент y входит самое большее одна дуга; некоторые элементы y не имеют прообразов в E .

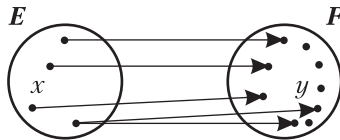


Рис. 3.4. Инъекция.

3.1.3. Биекция

↪ **Определение 3.5.** Если отображение является одновременно и сюръекцией, и инъекцией, то оно называется *биективным отображением*, или *биекцией*.

В этом случае каждый элемент F является образом некоторого, и притом единственного, элемента из E . На графе соответствия на рис. 3.5 показана биекция: в каждый элемент y входит одна и только

одна дуга, т.е. при биекции каждый образ имеет только один прообраз: $\forall y \in F |\Gamma^{-1}(y)| = 1$.

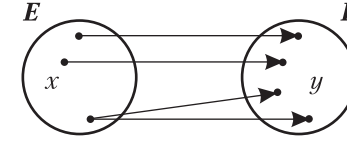


Рис. 3.5. Биекция.

3.1.4. Функциональные отображения

↪ **Определение 3.6.** Соответствие, при котором каждому $x \in E$ сопоставляется один и только один элемент $y \in F$, называется *функциональным соответствием*, или *функцией*.

Для функционального отображения выполняется условие: $\forall x \in E |\Gamma(x)| = 1$. Иными словами, функция — это соответствие или отображение, при котором два различных элемента не имеют одинаковых первых координат, т.е. если $\langle x, y \rangle, \langle x, z \rangle \in \Gamma$, то $y = z$. Если функциональное соответствие не является отображением, т.е. в E существуют элементы, не имеющие образа в F , то оно называется *частично определенной функцией*. Функциональное отображение является полностью определенной функцией, или просто *функцией*.

В дальнейшем мы будем рассматривать только функциональные отображения и обозначать их функциональными символами f, φ и т.п. Функция может быть биективной, сюръективной и инъективной, как показано на рис. 3.6, 3.7, 3.8.

Функциональная биекция $E \rightarrow F$ устанавливает такое отображение, при котором каждый элемент из E имеет единственный образ в F , а каждый элемент из F имеет единственный прообраз в E , поэтому функциональная биекция называется *взаимно однозначным соответствием*. Функциональное отображение $E \rightarrow F$, которое является сюръекцией, возможно только в том случае, если количество элементов в E не меньше количества элементов в F , т.е. $|E| \geq |F|$. Для функциональной инъекции, наоборот, должно выполняться соотношение $|E| \leq |F|$.

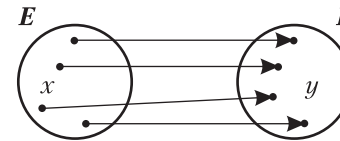


Рис. 3.6. Функциональная биекция.

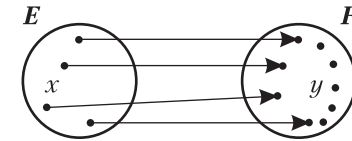


Рис. 3.7. Функциональная инъекция.

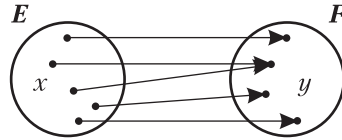


Рис. 3.8. Функциональная сюръекция.

↪ **Определение 3.7.** Отображение множества E в E , определенное равенством $f(x) = x$, называется *тождественным* отображением (оператором).

↪ **Определение 3.8.** Отображение множества в его фактор-множество называется *канонической сюръекцией*.

✱ **Примеры** отображений.

1. Пусть задано соответствие $f: \mathbf{R} \rightarrow \mathbf{R}$, такое, что $f(x) = x^2$. Это соответствие является отображением, так как для каждого $x \in \mathbf{R}$ существует образ $f(x) = x^2$. Область определения этого отображения — множество всех действительных чисел \mathbf{R} ; область значений — $\text{Im}(\mathbf{R}) = [0, \infty)$. Отображение f функционально, так как каждое значение $x \in \mathbf{R}$ имеет только один образ в \mathbf{R} . Отображение $f: \mathbf{R} \rightarrow [0, \infty)$ является функциональной сюръекцией, так как для каждого $f(x) \in [0, \infty)$ существует по крайней мере один прообраз $x \in \mathbf{R}$.

2. Если E — множество ограниченных кривых на плоскости, то функция вычисления длины кривой есть сюръекция $f: E \rightarrow \mathbf{R}^+$.

3. Отображение $f: \mathbf{R} \rightarrow \mathbf{R}$, такое, что $f(x) = 2x+3$, т.е. прямая, есть биекция.

4. Отображение $g: \mathbf{N} \rightarrow \mathbf{R}$, такое, что $g(x) = \pm\sqrt{x}$, является биекцией, но не является функциональным отображением.

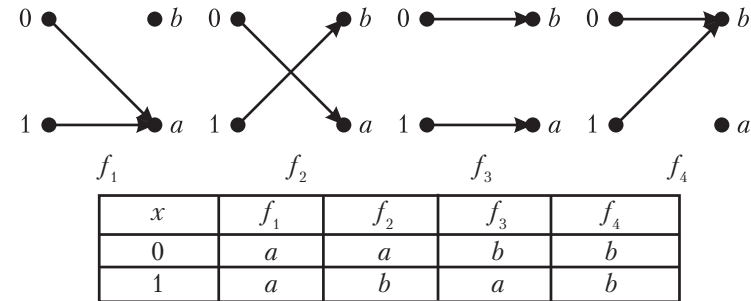
5. Соответствие $f: \mathbf{R} \rightarrow \mathbf{R}$, такое, что $f(x) = x/\sin x$, является частично определенной функцией: для $\sin x = 0$ значение функции не определено.

6. Индексирование элементов некоторого множества есть однозначное отображение этого множества в подмножество натуральных чисел \mathbf{N} .

3.2. Кардинальная степень множеств

Если E и F — два множества, то можно говорить о некотором новом множестве — множестве функциональных отображений E в F .

✱ **Пример.** На рис. 3.9 показано множество всех функциональных отображений из $E = \{0, 1\}$ в $F = \{a, b\}$. Это же множество задано в таблице — это множество всех одноместных функций, определенных на E со значениями в F .

Рис. 3.9. Множество отображений $E = \{0, 1\}$ в $F = \{a, b\}$.

Из таблицы видно, что множество всех функций из $E = \{0, 1\}$ в $F = \{a, b\}$ можно биективно отобразить на декартово произведение $F \times F$, так как каждой функции можно поставить в соответствие упорядоченную пару из $F \times F$. В данном примере такой биекцией будет: $f_1 \Leftrightarrow \langle a, a \rangle$, $f_2 \Leftrightarrow \langle a, b \rangle$, $f_3 \Leftrightarrow \langle b, a \rangle$, $f_4 \Leftrightarrow \langle b, b \rangle$.

Если E состоит из n элементов x_1, x_2, \dots, x_n , то множество (одноместных) функций из E в F можно биективно отобразить на F^n , так как каждое такое отображение эквивалентно заданию кортежа $\langle y_1, y_2, \dots, y_n \rangle \in F^n$ образов элементов x_1, x_2, \dots, x_n при этом отображении. Поэтому количество функциональных отображений определяется количеством элементов в декартовом произведении F^n , где n — количество элементов множества E . В нашем примере для $f: \{0, 1\} \rightarrow \{a, b\}$ количество функций $|f| = 2^2 = 4$. Если $|E| = 3$, $|F| = 2$, то $|f| = 2^3$. В общем случае $|f| = |F|^{|E|}$.

Это дает основание обозначать множество всех функциональных отображений $\{f: E \rightarrow F\}$ в виде степени F^E . Таким образом, мы определили еще одну операцию над множествами — это возведение множества в степень другого множества: F^E . Результатом ее является множество всех функциональных отображений $E \rightarrow F$, т.е. множество всех одноместных функций, определенных на E со значениями в F . В отличие от декартовой степени множества, степень множества F^E как множество всех функциональных отображений $E \rightarrow F$ называют *кардинальной степенью*.

↪ **Определение 3.9.** Множество всех функциональных отображений $\{f: E \rightarrow F\}$ называется (*кардинальной*) *степенью* множеств и обозначается F^E .

Отображение множества E^n в F , где $n \in \mathbf{N}$, E^n — декартова степень множества E , образует функцию от n переменных. Множество всех n -местных функций есть множество всех (функциональных)

отображений $f: E^n \rightarrow F$, т.е. степень множества F^{E^n} . Количество таких функций определяется как $|f| = |F|^{E^n}$.

В частности, отображение $f: E \times E \rightarrow F$ — двуместная функция, а множество $F^{E \times E}$ есть множество всех двуместных функций, определенных на $E \times E$ со значениями в F . Количество таких функций определяется как $|f| = |F|^{E \times E} = |F|^{E^2}$.

Если при возведении в степень $E = \emptyset$, то $f(\emptyset) = \emptyset$, следовательно, $F^\emptyset = \emptyset$.

★ **Пример.** Определим все возможные функции $f: E \times E \rightarrow F$, где $E = \{0, 1\}$, $F = \{a, b\}$. Таких функций будет $2^4 = 16$.

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	a	a	a	a	a	a	a	a	b	b	b	b	b	b	b	b
0	1	a	a	a	a	b	b	b	b	a	a	a	a	b	b	b	b
1	0	a	a	b	b	a	a	b	b	a	a	b	b	a	a	b	b
1	1	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b

Как видно из таблицы, каждая функция есть множество пар $\{ \langle \langle x_1, x_2 \rangle, y \rangle \}$, например, $f_4 = \{ \langle \langle 0, 0 \rangle, a \rangle, \langle \langle 0, 1 \rangle, a \rangle, \langle \langle 1, 0 \rangle, b \rangle, \langle \langle 1, 1 \rangle, b \rangle \}$.

3.3. Свойства функциональных отображений

Пусть f — функциональное отображение E в F и A — подмножество E . Обозначим через $f(A)$ подмножество F , образованное из всех элементов $f(x)$, где $x \in A$. Подмножество $f(A)$ называется *образом подмножества A при отображении $f: A \rightarrow f(A)$* , или *сужением функции $E \rightarrow f(E)$* . Очевидно, что $f(\emptyset) = \emptyset$. Исходя из отображения f , определим некоторое отображение $A \rightarrow f(A)$. Это отображение сохраняет операции $\subset, \cap, \cup, \setminus$ в следующем смысле. (В доказательствах символ \Rightarrow означает «влечет», «следовательно», символ \Leftrightarrow — «равносильно», «равнозначно».)

Утверждение 3.1. Если $A \subset B$, то $f(A) \subset f(B)$.

Доказать самостоятельно.

Утверждение 3.2. $f(A \cup B) = f(A) \cup f(B)$.

Доказательство.

$$\begin{aligned} f(x) \in f(A \cup B) &\Rightarrow x \in A \cup B \Leftrightarrow x \in A \text{ или } x \in B \Rightarrow f(x) \in f(A) \\ \text{или } f(x) \in f(B) &\Leftrightarrow f(x) \in f(A) \cup f(B) \Rightarrow \\ &\Rightarrow f(A \cup B) \subseteq f(A) \cup f(B). \quad (1) \\ f(x) \in f(A) \cup f(B) &\Leftrightarrow f(x) \in f(A) \text{ или } f(x) \in f(B) \Rightarrow x \in A \end{aligned}$$

$$\begin{aligned} \text{или } x \in B &\Leftrightarrow x \in A \cup B \Rightarrow f(x) \in f(A \cup B) \Rightarrow \\ &\Rightarrow f(A) \cup f(B) \subseteq f(A \cup B). \end{aligned} \quad (2)$$

Из (1) и (2) $\Rightarrow f(A \cup B) = f(A) \cup f(B)$.

Утверждение 3.3. $f(A \setminus B) = f(A) \setminus f(B)$.

Доказательство.

$$\begin{aligned} f(x) \in f(A \setminus B) &\Rightarrow x \in A \setminus B \Leftrightarrow x \in A \text{ и } x \notin B \Rightarrow f(x) \in f(A) \text{ и } \\ f(x) \notin f(B) &\Leftrightarrow f(x) \in f(A) \setminus f(B) \Rightarrow f(A \setminus B) \subseteq f(A) \setminus f(B). \quad (1) \end{aligned}$$

$$\begin{aligned} f(x) \in f(A) \setminus f(B) &\Leftrightarrow f(x) \in f(A) \text{ и } f(x) \notin f(B) \Rightarrow x \in A \text{ и } x \notin B \Leftrightarrow \\ &\Leftrightarrow x \in A \setminus B \Rightarrow f(x) \in f(A \setminus B) \Rightarrow f(A) \setminus f(B) \subseteq f(A \setminus B). \quad (2) \end{aligned}$$

Из (1) и (2) $\Rightarrow f(A \setminus B) = f(A) \setminus f(B)$.

Однако, операции \cap, \subset при этом отображении не сохраняются, имеет место лишь включение.

Утверждение 3.4. $f(A \cap B) \subset f(A) \cap f(B)$.

Доказательство.

$$\begin{aligned} f(x) \in f(A \cap B) &\Rightarrow x \in A \cap B \Leftrightarrow x \in A \text{ и } x \in B \Rightarrow f(x) \in f(A) \\ \text{и } f(x) \in f(B) &\Leftrightarrow f(x) \in f(A) \cap f(B) \Rightarrow \\ &\Rightarrow f(A \cap B) \subseteq f(A) \cap f(B). \quad (1) \end{aligned}$$

$f(x) \in f(A) \cap f(B) \Leftrightarrow f(x) \in f(A) \text{ и } f(x) \in f(B) \Rightarrow x \in A \text{ и } x \in B$. Однако возможно, что $A \cap B = \emptyset$, и тогда $f(A \cap B) = f(\emptyset) = \emptyset$, но при этом возможно, что $f(A) \cap f(B) \neq \emptyset$, и тогда $f(A \cap B) \subset f(A) \cap f(B)$, потому мы ограничимся результатом (1).

Пусть теперь B является некоторым подмножеством множества F . Будем обозначать через $f^{-1}(B)$ подмножество E , образованное из всех таких элементов x , что $f(x) \in B$. Подмножество $f^{-1}(B)$ называется *прообразом множества B при отображении f* . Это определение вовсе не предполагает биективности f . Если $y \in F$, то можно говорить о $f^{-1}(\{y\})$, но это — некоторое подмножество E , а не элемент E . Оно может содержать более одного элемента, если f не является инъективным, и может оказаться пустым, если f не сюръективно. Если f биективно, то $f^{-1}(\{y\}) = \{f^{-1}(y)\}$. Очевидно, что $f^{-1}(\emptyset) = \emptyset$.

Мы связали с отображением f отображение $B \rightarrow f^{-1}(B)$ множества $\wp(F)$ во множество $\wp(E)$. Это отображение сохраняет операции $\subset, \cup, \cap, \setminus$, в следующем смысле.

Утверждение 3.5. Если $A \subset B$, то $f^{-1}(A) \subset f^{-1}(B)$.

Доказать самостоятельно.

Утверждение 3.6. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Доказательство.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\Rightarrow f(x) \in A \cup B \Leftrightarrow f(x) \in A \text{ или } f(x) \in B \Rightarrow \\ &\Rightarrow x \in f^{-1}(A) \text{ или } x \in f^{-1}(B) \Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B) \Rightarrow \\ &\Rightarrow f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B). \quad (1) \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(A) \cup f^{-1}(B) &\Leftrightarrow x \in f^{-1}(A) \text{ или } x \in f^{-1}(B) \Rightarrow f(x) \in A \\ \text{или } f(x) \in B &\Leftrightarrow f(x) \in A \cup B \Rightarrow x \in f^{-1}(A \cup B) \Rightarrow \\ &\Rightarrow f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B). \end{aligned} \quad (2)$$

Из (1) и (2) $\Rightarrow f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

Утверждение 3.7. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Доказательство.

$$\begin{aligned} x \in f^{-1}(A \cap B) &\Rightarrow f(x) \in A \cap B \Leftrightarrow f(x) \in A \text{ и } f(x) \in B \Rightarrow \\ &\Rightarrow x \in f^{-1}(A) \text{ и } x \in f^{-1}(B) \Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B) \Rightarrow \\ &\Rightarrow f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B). \end{aligned} \quad (1)$$

$$\begin{aligned} x \in f^{-1}(A) \cap f^{-1}(B) &\Leftrightarrow x \in f^{-1}(A) \text{ и } x \in f^{-1}(B) \Rightarrow f(x) \in A \text{ и } \\ f(x) \in B &\Leftrightarrow f(x) \in A \cap B \Rightarrow x \in f^{-1}(A \cap B) \Rightarrow \\ &\Rightarrow f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B). \end{aligned} \quad (2)$$

Из (1) и (2) $\Rightarrow f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Утверждение 3.8. $f^{-1}(A') = (f^{-1})'(A)$.

Доказать самостоятельно.

Утверждение 3.9. $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

Доказать самостоятельно.

3.4. Композиция отображений

☞ **Определение 3.10.** Пусть даны три множества E, F и G , и заданы отображения $f: E \rightarrow F, g: F \rightarrow G$. Тогда *композицией* отображений $g \circ f: E \rightarrow G$ называется отображение E в G , которое определяется формулой $g \circ f = g(f(x))$.

Иными словами, если существует множество пар $\langle x, y \rangle \in f$ и $\langle y, z \rangle \in g$, то множество пар $\langle x, z \rangle \in g \circ f$ образует композицию отображений $g \circ f$. Запись $g \circ f$ производится в порядке, обратном тому, в котором производятся операции $f: E \rightarrow F, g: F \rightarrow G$. Таким образом, в математике принято правило, согласно которому композицию отображений $g \circ f$ надо начинать с выполнения операции f , которая расположена справа.

✱ **Примеры.**

1. Пусть $f: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = x - 1; g: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = e^x$. Композиция функций $g \circ f: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = e^{x-1}, f \circ g: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = e^{x-1}$.
2. Пусть $f: \mathbf{R} \rightarrow \mathbf{Z} \Leftrightarrow y = [x]$ (целая часть числа x); $g: \mathbf{Z} \rightarrow \{0, 1\} \Leftrightarrow (y) \bmod 2$. Тогда $g \circ f: \mathbf{R} \rightarrow \{0, 1\}$ есть $([x]) \bmod 2$ – остаток от деления целой части числа x на 2.

Теорема 3.1. Композиция отображений ассоциативна, т.е., если f, g, h – отображения E в F, F в G и G в H соответственно, то $(h \circ g) \circ f = h \circ (g \circ f)$, что записывается в виде: $h \circ g \circ f$.

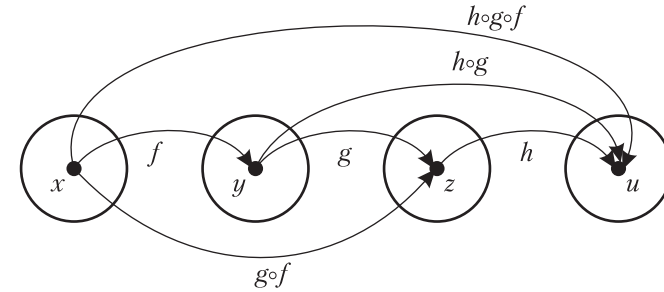


Рис. 3.10. Композиция отображений.

Доказательство. Пусть $\langle x, u \rangle \in h \circ (g \circ f)$, $\langle x, z \rangle \in g \circ f$, $\langle z, u \rangle \in h$. Поскольку $\langle x, z \rangle \in g \circ f$, то существует такое y , что $\langle x, y \rangle \in f$ и $\langle y, z \rangle \in g$, а поскольку существует $\langle z, u \rangle \in h$, то существует и $\langle y, u \rangle \in h \circ g$. Следовательно, если $\langle x, y \rangle \in f$ и $\langle y, u \rangle \in h \circ g$, то существует и $\langle x, u \rangle \in (h \circ g) \circ f$ (см. рис. 3.10). ☞

Теорема 3.2. Композиция отображений не коммутативна.

Доказательство этой теоремы очевидно, оно основано на самом определении композиции.

Для примера рассмотрим два отображения $f: y = \sin x$ и $g: y = x^2$, где $x, y \in \mathbf{R}$. Композиция $g \circ f: y = \sin^2 x$, а композиция $f \circ g: y = \sin x^2$. Очевидно, это различные функции.

☞ **Определение 3.11.** Отображение множества E в E , при котором каждый элемент переходит в себя, называется *тождественным отображением* и обозначается I_E . Для тождественных отображений справедливы равенства¹:

$$f \circ I_E = I_F \circ f = f.$$

Теорема 3.3. Отображение $f: E \rightarrow F$ имеет обратное тогда и только тогда, когда f – биекция.

Доказательство.

Достаточность. Если f – инъекция и сюръекция, то необходимо доказать, что существует $f^{-1}: F \rightarrow E$.

Так как $f(x)$ – сюръекция, то каждый элемент из F имеет хотя бы один прообраз в E : $\exists x \in E (f(x) = y)$, т.е. соответствие $f^{-1}: F \rightarrow E$ всюду определено на F и, следовательно, является отображением.

¹ Если все рассматриваемые отображения есть биекции, то для каждого отображения существует обратное, и множество всех отображений из E в F образует группу, в которой тождественные отображения I_E, I_F являются левой и правой единицей.

А так как $f(x)$ — инъекция, т.е. для $x_1 \neq x_2$ $f(x_1) \neq f(x_2)$, то каждый элемент y имеет только один прообраз, следовательно, отображение $f^{-1}: F \rightarrow E$ функционально.

Необходимость. Пусть $f^{-1}: F \rightarrow E$ — функциональное отображение. Докажем, что f — биекция.

Поскольку f^{-1} — отображение, то каждый элемент y из F имеет прообраз в E , т.е. отображение f сюръективно. Поскольку отображение f^{-1} функционально, то каждому образу $f(x)$ соответствует единственный прообраз x , т.е. f — инъекция. Следовательно, f — биекция. ∞

Теорема 3.4. Если f и g — функциональные отображения, либо сюръекции, либо инъекции, либо биекции, то можно доказать ряд утверждений о свойствах композиции этих отображений. Эти свойства отображены в табл. 3.1, где символами обозначены: О — отображение, С — сюръекция, И — инъекция, Б — биекция.

Доказательство этих 16 утверждений предоставляется читателю.

Таблица 3.1.

$g \circ f$	О	С	И	Б
О	О	О	О	О
С	О	С	О	С
И	О	О	И	И
Б	О	С	И	Б

*** Пример.** Докажем утверждение: композиция инъекции и сюръекции есть отображение.

Доказательство. Пусть g — сюръекция, f — инъекция, $g \circ f$ — их композиция, и пусть $\langle x, y \rangle \in f$, $\langle y, z \rangle \in g$, $\langle x, z \rangle \in g \circ f$ (см. рис. 3.11).

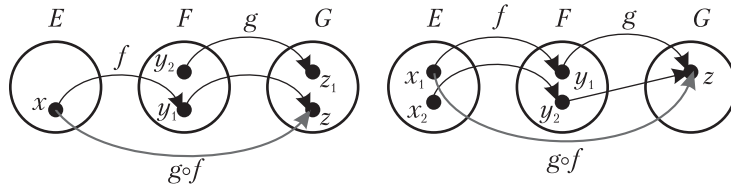


Рис. 3.11. Композиция инъекции и сюръекции.

Поскольку g — сюръекция, то для всякого $z \in G$ существует по меньшей мере один прообраз $y \in F$, и, возможно, существуют пары $\langle y_1, z \rangle \in g$, $\langle y_2, z \rangle \in g$, где $y_1, y_2 \in F$, $z_1, z_2 \in G$. Так как f — инъекция, то для всякого $x \in E$ существует не более одного образа $y \in F$.

Если y_1 есть образ элемента $x \in E$, то z_1 есть образ элемента $x \in G$, т.е. существует пара, $\langle x, z_1 \rangle \in g \circ f$. Элемент y_2 может не иметь прообраза в E , и, следовательно, не каждый элемент z имеет прообраз в E , откуда следует, что $g \circ f$ не сюръекция.

Поскольку f — инъекция, то существуют пары $\langle x_1, y_1 \rangle \in f$, $\langle x_2, y_2 \rangle \in f$, и $y_1 \neq y_2$, а так как g — сюръекция, то возможно, что существуют пары $\langle y_1, z \rangle \in g$, $\langle y_2, z \rangle \in g$, и, следовательно, существуют пары $\langle x_1, z \rangle \in g \circ f$, $\langle x_2, z \rangle \in g \circ f$, откуда следует, что $g \circ f$ не инъекция. Следовательно, $g \circ f$ — просто отображение.

*** Пример.** Пусть $f: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = x - 1$ — биекция; $g: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = e^{2x}$ — инъекция (так как нет ни одного элемента $x \in \mathbf{R}$, для которого $y = 0$ есть образ). Композиция функций $g \circ f: \mathbf{R} \rightarrow \mathbf{R} \Leftrightarrow y = e^{2(x-1)}$ — инъекция, согласно теореме 3.4.

3.5. Замена переменной и замена функции

Определение 3.12. Пусть f — функция, определенная на E со значениями в F . Если u является отображением некоторого множества E_1 во множество E , то можно построить новую функцию $f_1 = f \circ u$, определенную на E_1 со значениями в F (рис. 3.12). Говорят, что в этом случае произведена *замена переменной*, или замена исходного множества E на E_1 , и что f_1 является *прообразом* f при этой замене переменных. Произведя в выражении $f(x)$ подстановку $x = u(x_1)$, получают выражение $f_1(x_1)$. Иногда это обозначают как $f^*(x_1) = f(u(x_1))$.

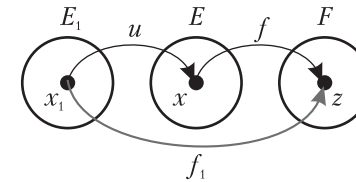


Рис. 3.12. Замена переменной.

Определение 3.13. Пусть v является некоторым отображением F в множество F_1 . Тогда можно определить новую функцию $f^* = v \circ f$, определенную на E со значениями в F_1 (рис. 3.13). В этом случае говорят, что произведена *замена функции* или замена множества значений F на множество F_1 и что f^* является *образом* f при этой замене. Замену функции называют еще *аппликацией* функций. Иногда это обозначают как $f^*(x) = v(f(x))$.

*** Пример.** Пусть исходная функция $E \rightarrow F: f(x) = x^2$. Заданы функции: $E_1 \rightarrow E: u(x_1) = x_1 + 1$; $F \rightarrow F_1: v(x) = 2x$. Выполним замену переменной в функции $f(x)$: $f(u(x_1)) = (x_1 + 1)^2$. Выполним замену

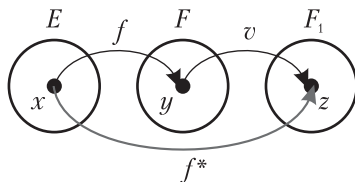


Рис. 3.13. Замена функции.

функции в функции $f(x)$: $v(f(x)) = 2x^2$. Таким образом, при замене переменной мы получаем новую функцию, зависящую от новой переменной, а при замене функции — новую функцию, зависящую от той же самой переменной.

Можно произвести одновременно и замену переменной и замену функции: $f_3 = v \circ f \circ u$. Здесь f_3 является образом f при замене переменной u и замене функции v . Например, для определенных выше функций: $f_3 = v \circ f \circ u = v(f(u(x_1))) = 2(x_1 + 1)^2$.

Глава 4.

МОЩНОСТЬ МНОЖЕСТВ**4.1. Определение мощности**

Понятие мощности множеств связано с оценкой числа элементов в нем. В конечном множестве количество элементов можно пересчитать. Число элементов в множестве X обозначается обычно как $|X|$. Например, если $X = \{a, b, c\}$, то $|X| = 3$. Если два множества имеют одинаковое число элементов, то между ними можно установить взаимно однозначное соответствие. Тогда все конечные множества, имеющие одинаковое количество элементов, будут эквивалентны по числу элементов в них и образуют один класс эквивалентности. Этот класс эквивалентности может быть обозначен целым натуральным числом, определяющим количество элементов в множествах. Все одноэлементные множества образуют один класс эквивалентности, двухэлементные — другой, и так далее. Каждому натуральному числу соответствует класс эквивалентности, объединяющий все конечные множества с числом элементов, равным данному числу.

Мощность объединения нескольких конечных множеств можно найти по формулам:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|;$$

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|.$$

(Читателю предлагается доказать эти равенства самостоятельно и найти общее выражение.)

Рассмотрим теперь бесконечные множества. Для некоторых бесконечных множеств тоже можно установить взаимно однозначное соответствие элементов. Например, для множества четных натуральных чисел, которое можно представить в виде списка: $\{2, 4, 6, \dots\}$, последовательность $(1, 2, 3, \dots)$ будет нумерацией этого списка, т.е. существует отображение $f(n) = 2n$, для каждого $n \in \mathbf{N}$ множества натуральных чисел \mathbf{N} в множество всех четных положительных целых чисел, которое является биекцией. Следовательно, множество всех четных натуральных чисел эквивалентно множеству всех натуральных чисел, т.е. *четных чисел ровно столько же, сколько всех натуральных чисел*. Но, с другой стороны, множество натуральных чисел можно разбить на два подмножества четных и нечетных чисел, т.е. четных чисел ровно половина из всех натуральных чисел! Получаем, что в некотором смысле *часть равна целому*¹. И это действительно так.

¹ Этот факт, заключающийся в том, что между бесконечной совокупностью и ее собственной частью можно установить взаимно однозначное соответствие, отмечался еще Плутархом и другими древними учеными. В 1638 году Галилей отметил, что между целыми положительными числами и их квадратами существует взаимно однозначное соответствие, и назвал «парадоксом» свое наблюдение, поскольку этот факт вступает в противоречие с евклидовой аксиомой, согласно которой целое больше любой из своих собственных частей, т.е. частей, не совпадающих со всем целым.

Можно показать, что существует биекция из множества натуральных чисел на любое его бесконечное подмножество. Действительно, пусть $P \subset \mathbf{N}$. Выберем в P наименьший элемент и обозначим его x_1 ; вычтем этот элемент из P и наименьший элемент из всех оставшихся обозначим x_2 . Продолжая этот процесс, мы присвоим номер каждому элементу из P . Эта нумерация есть биекция $\mathbf{N} \rightarrow P$: $n \rightarrow x_n$, где x_n есть $(n+1)$ -й в порядке возрастания элемент P . Таким образом, множество нечетных чисел, множество квадратов натуральных чисел и множество любых линейных комбинаций, например, $ax + b$, где $a, b \in \mathbf{N}$, будут эквивалентны между собой и войдут в один класс эквивалентности.

↪ **Определение 4.1.** Отношение эквивалентности, которое определяется взаимно однозначным соответствием двух множеств, называется *равномощностью*, а класс эквивалентности равномощных множеств называется *мощностью* этих множеств.

Мощность множества X обозначается $\text{card } X$. Число элементов конечного множества также называется мощностью, тогда $\text{card } X = |X|$. Для равномощных множеств часто используется обозначение $E \sim F$.

4.2. Кардинальные числа

Сравнение бесконечных множеств возможно благодаря свойствам функциональных отображений. Из определения инъекции следует, что инъекция из множества E в множество F возможна только в том случае, если количество элементов в E не больше, чем количество элементов в F : $|E| \leq |F|$ (для конечных множеств), причем, если не существует инъекции из F в E , то это неравенство превращается в строгое неравенство $|E| < |F|$ (см. рис. 4.1). Если же существует инъекция из F в E , причем не обязательно совпадающая с обратным отображением для инъекции $E \rightarrow F$, то это возможно лишь тогда, когда количество элементов в них совпадает, т.е. $|E| = |F|$, а в этом случае можно найти и взаимно однозначное соответствие между E и F , т.е. биекцию.

Аналогично, если существует сюръекция из E на F , такая, что один образ в F имеет несколько прообразов в E , то количество элементов в E строго больше количества элементов в F , т.е. $|E| > |F|$.

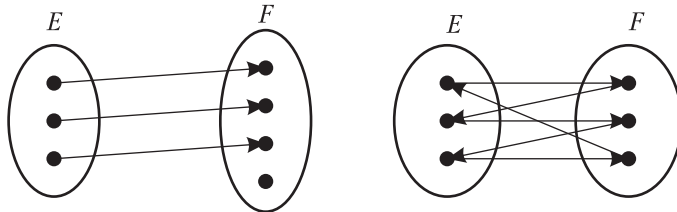


Рис. 4.1. Инъекция $E \rightarrow F$.

Эти свойства обобщаются для случая бесконечных множеств следующей теоремой.

Теорема 4.1 (Кантора — Бернштейна¹).

Пусть E и F — два произвольных бесконечных множества. Тогда: а) либо существует инъекция из E в F , либо существует инъекция из F в E (одно не исключает другого);

б) если существуют инъекции $E \rightarrow F$ и $F \rightarrow E$, то существует биекция из E в F .

Иными словами, если множество E равномощно некоторому подмножеству множества F , а множество F равномощно некоторому подмножеству множества E , то E и F равномощны.

Доказательство. Пусть E равномощно некоторому подмножеству F_1 множества F , а F равномощно некоторому подмножеству E_1 множества E (см. рис. 4.2, а). При взаимно однозначном соответствии между E_1 и F_1 подмножество $F_1 \subset F$ переходит в некоторое подмножество $E_2 \subset E_1$. При этом все три множества E , E_1 и E_2 равномощны, и нужно доказать, что они равномощны множеству F , или, что то же самое, множеству E_1 . Теперь мы можем забыть про множество F и его подмножества и доказывать такой факт:

если $E_2 \subset E_1 \subset E_0$ (где E_0 — обозначение для E) и E_2 равномощно E_0 , то все три множества равномощны.

Пусть f — функция, которая осуществляет взаимно однозначное соответствие $E_0 \rightarrow E_2$, так, что элемент $x \in E_0$ соответствует элементу $f(x) \in E_2$. Когда E_0 переходит в E_2 , меньшее множество E_1 переходит в какое-то множество $E_3 \subset E_2$ (см. рис. 4.2, б). Аналогично, само E_2 переходит в какое-то множество $E_4 \subset E_2$. При этом $E_4 \subset E_3$, так как $E_2 \subset E_1$.

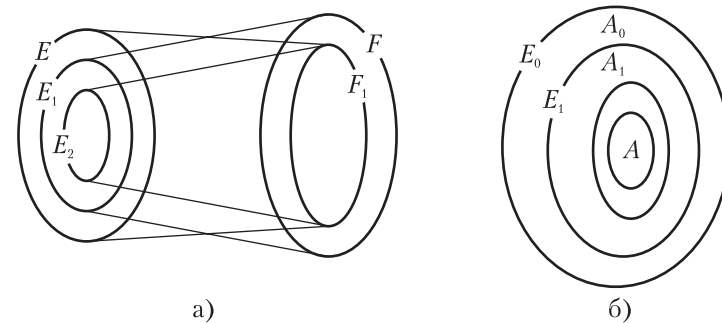


Рис. 4.2. К доказательству теоремы Кантора — Бернштейна.

¹ Кантор сформулировал эту теорему без доказательства в 1883 году, пообещав вернуться к ней позже, однако, не выполнил этого обещания. Первые доказательства теоремы были даны Шрёдером (1896) и Бернштейном (1897).

Продолжая это построение, получаем убывающую последовательность множеств $E_0 \supset E_1 \supset E_2 \supset E_3 \supset E_4 \supset \dots$ и взаимно однозначное соответствие $f: E_0 \rightarrow E_2$, при котором E_i отображается в E_{i+2} . Формально можно описать E_{2n} как множество тех элементов, которые получаются из множества E_0 после n -кратного применения функции f .

Таким образом, множество E_0 мы разбили на непересекающиеся слои $A_i = E_i \setminus E_{i+1}$ и на сердцевину $A = \bigcap_i E_i$. Слои A_0, A_2, A_4, \dots равномогны, так как функция f осуществляет взаимно однозначное соответствие между A_0 и A_2 , между A_2 и A_4 и т.д. Аналогично, равномогны и слои с нечетными номерами.

Теперь можно легко построить взаимно однозначное соответствие g между E_0 и E_1 .

Пусть $x \in E_0$, тогда соответствующий ему элемент $g(x)$ строится так: $g(x) = f(x)$ при $x \in A_{2k}$ и $g(x) = x$ при $x \in A_{2k+1}$ или $x \in A$ (как показано ниже).

$$\begin{array}{ccccccc} E_0 = & A_0 & + & A_1 & + & A_2 & + & A_3 & + & A_4 & + & \dots & + & A \\ & \searrow & & \downarrow & & \searrow & & \downarrow & & \searrow & & \downarrow & & \downarrow \\ E_1 = & & & A_1 & + & A_2 & + & A_3 & + & A_4 & + & \dots & + & A \end{array}$$

Это доказывает теорему. \simeq

Следствия из теоремы Кантора — Бернштейна:

а) если существует инъекция $E \rightarrow F$ и не существует инъекции $F \rightarrow E$, то множество F имеет мощность, строго большую, чем мощность E : $\text{card } F > \text{card } E$.

б) если существует инъекция $F \rightarrow E$ и не существует инъекции $E \rightarrow F$, то множество F имеет мощность, строго меньшую, чем мощность E : $\text{card } F < \text{card } E$.

в) если существует биекция из F в E , то множества F и E равномогны: $\text{card } F = \text{card } E$.

Класс эквивалентности равномогных множеств называется *мощностью*, или *кардинальным числом*. Классы эквивалентности равномогных конечных множеств являются конечными кардинальными числами. Эти числа по определению являются натуральными числами, соответствующими количеству элементов в конечном множестве. Мощность пустого множества равна нулю: $\text{card } \emptyset = 0$. Мощность бесконечного множества называется *трансфинитным кардинальным числом*, или просто *трансфинитным числом*. Таким образом, множество кардинальных чисел — это фактор-множество равномогных множеств, которое представляет собой объединение множеств натуральных и трансфинитных чисел.

4.3. Счетные множества

↪ **Определение 4.2.** *Мощностью счетного множества называется мощность множества натуральных чисел \mathbf{N} . Счетным называется всякое множество X , равномогное множеству \mathbf{N} натуральных чисел. Мощность счетного множества обозначается кардинальным трансфинитным числом \aleph_0 (читается: *алеф-нуль*)¹.*

Счетность множества X означает, что существует по крайней мере одна биекция из X на \mathbf{N} (однако это не значит, что такая биекция задана). Иначе счетное множество можно определить как множество, элементы которого можно расположить в виде *списка* (даже, если этот список будет бесконечным). Тогда каждому элементу множества можно поставить в соответствие его порядковый номер в этом списке, т.е. может быть построено отображение из \mathbf{N} в X $f(n): \mathbf{N} \rightarrow X$, где $n \in \mathbf{N}$. Такое отображение называется *нумерацией*. Очевидно, что занумеровать можно любое конечное множество. Множество X конечно или счетно тогда и только тогда, когда существует инъекция X в \mathbf{N} , или, если $X \neq \emptyset$, тогда и только тогда, когда существует сюръекция \mathbf{N} на X .

✱ **Пример.** Множества всех четных натуральных чисел X и множество \mathbf{N} равномогны, так как существует инъекция $X \rightarrow \mathbf{N}$ и сюръекция $\mathbf{N} \rightarrow X$.

Докажем ряд теорем о счетных множествах.

Теорема 4.2. Множество положительных рациональных чисел \mathbf{Q}^+ счетно.

Доказательство. Любое рациональное число представимо в виде дроби m/n , где m, n — натуральные числа, $n \neq 0$. Запишем рациональные числа в виде таблицы:

1/1	2/1	3/1	4/1	...
1/2	2/2	3/2	4/2	...
1/3	2/3	3/3	4/3	...
...

1	2	5	10	...
4	← 3	↓ 6	11	...
9	← 8	← 7	↓ 12	...
...

Правая таблица задает нумерацию элементов левой таблицы (стрелки указывают направление нумерации). Тогда мы можем выписать элементы левой таблицы (множество рациональных положительных чисел) в виде списка, в котором каждому элементу соответствует натуральное число:

1/1	2/1	2/2	1/2	3/1	3/2	3/3	2/3	1/3	4/1	4/2	4/3	...
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	...
1	2	3	4	5	6	7	8	9	10	11	12	...

¹ Можно встретить другое обозначение мощности счетного множества: $\text{card } \mathbf{N} = \mathbf{v}$.

Полученный пересчет доказывает счетность множества положительных рациональных чисел. \asymp

Можно заметить, что рациональные числа входят в этот пересчет с повторениями: например, $1/1 = 2/2 = 3/3 = \dots = 1$. Однако, нетрудно составить эффективную процедуру вычеркивания повторяющихся чисел из этого пересчета. Мы покажем далее, что и без вычеркивания повторений доказательство счетности множества \mathbb{Q}^+ уже завершено.

Теорема 4.3. Множество целых чисел \mathbb{Z} счетно.

Доказательство. Построим список:

0	1	-1	2	-2	3	-3	...
↓	↓	↓	↓	↓	↓	↓	...
0	1	2	3	4	5	6	...

Тогда каждому четному числу соответствует отрицательное число, а каждому нечетному — положительное. Построенная биекция доказывает теорему. \asymp

Теорема 4.4. Множество всех рациональных чисел \mathbb{Q} счетно.

Доказательство аналогично предыдущему.

Теорема 4.5. Мощность счетного множества \aleph_0 является наименьшим трансфинитным кардинальным числом. Это означает, что всякое бесконечное множество E имеет по крайней мере одну счетную часть (т.е. счетное подмножество).

Доказательство. Предположим, что для некоторого бесконечного множества E соотношение $\text{card } E > \aleph_0$ не выполняется, т.е. $\text{card } E \leq \aleph_0$. Это означает, по теореме Бернштейна, что существует инъекция $E \rightarrow \mathbb{N}$, т.е. в \mathbb{N} существует бесконечная часть P , такая, что между E и P существует биекция. Однако между множеством \mathbb{N} и его бесконечной частью P тоже существует биекция. Отображение $n \rightarrow x_n$, где x_n есть $(n+1)$ -й в порядке возрастания элемент P , определяет биекцию \mathbb{N} на P . Тогда получим, что $\text{card } E = \aleph_0$. \asymp

4.4. Кардинальная арифметика

Если существует сюръекция $E \rightarrow F$, то $\text{card } F \leq \text{card } E$. Действительно, прообраз каждой точки F не пуст, и если в каждом из прообразов выбрать по одному элементу¹, то получим некоторую часть E , равносильную F . Например, фактор-множество множества

¹ Выбрать по одному элементу в каждом из конечного числа множеств нетрудно, но подобный выбор в случае бесконечного числа множеств затруднителен. После многочисленных споров в начале века возможность такого выбора была введена как аксиома теории множеств — аксиома выбора, или аксиома Цермело.

E по некоторому отношению эквивалентности всегда имеет не большую мощность, чем само множество E . Отсюда, а также из теоремы 4.5 следует, что в классе кардинальных чисел существует отношение порядка: если α является кардинальным числом некоторого подмножества множества мощности β , то $\alpha \leq \beta$.

Нетрудно показать (для конечных множеств это просто, а для бесконечных это следует из теоремы Кантора-Бернштейна), что это отношение рефлексивно, антисимметрично и транзитивно, следовательно, оно действительно является отношением порядка. Из теоремы Кантора-Бернштейна следует также, что это отношение является отношением линейного порядка, т.е. любые два кардинальные числа сравнимы.

На множестве кардинальных чисел можно определить операции сложения, умножения и возведения в степень.

1. Сложение. Пусть α и β кардинальные числа, а множества E и F имеют соответственно мощности $\text{card } E = \alpha$ и $\text{card } F = \beta$. Тогда $\alpha + \beta$ — сумма мощностей E и F , — это мощность всякого множества, допускающего разбиение на два класса эквивалентности, равносильных множествам E и F соответственно. Иными словами, если множества E и F не пересекаются, то мощность их объединения равна $\alpha + \beta$.

2. Умножение. Через $\alpha \cdot \beta$ обозначается мощность декартового произведения $E \times F$. Иными словами, произведение $\alpha \cdot \beta$ — это кардинальное число объединения α непересекающихся частей, каждая из которых имеет мощность β .

3. Возведение в степень. Через α^β обозначается мощность множества E^F , т.е. мощность множества всех функциональных отображений из F в E : $\text{card } (F \rightarrow E) = \text{card } (E^F) = \text{card } E^{\text{card } F}$.

Теорема 4.6. Операции, определенные на множестве кардинальных чисел, обладают следующими свойствами.

1. Ассоциативность и коммутативность сложения.
2. Ассоциативность и коммутативность умножения.
3. Дистрибутивность умножения по отношению к сложению:
 $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.
4. Для возведения в степень выполняются соотношения:
 а) $(\alpha^\beta) \cdot (\alpha^\gamma) = \alpha^{\beta + \gamma}$,
 б) $\alpha^\beta \cdot \alpha^\gamma = (\alpha \cdot \beta)^\gamma$,
 в) $((\alpha)^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$.

Доказательство этих свойств основано на определении и свойствах операций объединения, декартова произведения и функциональных отображений множеств. \asymp

В качестве примеров докажем следующие свойства.

Свойство 3. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Доказательство. Пусть $\text{card } A = \alpha$, $\text{card } B = \beta$, $\text{card } C = \gamma$, где множества A, B, C попарно не пересекаются, и пусть $a \in A, b \in B, c \in C$. Соотношение 3 выполняется, если $A \times (B \cup C) \sim (A \times B) \cup (A \times C)$. Рассмотрим эти множества.

Множество $A \times (B \cup C)$ состоит из пар $\{<a, b>, <a, c>\}$, причем $b \neq c$, так как $B \cap C = \emptyset$.

Множество $(A \times B) \cup (A \times C)$ состоит из объединения множеств пар $\{<a, b>\} \cup \{<a, c>\}$, что эквивалентно множеству $\{<a, b>, <a, c>\}$, где $b \neq c$. Как видим, эти два множества совпадают.

Покажем, что дистрибутивность сложения относительно умножения не выполняется, т.е. $\alpha + (\beta \cdot \gamma) \neq (\alpha + \beta) \cdot (\alpha + \gamma)$.

Для этого покажем, что в общем случае отношение равномощности $A \cup (B \times C) \sim (A \cup B) \times (A \cup C)$ невыполнимо. Действительно, $A \cup (B \times C)$ — это множество, полученное объединением $\{a\} \cup \{<b, c>\} = \{a, <b, c>\}$, т.е. это множество, составленное из всех элементов множества A и пар $<b, c>$, в то время как $(A \cup B) \times (A \cup C) = \{<a, a>, <b, a>, <a, c>, <b, c>\}$. Очевидно, что это различные множества.

Иначе это можно показать так: $(A \cup B) \times (A \cup C) = ((A \cup B) \times A) \cup ((A \cup B) \times C) = (A \times A) \cup (B \times A) \cup (A \times C) \cup (B \times C)$, что не эквивалентно $A \cup (B \times C) = (A \times B) \cup (A \times C)$. \simeq

4.5. Основные соотношения кардинальной арифметики

Теорема 4.7. Для любого конечного числа $m \geq 1$ выполняются равенства:

$$m \cdot \aleph_0 = \aleph_0 \text{ и } \aleph_0^m = \aleph_0.$$

Доказательство. Воспользуемся методом математической индукции. Покажем сначала, что $N \times N$ равномощно N , т.е. $\aleph_0 \cdot \aleph_0 = \aleph_0$ (базис индукции).

Элементы декартового произведения $N \times N$ можно выписать в виде таблицы:

(0,0)	→	(0,1)	→	(0,2)	→	(0,3)	...
(1,0)	→	(1,1)	→	(1,2)	→	(1,3)	...
(2,0)	→	(2,1)	→	(2,2)	→	(2,3)	...
(3,0)	→	(3,1)	→	(3,2)	→	(3,3)	...
...	

Введем диагональную нумерацию. Получим последовательность $(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), \dots$. Эта последовательность определяет биекцию N на $N \times N$. Следовательно, N эквивалентно $N \times N$, т.е. $\aleph_0 \cdot \aleph_0 = \aleph_0^2 = \aleph_0$.

Предположим теперь, что $\aleph_0^{m-1} = \aleph_0$, и покажем, что тогда $\aleph_0^m = \aleph_0$.

По предположению индукции декартово произведение N^{m-1} счетно. Тогда, согласно базису индукции, декартово произведение двух счетных множеств $N^{m-1} \times N = N^m$ также счетно, т.е. $\aleph_0^m = \aleph_0$.

Следствие. Объединение конечного или счетного множества конечных или счетных подмножеств множества E конечно или счетно.

Доказательство. Пусть I — некоторая часть N ($I \subset N$) и A_i ($i \in I$) — некоторые подмножества E , и для всякого i $A_i \neq \emptyset$ (но, если $A_i = \emptyset$, то это ничего не меняет, так как если $A_i = \emptyset$, то объединение не изменится). Пусть f_i — сюръекция N на A_i . Тогда отображение $(i, n) \rightarrow f_i(n)$ будет сюръекцией $I \times N$ на $\bigcup_{i \in I} A_i$.

Поскольку $I \times N$ счетно, то $\bigcup_{i \in I} A_i$ конечно или счетно. \simeq

Теперь можно иначе доказать, что множество рациональных чисел Q счетно. Каждой паре (p, q) ($q \neq 0$) множества $Z \times Z$ можно поставить в соответствие рациональное число p/q . Это отображение является сюръекцией подмножества $Z \times Z$ на Q . Значит, Q не более чем счетно, но так как оно содержит N в качестве своего подмножества, то Q счетно.

Теорема 4.8. Если A — бесконечное множество, а B конечно или счетно, то $A \cup B \sim A$ (равномощны), т.е. $\text{card}(A \cup B) = \text{card}(A)$.

Доказательство. Пусть A_1 — счетное подмножество множества A . Объединение счетного и конечного множеств счетно, объединение счетных множеств также счетно, поэтому $A_1 \cup B \sim A_1$. Множество $A \cup B$ не изменится, если из него вычесть, а потом добавить подмножество A_1 . Тогда $A \cup B = (A \setminus A_1) \cup (A_1 \cup B)$. Поскольку $A_1 \cup B \sim A_1$, то $(A \setminus A_1) \cup (A_1 \cup B) \sim (A \setminus A_1) \cup A_1$. Но $(A \setminus A_1) \cup A_1 = A$, следовательно, $A \cup B \sim A$, что и требовалось доказать. \simeq

Теорема 4.9. Если α и β — кардинальные числа, такие что $\alpha \neq 0$ и $\beta \neq 0$, и если по крайней мере одно из них трансфинитно, то сумма $\alpha + \beta$ и произведение $\alpha \cdot \beta$ равны наибольшему из них, т.е. $\alpha + \beta = \max\{\alpha, \beta\}$, $\alpha \cdot \beta = \max\{\alpha, \beta\}$.

Доказательство этой теоремы непосредственно следует из предыдущей теоремы. Действительно, поскольку множество кардинальных чисел линейно упорядочено, то либо $\alpha \leq \beta$, либо $\beta \leq \alpha$. Из теоремы 4.8 следует, что мощность объединения двух бесконечных множеств будет определяться большей мощностью. Из определения произведения кардинальных чисел и первого равенства: $\alpha + \beta = \max\{\alpha, \beta\}$, следует выполнимость и второго: $\alpha \cdot \beta = \max\{\alpha, \beta\}$.

Теперь мы можем доказать теорему 4.7 полностью.

Доказательство.

$$m \cdot \aleph_0 = \underbrace{\aleph_0 + \aleph_0 + \dots + \aleph_0}_{m \text{ раз}} = \aleph_0 \text{ (по теореме о счетности объеди-}$$

нения счетных множеств);

$$\aleph_0^m = \underbrace{\aleph_0 \cdot \aleph_0 \cdot \dots \cdot \aleph_0}_{m \text{ раз}} = \aleph_0 \text{ (по теореме о счетности декартова}$$

произведения счетных множеств).

Этот же результат мы получаем согласно теореме 4.9: так как $m \leq \aleph_0$, то $m \cdot \aleph_0 = \aleph_0$.

Использование кардинальной арифметики позволяет нам легко доказывать некоторые теоремы о мощности множеств.

* Примеры.

1. Определим мощность множества всех конечных последовательностей натуральных чисел.

Рассмотрим, из чего состоит это множество. Множество всех одноэлементных последовательностей — это множество \mathbf{N} , все двухэлементные последовательности образуются декартовым произведением $\mathbf{N} \times \mathbf{N}$, трехэлементные — \mathbf{N}^3 , k -элементные последовательности образованы декартовым произведением \mathbf{N}^k и так далее. Какое бы большое число k мы ни взяли, для него существует число $k+1$ и, соответственно, существует последовательность длиной $k+1$. Поэтому процесс построения последовательностей уходит в бесконечность. В результате мы получаем, что множество всех конечных последовательностей есть $E = \mathbf{N} \cup \mathbf{N}^2 \cup \mathbf{N}^3 \cup \dots \cup \mathbf{N}^k \cup \dots$, т.е. это объединение счетного множества счетных подмножеств множества E . Поскольку $\text{card } \mathbf{N} = \aleph_0$, $\text{card } \mathbf{N}^2 = \aleph_0^2$, ..., $\text{card } \mathbf{N}^k = \aleph_0^k$..., то мощность этого множества определяется выражением $\text{card } E = \aleph_0 + \aleph_0^2 + \aleph_0^3 + \dots + \aleph_0^k + \dots = \aleph_0$.

2. Для доказательства счетности некоторых множеств можно использовать способ кодирования¹. Наиболее распространенным

кодом натуральных чисел является двоичный код: каждому натуральному числу можно единственным образом поставить в соответствие двоичное число. Существуют эффективные процедуры перевода числа в двоичный код и обратно, поэтому такое соответствие является взаимно однозначным. Установив такое соответствие, мы получаем, например, что бесконечное множество всех конечных двоичных последовательностей счетно (на основании примера 1). Для кодирования можно использовать не только двоичную, но любую систему счисления с основанием k .

В качестве примера докажем, что *множество всех вещественных алгебраических чисел счетно*. Алгебраические числа — это действительные корни алгебраических (полиномиальных) уравнений с одним неизвестным с целыми коэффициентами:

$$a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0, \quad (n \geq 1, a_0 \neq 0).$$

Доказательство. Для каждого алгебраического уравнения количество его действительных корней конечно и не превышает степени уравнения. Тогда, если мы сможем пересчитать все алгебраические уравнения, то множество всех алгебраических чисел будет представлять собой объединение множеств действительных корней каждого уравнения, т.е. это будет объединение счетного множества конечных множеств, которое счетно. Следовательно, задача сводится к доказательству счетности множества алгебраических уравнений.

Алгебраические уравнения с целыми коэффициентами без потери однозначности можно представлять в виде строки, записывая показатели степеней после переменной x , например: $3x^3 + 6x^2 + x - 2 = 0$. Тогда уравнения оказываются конечными последовательностями, составленными из 14 символов: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, x , $+$, $-$, $=$. Первый символ последовательности не есть 0. Тогда мы можем рассматривать эти последовательности как числа в четырнадцатеричной системе счисления. В результате каждое уравнение, представленное как последовательность этих символов, является записью некоторого целого положительного числа в этой системе счисления, т.е. кодом этого числа в системе счисления с основанием 14. Таким образом, каждому алгебраическому уравнению будет поставлено в соответствие некоторое натуральное число. Тем самым будет построено взаимно однозначное соответствие между множеством алгебраических уравнений и подмножеством натуральных чисел. Иными словами, алгебраические уравнения могут быть пересчитаны в порядке возрастания натуральных чисел, кодами которых они являются при интерпретации входящих в уравнения символов как цифр четырнадцатеричной системы счисления. Построенный пересчет доказывает счетность множества алгебраических уравнений с целыми коэффициентами. Счетность

¹ В [Клини, 1973] этот способ называется методом цифр.

множества алгебраических чисел, как указано выше, следует как счетность объединения счетного множества конечных множеств.

4.6. Несчетные множества

Теорема 4.10 (Кантора). Каково бы ни было множество E , множество его подмножеств имеет мощность, строго большую мощности E .

Эта теорема показывает, что последовательность трансфинитных кардинальных чисел не ограничена.

Доказательство. Предположим, что существует сюръекция $f: E \rightarrow \wp(E)$, т.е. сюръекция f множества E на множество его подмножеств $\wp(E)$. Тогда для $x \in E$ $f(x)$ является элементом $\wp(E)$, т.е. некоторым подмножеством E . Обозначим через A подмножество E , образованное из таких $x \in E$, что $x \notin f(x)$. Так как $A \in \wp(E)$, то в E существует по крайней мере один элемент y , такой, что $f(y) = A$. Если $y \in f(y) = A$, то, по определению множества A , $y \notin A$, что невозможно. Если $y \notin f(y) = A$, то $y \in A$. В обоих случаях мы приходим к противоречию.

Поскольку, однако, существует инъекция E в $\wp(E)$, а именно, $x \rightarrow \{x\}$, то E имеет мощность, меньшую мощности $\wp(E)$, а значит, и строго меньшую мощности $\wp(E)$. \approx

Теорема 4.11. Если множество E бесконечно, то множество $\wp_f(E)$ конечных подмножеств E равномощно множеству E .

Доказательство. Отображение $(x_1, x_2, \dots, x_n) \rightarrow \{x_1, x_2, \dots, x_n\}$, ставящее в соответствие каждому элементу (x_1, x_2, \dots, x_n) из E^n подмножество E , образованное из этих элементов (не обязательно различных), является некоторой сюръекцией E^n на множество $\wp_n(E)$ непустых подмножеств E , образованных не более чем из n элементов. Но тогда $\text{card } \wp_n(E) \leq \text{card } E^n = \text{card } E$ (теорема 4.7), и поскольку $\text{card } \wp_n(E) \geq \text{card } E$, то $\text{card } \wp_n(E) = \text{card } E$. Пусть теперь $f_n: x \rightarrow f_n(x)$ — некоторая биекция E на $\wp_n(E)$. Положим $f_0(x) \neq \emptyset$ для всех $x \in E$. Тогда $(n, x) \rightarrow f_n(x)$ будет некоторой сюръекцией $N \times E$ на $\wp_f(E)$, а значит $\text{card } \wp_f(E) \leq \text{card } (N \times E) = \aleph_0 \cdot \text{card } E = \text{card } E$ (в силу теоремы 4.8, неравенства $\aleph_0 \leq \text{card } E$ и теоремы 4.9). Поскольку обратное неравенство очевидно, окончательно получаем $\text{card } \wp_f(E) = \text{card } E$. \approx

Замечание. Характеристической функцией некоторого подмножества A множества E называется функция φ_A , определенная на E и принимающая значения в множестве $\{0, 1\}$, такая, что $\varphi_A(x) = 1$, если $x \in A$, и $\varphi_A(x) = 0$, если $x \notin A$.

Задание этой функции однозначно определяет подмножество (часть) A множества E . Тогда каждому подмножеству будет соот-

ветствовать характеристический вектор, состоящий из 0 и 1. Например, если $E = \{a, b, c\}$, то подмножеству $A = \{a, c\}$ будет соответствовать вектор $\varphi_A = \langle 1, 0, 1 \rangle$, подмножеству $B = \{b\}$ — вектор $\varphi_B = \langle 0, 1, 0 \rangle$ и т.д.

Характеристическая функция $\varphi(x)$ задает множество отображений $\varphi: E \rightarrow \{0, 1\}$, т.е. $\{0, 1\}^E$. Тогда, на основании теоремы 4.11, существует биекция множества-степени $\wp(E)$ множества E на множество отображений $\varphi: E \rightarrow \{0, 1\}$. Отсюда следует, что кардинальным числом множества $\wp(E)$ является $\text{card } \{0, 1\}^E = 2^{\text{card } E}$.

Теперь теорему Кантора (4.10) можно сформулировать следующим образом:

Каково бы ни было кардинальное число α , $2^\alpha > \alpha$.

В частности, $2^{\aleph_0} > \aleph_0$. Отсюда следует, что существуют несчетные множества.

Мы доказали в предыдущем параграфе, что множество всех конечных последовательностей натуральных чисел счетно. Рассмотрим теперь множество всех бесконечных последовательностей натуральных чисел.

Теорема 4.12. Множество всех бесконечных последовательностей натуральных чисел несчетно.

Доказательство (1). Предположим, что множество бесконечных последовательностей натуральных чисел счетно. Тогда его можно занумеровать, и каждая последовательность получит свой номер. Будем обозначать эти последовательности S_n , где $n = 1, 2, 3, \dots$. Будем использовать характеристическую функцию $\varphi_n(p)$, которая показывает, принадлежит ли некоторое натуральное число p последовательности S_n или нет: $\varphi_n(p) = 1$, если $p \in S_n$, и $\varphi_n(p) = 0$, если $p \notin S_n$. Тогда каждой бесконечной последовательности натуральных чисел S_n будет соответствовать бесконечный двоичный вектор φ_n и множество этих векторов, согласно предположению, также можно занумеровать. Составим эту нумерацию и запишем ее в виде таблицы:

	1	2	3	4	...	k	...
φ_1	$\varphi_1(1)$	$\varphi_1(2)$	$\varphi_1(3)$	$\varphi_1(4)$...	$\varphi_1(k)$...
φ_2	$\varphi_2(1)$	$\varphi_2(2)$	$\varphi_2(3)$	$\varphi_2(4)$...	$\varphi_2(k)$...
φ_3	$\varphi_3(1)$	$\varphi_3(2)$	$\varphi_3(3)$	$\varphi_3(4)$...	$\varphi_3(k)$...
...
φ_k	$\varphi_k(1)$	$\varphi_k(2)$	$\varphi_k(3)$	$\varphi_k(4)$...	$\varphi_k(k)$...

Элементами таблицы являются последовательности, составленные из 0 и 1. На диагонали таблицы также находится последовательность нулей и единиц:

$$\varphi_d = \varphi_1(1), \varphi_2(2), \varphi_3(3), \dots, \varphi_k(k), \dots$$

Составим антидиагональную последовательность φ_d' по правилу:

$$\varphi_d'(1) = 1 - \varphi_1(1),$$

$$\varphi_d'(2) = 1 - \varphi_2(2),$$

...

$$\varphi_d'(k) = 1 - \varphi_k(k).$$

Эта последовательность будет отличаться от любой последовательности в таблице хотя бы одним — диагональным элементом. Предположим, что последовательность φ_d' все-таки входит в построенный пересчет, допустим, с номером k . Тогда $\varphi_d' = \varphi_k$, и, согласно правилу, ее элементы:

$$\varphi_d'(1) = \varphi_k(1) = 1 - \varphi_1(1),$$

$$\varphi_d'(2) = \varphi_k(2) = 1 - \varphi_2(2),$$

...

$$\varphi_d'(k) = \varphi_k(k) = 1 - \varphi_k(k).$$

Последнее невозможно. Полученное противоречие доказывает теорему. \simeq

Мы доказали, что множество всех бесконечных двоичных последовательностей несчетно. Согласно замечанию к теореме 4.11, это множество есть не что иное, как множество всех отображений $\varphi: \mathbf{N} \rightarrow \{0, 1\}$, т.е. $\{0, 1\}^{\mathbf{N}}$, и мощность этого множества равна 2^{\aleph_0} . Поскольку каждая бесконечная двоичная последовательность является характеристическим вектором бесконечного подмножества натуральных чисел, т.е., между ними существует биекция, то тем самым доказана несчетность множества всех бесконечных последовательностей натуральных чисел. Но множество всех бесконечных последовательностей натуральных чисел есть не что иное, как множество всех функций, определенных на \mathbf{N} и принимающих значения в \mathbf{N} , т.е. множество всех функциональных отображений $f(n): \mathbf{N} \rightarrow \mathbf{N}$, т.е. $\mathbf{N}^{\mathbf{N}}$, следовательно, мощность этого множества есть $\aleph_0^{\aleph_0}$. Поскольку эти два множества равномощны, мы получаем, что $\aleph_0^{\aleph_0} = 2^{\aleph_0}$.

С другой стороны, множество всех последовательностей натуральных чисел (как конечных, так и бесконечных) есть множество всех подмножеств $\wp(\mathbf{N})$ множества натуральных чисел, мощность которого, согласно замечанию к теореме 4.11, равна 2^{\aleph_0} . Отсюда мы получаем тот же результат: $\aleph_0^{\aleph_0} = 2^{\aleph_0}$.

Метод доказательства несчетности множества, использованный в данной теореме, называется *диагональным методом Кантора*.

Мы доказали несчетность множества $\wp(\mathbf{N})$ с помощью характеристической функции, устанавливающей взаимно однозначное соответствие между последовательностями натуральных чисел и

двоичными векторами. Однако мы могли бы применить диагональный метод непосредственно к последовательностям натуральных чисел. Доказательство следующей теоремы 4.13 еще раз демонстрирует применение этого метода для доказательства несчетности всех действительных чисел из интервала $(0, 1)$, хотя этот результат непосредственно следует из теоремы 4.12. Каждое действительное число из интервала $(0, 1)$ можно рассматривать как бесконечную последовательность натуральных чисел, запись которой начинается с символов 0,... Тем самым устанавливается взаимно однозначное соответствие между этими двумя множествами.

Диагональный метод Кантора имеет и другую формализацию, не использующую непосредственного пересчета элементов множества. Для того, чтобы познакомиться с этим способом, рассмотрим другое доказательство несчетности множества всех бесконечных последовательностей натуральных чисел.

Доказательство (2) теоремы 4.12. Предположим, что множество всех бесконечных последовательностей натуральных чисел счетно. Тогда можно составить список $L = S_0, S_1, \dots, S_k, \dots$, в котором каждая последовательность получит свой номер. Составим теперь еще две последовательности U и U' следующим образом: если $i \in S_i$, то $i \in U$, и если $i \notin S_i$, то $i \in U'$. Таким образом, в U' попадут все те числа $i \in \mathbf{N}$, которые не входят в последовательности S_i с соответствующим номером i . (Например, если число 3 входит в последовательность S_3 , то оно войдет в U , а если не входит, то в U' .) Тогда, по предположению, последовательности U и U' также должны войти в список L с некоторыми номерами. Предположим, что последовательность U' входит в список с номером k : $U' = S_k$. Тогда номер этой последовательности k тоже должен войти либо в U , либо в U' . Однако, если $k \in S_k$, то $k \in U$, следовательно, $k \notin U'$, т.е. $k \notin S_k$, а если $k \notin S_k$, то $k \in U'$, т.е. $k \in S_k$. Полученное противоречие доказывает теорему. \simeq

4.7. Мощность континуума

Теорема 4.13 (Кантора). Множество действительных чисел из интервала $(0, 1)$ несчетно.

Доказательство. Для доказательства воспользуемся диагональным методом Кантора. Будем представлять любое число из интервала $(0, 1)$ в виде бесконечной десятичной дроби. Конечные дроби также представимы в таком виде, например, число 0,5 может быть представлено как 0,4999999...

Предположим, что множество этих чисел счетно. Тогда их можно записать в виде списка. Составим этот список и запишем его в виде таблицы, где представлены десятичные части чисел:

	1	2	3	...	k	...
a_1	a_{11}	a_{12}	a_{13}	...	a_{1k}	...
a_2	a_{21}	a_{22}	a_{23}	...	a_{2k}	...
a_3	a_{31}	a_{32}	a_{33}	...	a_{3k}	...
...
a_k	a_{k1}	a_{k2}	a_{k3}	...	a_{kk}	...
...

Составим теперь бесконечное антидиагональное число $b = b_1 b_2 \dots b_k \dots$ по правилу: i -й разряд числа b_i положим равным $1 + a_{ii}$, если $a_{ii} \neq 9$ и $a_{ii} = 8$ (или любому другому числу, отличному от 9), если $a_{ii} = 9$. Если множество чисел из $(0, 1)$ счетно, то построенное число b должно войти в этот список с каким-либо номером, например, с номером k : $b = a_k$. Но тогда $b_1 = a_{k1} = a_{11} + 1$, $b_2 = a_{k2} = a_{22} + 1$, ..., $b_k = a_{kk} = a_{kk} + 1$, что невозможно. Следовательно, множество действительных чисел из интервала $(0, 1)$ несчетно. \aleph

☞ **Определение 4.3.** Мощность множества $(0, 1)$ называют *мощностью континуума*. Мощность континуума обозначается символом C .

Мощность континуума — это мощность множества действительных чисел \mathbf{R} , т.е. $\text{card } \mathbf{R} = C$, ибо существует биекция $(0, 1) \rightarrow \mathbf{R}$, например, $x \rightarrow \log x / (1 - x)$.

* Примеры.

1. В предыдущем разделе мы доказали, что множество алгебраических вещественных чисел счетно. Вещественные числа, не являющиеся алгебраическими, называются *трансцендентными*. (Трансцендентными являются числа e и π .) Поскольку множество алгебраических чисел счетно, а множество вещественных чисел несчетно, то существуют трансцендентные числа и даже «большинство» вещественных чисел трансцендентно.

2. Множество всех точек \mathbf{R}^n с рациональными или алгебраическими координатами счетно, так как его кардинальное число равно $\aleph_0^n = \aleph_0$, а множество всех точек \mathbf{R}^n с вещественными координатами несчетно и равно континууму.

Теорема 4.14. Имеют место равенства:

$$m \cdot C = \aleph_0 \cdot C = C \cdot C = C^m = C^{\aleph_0} = C, \text{ где } m \geq 1 \text{ — целое.}$$

Доказательство. Все эти кардинальные числа не больше C^{\aleph_0} и не меньше C , поэтому достаточно показать, что $C^{\aleph_0} = C$.

$$\text{Действительно, } C^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0} = C.$$

Однако, факт: $2^{\aleph_0} = C$ — требует доказательства.

Если взять числа из $E = (0, 1)$, такие, что в их изображении присутствуют числа $0, 1, 2, \dots, 7$, то это множество будет равномощно множеству $\{0, 1, 2, 3, 4, 5, 6, 7\}^{\aleph}$, следовательно, его мощность равна 8^{\aleph_0} . Само множество E имеет мощность $\leq 10^{\aleph_0}$ (мы пишем \leq из-за двоякого десятичного изображения чисел). Поэтому $8^{\aleph_0} \leq \text{card } E \leq 10^{\aleph_0}$, откуда $2^{\aleph_0} \leq \text{card } E \leq 16^{\aleph_0} = (2^4)^{\aleph_0} = 2^{4\aleph_0} = 2^{\aleph_0}$, следовательно $\text{card } E = 2^{\aleph_0}$. С другой стороны, $\text{card } E = C$. Следовательно, $2^{\aleph_0} = C$. \aleph

Следствие 1. Множество комплексных чисел имеет мощность континуума (поскольку оно равномощно \mathbf{R}^2 : $C^2 = C$).

Следствие 2. Любое векторное пространство конечного числа измерений n над полем вещественных или комплексных чисел имеет мощность континуума.

Следствие 3. Множество всех последовательностей вещественных чисел и последовательностей комплексных чисел имеет мощность континуума, ибо их кардинальное число равно $C^{\aleph_0} = C$.

Следствие 4. Множество E непрерывных вещественных функций вещественной переменной имеет мощность континуума. Каждой такой функции можно поставить в соответствие последовательность вещественных чисел — значений функции в точках с рациональными абсциссами. Можно считать, что эти точки взаимно однозначны с \mathbf{N} , так как \mathbf{Q} счетно. Последовательность вещественных чисел, соответствующая непрерывной функции, ее полностью определяет. Следовательно, существует биекция множества непрерывных функций на часть множества последовательностей вещественных чисел. Значит, это множество E имеет мощность, не большую C . А так как это отображение, которое каждой непрерывной функции ставит в соответствие ее значение в одной точке, например, в начале координат, является сюръекцией E на \mathbf{R} , то E имеет мощность, не меньшую мощности континуума. Следовательно, E имеет мощность C .

Следствие 5. Множество всех вещественных функций вещественной переменной имеет мощность, строго большую мощности континуума, ибо его мощность равна C^C (а если со значениями 0 и 1 — то 2^C), а $C^C = (2^{\aleph_0})^C = 2^{\aleph_0^C} = 2^C > C$. Таким образом, большинство функций имеет не менее одной точки разрыва.

4.8. Континуум-гипотеза

При исследовании мощностей бесконечных множеств был установлен тот факт, что множество кардинальных чисел линейно упорядочено. Линейная упорядоченность означает, что для каждого кардинального числа существует непосредственно следующее за ним число. \aleph_0 является наименьшим трансфинитным числом. Однако ничего не известно о том, какое трансфинитное число является следующим за \aleph_0 . Существует лишь предположение, которое называется *континуум-гипотезой*.

Континуум-гипотеза. Кардинальное число 2^{\aleph_0} непосредственно следует за \aleph_0 .

Это означает, что $\aleph_0 < 2^{\aleph_0}$ и между ними нет никакого другого кардинального числа. Этот факт требует доказательства. Мы ничего не знаем о множествах, которые несчетны, но менее, чем континуальны, не знаем даже, существуют ли такие множества. Отсутствие примеров подобных множеств не является доказательством невозможности их существования, поэтому утверждение о *непосредственном следовании* 2^{\aleph_0} за \aleph_0 является гипотезой, а не теоремой.

Можно пойти дальше и сформулировать более общее утверждение.

Обобщенная континуум-гипотеза заключается в предположении о том, что для любого кардинального числа α кардинальное число 2^α непосредственно следует за α . Отсюда следует, что последовательность кардинальных чисел неограниченна: $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$

Действительно, 2^{\aleph_0} есть мощность множества-степени $\wp(N)$ (вместо N может быть любое другое бесконечное счетное множества). Но из этого множества можно образовать опять множество

всех его подмножеств $\wp(\wp(N))$, мощность которого есть $2^{2^{\aleph_0}}$, и этот процесс можно продолжать до бесконечности. Отсюда следует, что не существует наибольшего трансфинитного числа.

Попытки доказать континуум-гипотезу в качестве теоремы были безуспешны, а 1963 г. П. Коэн (см. [Коэн, 1973]) доказал, что континуум-гипотеза неразрешима — ее невозможно ни доказать, ни опровергнуть, можно лишь принять ее или противоположное ей утверждение в качестве аксиомы.

4.9. Парадоксы теории множеств

Канторовскую теорию множеств в том виде, как мы с ней познакомились, называют «*наивной*» теорией множеств. Канторовское понятие множества отсылает нас к нашей интуиции при решении вопроса о том, какие объекты считать множествами. Попытки построить теорию множеств на интуитивной основе, при которой отсутствует четкое математическое определение множества, привели к возникновению парадоксов.

Один из первых парадоксов теории множеств был открыт самим Кантором в 1899 году.

Из теоремы Кантора (4.10) следует, что каково бы ни было трансфинитное число, существует большее трансфинитное число, и что наибольшего трансфинитного числа не существует. Однако, определение понятия множества не накладывает никаких ограничений на рассматриваемые множества. Можно рассмотреть универ-

сальное множество, элементами которого являются все *возможные множества*. Очевидно, что такое *множество всех множеств* содержит больше элементов, чем любое другое множество. Но если это так, то как тогда может существовать трансфинитное число, большее трансфинитного числа, которое соответствует этому множеству?

Парадокс Бертрانا Рассела был открыт в 1902 году и связан с одним лишь определением понятия множества. Эти парадоксы, а также другие, например, парадокс Бурали-Форти (1897 г.), связанный с теорией *порядковых* чисел, называют *логическими* парадоксами. Другую группу парадоксов условно называют *семантическими*.

В 1905 году был открыт парадокс Ришара, который можно сформулировать следующим образом. Рассмотрим конечный алфавит, состоящий из 33 букв русского алфавита и двух разделительных символов: пробела и запятой. Будем понимать под «фразой» конечную последовательность букв, включающую пробел или запятую в середине последовательности в качестве разделителей. Каждую такую последовательность можно рассматривать как число в 35-ричной системе счисления. Некоторые такие фразы являются описаниями одноместных арифметических функций на естественном языке, например, «а в квадрате», «модуль корня квадратного из а». Из множества всех последовательностей вычеркнем фразы, не являющиеся описаниями функций. В результате мы можем получить последовательность P_0, P_1, P_2, \dots всех таких описаний. Обозначим функции, описываемые этими фразами, через $f_0(a), f_1(a), f_2(a), \dots$.

Рассмотрим теперь фразу P , описывающую функцию $f(a) = f_a(a) + 1$: «Функция, значение которой для любого аргумента a , являющегося натуральным числом, равно увеличенному на единицу значению для этого же аргумента той функции, которая определяется фразой, соответствующей в пересчете P_0, P_1, P_2, \dots этому натуральному числу». Эта фраза тоже описывает арифметическую функцию, следовательно, P входит в пересчет P_0, P_1, P_2, \dots с некоторым номером, например, k . Тогда $f(a) = f_k(a)$. Подставляя k вместо a , получим $f(k) = f_k(k)$, однако, по определению этой функции, $f(k) = f_k(k) + 1$, что невозможно.

Этот парадокс связан с тем, что множество фраз данного языка является счетно-бесконечным, и, следовательно, множество определенных выше функций также является счетно-бесконечным, в то время, как множество всех арифметических функций несчетно (см. теорему 4.12).

Похожий парадокс предложил Берри. Рассмотрим выражение: «Наименьшее натуральное число, которое нельзя назвать посредством меньше, чем тридцати трех слогов». Это выражение называет некоторое натуральное число. Тогда, согласно этому определению, это число нельзя назвать посредством менее, чем 33 слогов. Но данное выражение определяет это число, причем с помощью ровно 32 слогов!

Эти парадоксы родственны известным еще в древности семантическим парадоксам. Древнегреческому философу с острова Крит Эпимениду (VI до н.э.) приписывается высказывание: «Все критяне — лжецы». Учитывая, что сам Эпименид является критянином, невозможно сказать, истинно это утверждение или ложно. Другой философ, Эвбулид (VI до н.э.), тот же парадокс сформулировал таким образом: «То, что я сейчас говорю, — ложь» («Я лгу»). Этот парадокс известен как парадокс «лжеца», для которого существует множество модификаций.

В древней «дилемме крокодила» крокодил украл ребенка, но обещал вернуть его отцу, если тот угадает, вернет ли ему крокодил ребенка. Неразрешимая дилемма встает перед крокодилом, если отец скажет ему, что он не вернет ребенка.

Миссионер, попавший к людоедам, может произнести какую-нибудь фразу, и, если она окажется истинной, то его сварят, а если ложной, то зажарят. Что должен сказать миссионер, чтобы остаться живым?

Открытие парадоксов в канторовской теории множеств ставило под сомнение последние достижения в области математики и привело к кризису основ математики¹. К этому времени большинство разделов математики уже использовали теоретико-множественные

¹ История математики уже знала подобные кризисы. Первый кризис основ математики произошел в V веке до н.э. Он был вызван неожиданным открытием: оказалось, что не все однородные геометрические величины соизмеримы друг с другом. Было, например, показано, что диагональ квадрата не соизмерима с его стороной. Это нанесло громадный ущерб учению Пифагора о величинах, которое полагалось на соизмеримость однородных геометрических величин. Пифагорова теория была отброшена как необоснованная. Первый кризис преодолевался нелегко. Конец кризиса относится к 370 г. до н.э. и связан с именем выдающегося математика Евдокла — построенная им теория величин и учение о несоизмеримостях в основном совпадает с современной теорией иррациональных чисел, построенной Рихардом Дедекиндом в 1872 г. Этот кризис сыграл выдающуюся роль в становлении математического метода. Открытия Ньютона и Лейбница, зарождение анализа в конце XVII в. привело ко второму кризису основ математики. Последователи Ньютона и Лейбница, увлеченные огромными практическими возможностями и силой своего метода, мало заботились о прочности фундамента, на котором был построен анализ, так что не доказательства гарантировали правильность результатов, а наоборот, справедливость результатов давала уверенность в правильности доказательств. С течением времени парадоксы и противоречия возникали все в большем количестве, пока кризис основ математики не стал для всех очевидной реальностью. Наконец, в начале XIX в. Коши отбросил туманную теорию бесконечно малых и заменил ее строгой теорией пределов. Вслед за ним Вейерштрасс осуществил так называемую арифметизацию анализа, и второй кризис основ математики был преодолен.

понятия. Теория множеств легла в основу новой науки — формальной (математической) логики, которая в конце XIX-го — начале XX-го века бурно развивалась. Опубликованные в 1879 — 1903 г.г. работы немецкого ученого Готлиба Фреге и исследования итальянского математика Пеано положили начало новым направлениям в математической логике. Пеано хотел построить математику на базе логического исчисления, а Фреге работал над логическим обоснованием математической науки. Первая часть его труда «Основания арифметики» появилась в 1903 г., и в это же время произошло одно из самых трагических событий в истории математики. Бертран Рассел сообщил о своем парадоксе Фреге, который перед этим только что закончил последний том своего громадного трактата по основаниям арифметики. В конце второго тома Фреге подтвердил получение этого сообщения: «Закончив свой труд, ученый обнаруживает несостоятельность исходных позиций — вряд ли можно придумать что-нибудь более нежелательное. Именно в этом положении оказался я после получения письма мистера Бертрана Рассела, когда рукопись была почти готова к набору.» Этими словами Фреге закончил свой двенадцатилетний труд.

Поскольку теория множеств была положена в основу математики, обнаруженные парадоксы поставили под сомнение достоверность всей математической науки в целом. Выход из этого кризиса был длительным и трудным.

При внимательном рассмотрении логических парадоксов теории множеств можно заметить, что они имеют ряд общих свойств, связанных с самим определением множества. Во-первых, они допускают существование «слишком больших» множеств, таких как «множество всех множеств» в парадоксе Кантора; во-вторых, они допускают *импредикативные* определения множеств, т.е. такие определения, в которых фигурирует какое-то множество S и элемент x из S , определение которого зависит от S . Такие определения являются в известном смысле круговыми: определяемое понятие зависит само от себя. Можно было бы запретить использование таких определений, однако исключить их полностью из математики нельзя. Примером такого определения является определение *точной верхней грани* упорядоченного множества — это наименьший элемент множества всех верхних граней данного множества.

4.10. Преодоление парадоксов

Для выхода из создавшегося положения было предложено построить строгое аксиоматическое определение понятия множества и ограничиться рассмотрением множеств, удовлетворяющих этим аксиомам. Эти аксиомы сформулированы так, что из них не выводи-

мы известные парадоксы и, в то же время, они достаточны для вывода основных предложений классической математики, в том числе и абстрактной теории множеств. Такая система аксиом была предложена 1908 г. Цермело, а затем усовершенствованна Френкелем, Сколемом, фон Нейманом, Бернайсом. В качестве примера ниже приводится одна из наиболее известных аксиоматических систем — система аксиом Цермело—Френкеля (см. [Клини, 1973]).

Система аксиом Цермело—Френкеля.

1. Аксиома объемности.

Два множества A и B равны, если и только если они состоят из одних и тех же элементов: $A = B \equiv (A \subseteq B \ \& \ B \subseteq A)$.

2. Аксиома выделения.

Для любого множества A и предиката $P(x)$, такого, что для любого $x \in A$ $P(x)$ либо истинно, либо ложно, существует множество $X = \{x \mid x \in A \ \& \ P(x)\}$, состоящее в точности из тех элементов A , для которых $P(x)$ истинно.

3. Аксиома пары.

Если a и b — различные объекты, то существует множество $\{a, b\}$, состоящее в точности из a и b .

4. Аксиома объединения.

Для любого множества множеств A существует объединение всех множеств, состоящее в точности из всех элементов, которые принадлежат элементам множества A .

5. Аксиома бесконечности.

Существует по крайней мере одно бесконечное множество — множество натуральных чисел $\{0, 1, 2, \dots\}$.

6. Аксиома множества-степени.

Для любого множества A существует множество 2^A всех подмножеств A .

7. Аксиома выбора.

Для любого непустого множества S попарно непересекающихся множеств существует некоторое множество A , содержащее в качестве своих элементов ровно по одному элементу из каждого элемента множества S .

8. Аксиома подстановки.

Для каждого множества A и однозначной функции f , определенной на A , существует множество, содержащее в точности объекты $f(x)$ для $x \in A$.

Система аксиом теории множеств ограничивает множество объектов, которые можно считать множествами. Так, интуитивный принцип абстракции, согласно которому для любого свойства $P(x)$ существует соответствующее множество всех элементов x , обладающих этим свойством, заменен более строгой аксиомой выделения, требующей определенности предиката $P(x)$ — он должен быть либо истинен, либо ложен. Тогда парадокс Рассела доказывает, что не существует множества всех множеств, которые не принадлежат самим себе в качестве элемента. Парадокс Кантора показывает, что не существует универсального множества — множества всех множеств.

В некоторых других системах аксиом теории множеств, например, в системе Гёделя (см. [Мендельсон, 1976]), все совокупности объектов делятся на два вида: *множества* и *классы*. Все множества могут входить как элементы в другие совокупности, как во множества, так и в классы. Классы могут быть или не быть множествами. Классы, которые не являются множествами, называются *собственными* классами. Совокупность всех множеств образует класс. Парадокс Кантора устраняется тем обстоятельством, что этот класс уже не является множеством, — он является собственным классом. Аналогично устраняется и парадокс Рассела: из системы аксиом выводимо предложение о том, что совокупность, определенная таким образом, что она содержит все множества, не являющиеся элементами самих себя, не является множеством, — она является собственным классом.

Не все, однако, обстояло гладко с аксиоматической теорией множеств. Аксиома выбора, введенная Цермело, явилась предметом многочисленных исследований и споров, суть которых сводилась к вопросу, принимать или не принимать ее в качестве допущения, которое можно без противоречий присоединить к другим аксиомам теории множеств, при условии, что эти аксиомы непротиворечивы. В 1963 году Коэн показал, что можно без противоречия присоединить к аксиоматике теории множеств и отрицание аксиомы выбора.

Однако из аксиомы выбора Цермело следуют некоторые вызывающие сомнения выводы. В частности, из нее следует, что любое множество можно вполне упорядочить. Поясним, что *вполне упорядоченное множество* — это линейно упорядоченное множество, т.е. *цепь*, в котором каждое непустое подмножество имеет наименьший элемент. Любая конечная цепь вполне упорядочена, например, конечное подмножество натуральных чисел. Множество натуральных чисел \mathbf{N} вполне упорядочено отношением «меньше»: оно имеет наименьший элемент, является цепью и любое его подмножество также вполне упорядочено. Отношение «меньше» на множестве

неотрицательных рациональных чисел является линейным порядком, но не является вполне упорядочением,— это множество не имеет наименьшего элемента. Аналогично, множество целых чисел линейно упорядочено отношением «меньше», но не вполне упорядочено, так как не имеет наименьшего элемента.

Аксиома выбора эквивалентна *принципу полного упорядочения*, согласно которому всякое множество может быть вполне упорядочено. Например, пересчет, построенный нами при доказательстве счетности множества неотрицательных рациональных чисел, вполне упорядочивает это множество (не по величине чисел, а в порядке их пересчета). Однако по вопросу о законности этого принципа возникла серьезная полемика. Например, Биркгоф пишет: «Это ведет к весьма специфическому заключению о том, что **R** можно вполне упорядочить, а это, по-видимому, невозможно сделать в каком-нибудь конструктивном смысле... Никому до сих пор не удалось «построить» какую-нибудь явно заданную функцию, которая бы вполне упорядочивала несчетное множество; мы совершенно не представляем себе, как «выглядит» несчетное вполне упорядоченное множество. Проблема «конструктивного» вполне упорядочения несчетного множества является основной проблемой теории множеств.» [Биркгоф, 1984. С. 172—273].

Глава 5.

ОТНОШЕНИЕ ПОРЯДКА

5.1. Основные определения

↪ **Определение 5.1.** Отношение на множестве P , удовлетворяющее свойствам

рефлексивности: $x \leq x$ для всех x ,

P1.

антисимметричности:

если $x \leq y$ и $y \leq x$, то $x = y$ для всех x, y ,

P2.

транзитивности:

если $x \leq y$ и $y \leq z$, то $x \leq z$ для всех x, y, z

P3.

называется *отношением порядка*.

Свойства, которым удовлетворяет это отношение, приводит к понятию упорядоченного множества.

↪ **Определение 5.2.** Непустое множество P , на котором задано бинарное отношение порядка, удовлетворяющее свойствам **P1**, **P2**, **P3**, называется *частично упорядоченным множеством*.

Отношение порядка ρ условимся обозначать символом \leq , хотя далеко не всегда этот символ будет обозначать отношение «меньше или равно», определенное на множестве чисел. Запись $x \geq y$ будет означать, что $y \leq x$. Поскольку свойства **P1**, **P2**, **P3** задают наиболее общий тип порядка, частично упорядоченное множество называют просто *упорядоченным*, или u -множеством, в отличие от линейно и строго упорядоченных множеств, которые будут определены ниже. Упорядоченное множество P часто обозначают в виде двойки $\langle P, \leq \rangle$. Одноэлементное множество считается u -множеством.

Если $\langle P, \leq \rangle$ — u -множество и $a, b \in P$, то a и b называются *сравнимыми* элементами, если $a \leq b$ или $b \leq a$. В противном случае они называются *несравнимыми*. Несравнимые элементы будем обозначать $a \parallel b$. В частично упорядоченном множестве есть как сравнимые, так и несравнимые элементы.

↪ **Определение 5.3.** Если $x \leq y$ и $x \neq y$, то отношение называется отношением *строгого порядка* и обозначается $x < y$.

Отношение строгого порядка не является рефлексивным: в любом строго упорядоченном множестве ни для какого x не имеет места соотношение $x < x$. Для отношения $<$ выполним свойство *асимметричности*: если $x < y$, то не выполняется $y < x$. Во всех случаях, когда различие между строгим и нестрогим порядком не имеет принципиального значения, мы будем пользоваться обозначением \leq .

↪ **Определение 5.4.** U -множество $\langle P, \leq \rangle$, удовлетворяющее свойству линейности:

$x \leq y$ или $y \leq x$ для всех $x, y \in P$,
называется *линейно упорядоченным множеством*, или *цепью*. **Р4.**

В цепи каждые два произвольно взятые элемента сравнимы и нет несравнимых элементов. У-множество, являющееся цепью, можно записать в виде: $x_1 \leq x_2 \leq \dots \leq x_n$.

У-множество, в котором все элементы несравнимы, иногда называют *антицепью*.

Свойство *ацикличности* порядка: если $x_1 \leq x_2 \leq \dots \leq x_n \leq x_1$, то $x_1 = x_2 = \dots = x_n$, — непосредственно следует из свойств транзитивности и антисимметричности.

Цепью C в у-множестве P называется такое его непустое подмножество, которое как у-множество является цепью. Цепь $x_1 \leq x_2 \leq \dots \leq x_n$ в у-множестве P называется *максимальной цепью*, если в ней отсутствуют транзитивно замыкающие дуги. Это означает, что если $x_i \leq x_j$, то ни для каких x_i, x_j не существует такого y , что $x_i \leq y \leq x_j$.

* Примеры.

1. Отношение включения $x \subseteq y$, т.е. « x — подмножество y », заданное на множестве всех подмножеств некоторого множества U , есть отношение частичного порядка. Действительно, это отношение рефлексивно: $x \subseteq x$, антисимметрично: если $x \subseteq y$ и $y \subseteq x$, то $x = y$, и транзитивно: если $x \subseteq y$ и $y \subseteq z$, то $x \subseteq z$. Пусть дано множество $A = \{a, b, c\}$. Множество-степень $\langle \wp(A), \subseteq \rangle$ — частично упорядоченное множество. Подмножество $\emptyset \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$ является максимальной цепью в $\langle \wp(A), \subseteq \rangle$. Подмножество $\emptyset \subseteq \{a, b\} \subseteq \{a, b, c\}$ также является цепью, но не максимальной.

2. На числовых множествах N, Z, Q, R установлены отношения порядка \leq (меньше либо равно), $<$ (меньше), \geq (больше либо равно), $>$ (больше). Эти отношения являются отношениями линейного порядка, поэтому эти множества, а также любые их подмножества являются цепями. Например, множество $\{1, 2, 3, 4\}$ — цепь.

3. Отношение « x — предок y », определенное на множестве всех людей, есть отношение порядка. Это отношение строгого порядка, так как оно не рефлексивно (никакой человек не является предком самого себя); это отношение частичного порядка, так в нем есть несравнимые элементы: не каждые два человека находятся в отношении родства.

4. Множество символов русского алфавита $A = \{a, б, в, \dots, я\}$ — цепь. В этом множестве отношение \leq можно читать как «предшествует»: a предшествует $б$, $б$ предшествует $в$, и так далее. Тогда a , как первая буква алфавита, предшествует всем остальным, т.е.

$\forall x \in A$ ($a \leq x$), а буква $я$, последняя буква в алфавите, «больше» всех остальных, т.е. $\forall x \in A$ ($x \leq я$).

5. На множестве целых положительных чисел Z^+ можно задать отношение порядка, такое, что $x \leq y$ означает: « x делится на y ». Его можно определить как $x/y = k$, где $k \in N$. Это отношение рефлексивно: $x/x = 1$, и $1 \in N$; антисимметрично: если $x/y = k$ и $y/x = k$, то $x/y = y/x$, — отсюда $x = y$; транзитивно: если $x/y = k_1$ и $y/z = k_2$, то $x/z = k_3$, где $k_1, k_2, k_3 \in N$. Действительно, если $x = k_1 y$ и $y = k_2 z$, то $x = k_1 k_2 z$, т.е. $x = k_3 z$, где $k_3 = k_1 k_2$. Совершенно очевидно, что не всякие два целые числа $x, y \in Z^+$ находятся в отношении порядка « x делится на y », следовательно, это отношение частичного порядка. Таким образом, множество Z^+ является линейно упорядоченным множеством по отношению \leq (меньше или равно), и является частично упорядоченным по отношению « x делится на y ».

5.2. Свойства у-множеств

↪ **Определение 5.5.** Порядком $n(P)$ у-множества P называется (кардинальное) число его элементов. Если это число конечно, P называется *конечным* у-множеством.

↪ **Определение 5.6.** Если в у-множестве P существует единственный элемент $a \in P$, такой что $\forall x \in P$ ($a \leq x$), то a называется *наименьшим элементом* у-множества.

Можно показать, что у-множество P может содержать только один наименьший элемент a . Это следует из определения: элемент a таков, что все остальные элементы множества P «больше» a . Поэтому, если предположить, что a и b — два наименьших элемента, то $a \leq b$, и, одновременно, $b \leq a$, откуда следует, что $a = b$, т.е. это один и тот же элемент. Следовательно, наименьший элемент у-множества, если он существует, всегда *единственный*. Его называют *нулем* у-множества и обозначают символом 0 .

↪ **Определение 5.7.** Если в у-множестве P существует единственный элемент $b \in P$, такой что $\forall x \in P$ ($x \leq b$), то b называется *наибольшим элементом* у-множества.

Наибольший элемент у-множества P , если он существует, также всегда единственный. Его обозначают символом 1 и называют *единицей* у-множества.

↪ **Определение 5.8.** У-множество P , в котором существуют наибольший и наименьший элементы, называют *упорядоченным множеством с нулем и единицей*. Тогда $\forall x \in P$ ($0 \leq x \leq 1$), т.е. любой другой элемент у-множества лежит между *нулем* и *единицей*, поэтому элементы 0 и 1 , если они существуют, называются *универсальными гранями множества P*.

Может показаться, что наименьший и наибольший элементы существуют в любом u -множестве. Однако это не так.

Рассмотрим множество $A = \{2, 3, 6, 12, 24\}$ с определенным на нем отношением порядка $x \leq y$: « x делит y », например, 2 делит 6, 12, 24; 3 делит 6, 12, 24; 6 делит 12, 24, и т.д. В этом множестве наименьший элемент, если он существует, должен делить **все** следующие за ним числа. Однако этим свойством не обладают ни 2, ни 3, которые **не сравнимы** между собой по отношению x делит y , и ни одно из них не является наименьшим, так как **не все** числа «больше» 2 (или 3) по данному отношению (2 не делит 3 и 3 не делит 2). Поэтому в этом множестве нет наименьшего элемента. Однако числа 2 и 3 обладают тем свойством, что **никакое** другое число не меньше их по данному отношению, т.е. ни одно другое число не делит 2 и 3. Такие элементы, которые *меньше* всех остальных элементов u -множества, являются *минимальными* в u -множестве.

☞ **Определение 5.9.** Минимальным элементом u -множества P называется такой элемент $a \in P$, что ни для какого $x \in P$ не выполняется условие $x \leq a$.

☞ **Определение 5.10.** Максимальным элементом u -множества P называется такой элемент $b \in P$, что ни для какого $x \in P$ не выполняется условие $b \leq x$.

Нетрудно показать, что наименьший элемент всегда является минимальным в u -множестве, а наибольший — максимальным, но обратное выполнимо далеко не всегда. В рассмотренном выше примере число 24 является наибольшим элементом, так как оно делится на все предшествующие числа, и, в то же самое время, максимальным, а числа 2 и 3 являются минимальными, в то время, как наименьшего числа в этом u -множестве не существует. Данное множество не является также и цепью, так как оно содержит *несравнимые* элементы 2 и 3.

Рассмотрим произвольное u -множество P . Пусть S есть подмножество P . Тогда, если $x \leq y$ для $x, y \in S$, то $x \leq y$ в P . Поскольку свойства **P1** — **P3** выполняются в P , то они выполняются и в S . Если в P выполняется и **P4**, то оно выполняется и в S . Отсюда приходим к следующему заключению.

Теорема 5.1. Всякое подмножество S u -множества P само является u -множеством относительно того же самого порядка (ограниченного на S). В частности, любое подмножество цепи является цепью.

Теорема 5.2. Любое конечное непустое подмножество X произвольного u -множества P имеет минимальные и максимальные элементы.

Доказательство. Пусть $X = \{x_1, \dots, x_n\}$. Положим $m_1 = x_1$, а $m_k = x_k$, если $x_k < m_{k-1}$, и $m_k = m_{k-1}$ в противном случае. Тогда элемент m_n будет минимальным. Аналогично можно доказать существование в X максимального элемента.

В любой конечной цепи понятия наименьшего и минимального (наибольшего и максимального) элемента совпадают. Таким образом, любая конечная цепь содержит наименьший (первый) и наибольший (последний) элементы. \asymp

Множество натуральных чисел $\{1, 2, \dots, n\}$ образует цепь n (ординальное число n) в своей естественной упорядоченности.

☞ **Определение 5.11.** Подмножество X множества P называют *ограниченным*, или *интервалом*, если $\forall a, b \in P \forall x \in X (a \leq x \leq b)$.

5.3. Диаграммы u -множеств

Граф отношения порядка, построенный по его матрице, будет содержать большое число транзитивно замыкающих дуг. Поэтому он будет выглядеть слишком сложным (см., например, рис. 5.2, б). Для отношения порядка обычно строится диаграмма Хассе, которая отображает *отношение покрываемости*.

☞ **Определение 5.12.** В упорядоченном множестве с отношением порядка \leq элемент b *покрывает* a , если $a < b$ и не существует такого элемента x , чтобы $a < x < b$.

✱ **Пример.**

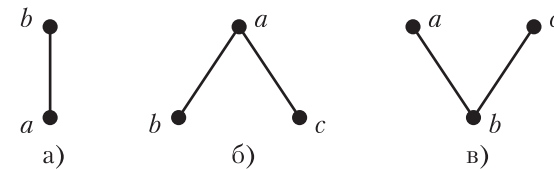


Рис. 5.1.

а) b покрывает a ; б) a покрывает b и c ; в) a, c покрывают b .

Тогда u -множество можно изобразить в виде графа. Принято граф u -множества строить снизу вверх: если элемент b покрывает элемент a , то он располагается выше элемента a и соединяется с ним прямой. Несравнимые элементы располагаются на одном уровне. Полученный граф называется *диаграммой* u -множества, или *диаграммой Хассе* (см. рис. 5.1). Граф отношения покрываемости не содержит транзитивно замыкающих дуг и петель, отражающих рефлексивность отношения, поэтому диаграмма u -множества P может быть получена из ориентированного графа отношения

порядка $x \leq y$, где $x, y \in P$, удалением петель и транзитивно замыкающих дуг. Примеры диаграмм Хассе приведены на рис. 5.2.

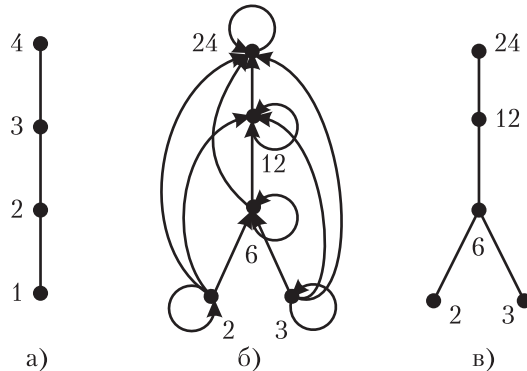


Рис. 5.2. Примеры диаграмм Хассе:

- а) — линейно упорядоченное множество (цепь);
 б) — граф отношения « x делит y »;
 в) — диаграмма Хассе множества, упорядоченного отношением « x делит y ».

Если два элемента $a, b \in P$ находятся в отношении порядка $a \leq b$, то на диаграмме существует путь из a в b . Таким образом, любое конечное u -множество с точностью до изоморфизма определяется своей диаграммой.

* Пример.

Продолжая предыдущий пример, рассмотрим диаграмму Хассе для множества $A = \{2, 3, 6, 12, 24\}$ с отношением « x делит y » (рис. 5.2, в). Эта диаграмма получена удалением кольцевых и транзитивно замыкающих дуг на ориентированном графе (рис. 5.2, б). Мы видим, что каждый вышележащий элемент на диаграмме «больше» всех, лежащих ниже его. Таким образом, нет необходимости стрелками указывать отношение порядка между элементами: это легко определить по уровню, который занимает каждый элемент на диаграмме Хассе. Поэтому диаграмма Хассе обычно изображается без стрелок.

↪ **Определение 5.13.** Элемент u называется *нижней гранью* элементов a и b , если $u \leq a$ и $u \leq b$.

↪ **Определение 5.14.** Элемент v называют *верхней гранью* элементов a и b , если $a \leq v$ и $b \leq v$.

У двух элементов может быть несколько нижних и верхних граней, что хорошо видно на диаграммах Хассе: это все элементы,

расположенные ниже (для верхних граней — выше) обоих элементов.

↪ **Определение 5.15.** Элемент x называется *наибольшей нижней гранью* (точной нижней гранью) элементов a и b , если он является их нижней гранью и для любой нижней грани u $u \leq x$. Обозначается $x = \inf\{a, b\}$ ($\inf\{a, b\}$).

↪ **Определение 5.16.** Элемент y называется *наименьшей верхней гранью* (точной верхней гранью) элементов a и b , если он является верхней гранью a и b и для любой верхней грани v $y \leq v$. Обозначается $y = \sup\{a, b\}$ ($\sup\{a, b\}$).

* Примеры.

1. Рассмотрим множество, представленное диаграммой Хассе на рис. 5.3. Для элементов d, e нижними гранями будут элементы b , так как $b \leq d, b \leq e$, и a , так как $a \leq d$ и $a \leq e$, однако, $a \leq b$, следовательно, b является наибольшей нижней гранью. Для элементов e и c $c \leq e, a \leq e, a \leq c$, поэтому a и c — нижние грани элементов e и c , но $a \leq c$, следовательно, $c = \inf\{e, c\}$ — наибольшая нижняя грань. Аналогично определяются и точные верхние грани: $\sup\{b, c\} = e, \sup\{d, e\} = f, \sup\{e, c\} = e$.

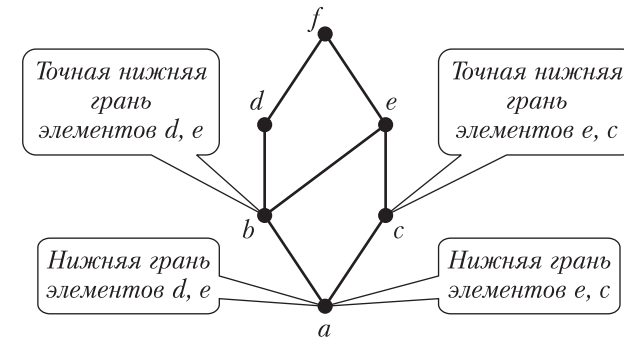


Рис. 5.3. Точные нижние грани

2. Рассмотрим множество на рис. 5.4. Для элементов d, e нижними гранями будут элементы: b ($b \leq d, b \leq e$), c ($c \leq d, c \leq e$), и a ($a \leq d$ и $a \leq e$), при этом $a \leq b$ и $a \leq c$, однако, $c \parallel b$ (несравнимы), следовательно, ни b , ни c не является наибольшей нижней гранью. Точной нижней гранью элементов b и c будет элемент a . Аналогично, для элементов b, c не существует точной верхней грани. Таким образом, в данном u -множестве не для всяких двух элементов существует точная нижняя и точная верхняя грани.

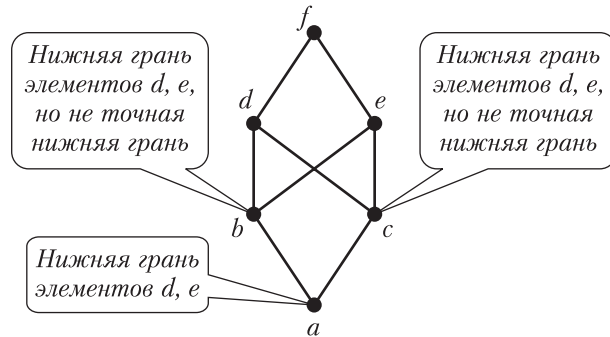
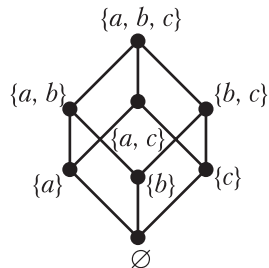
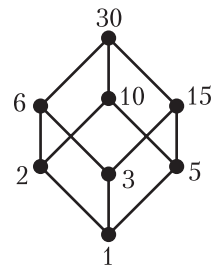


Рис. 5.4. У-множество, не являющееся решеткой.

⇨ **Определение 5.17.** Упорядоченные множества, в которых для каждого двух элементов существует точная верхняя и точная нижняя грани, называются *решетками*.

Таким образом, множество на рис. 5.3 является решеткой, а множество на рис. 5.4 — у-множество, но не решетка.

3. Рассмотрим множество всех подмножеств множества $A = \{a, b, c\}$: $\wp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Это множество упорядочено отношением включения и его можно представить на диаграмме Хассе (рис. 5.5). Здесь точной нижней гранью подмножеств является их теоретико-множественное пересечение, например для $\{a\}$ и $\{b\}$ это \emptyset : $\{a\} \cap \{b\} = \emptyset$; для $\{a, b\}$ и $\{b, c\}$ это $\{b\}$ и т. д. Точной верхней гранью двух подмножеств является их теоретико-множественное объединение, например, для $\{a\}$ и $\{b\}$ — это $\{a, b\}$, для $\{a, b\}$ и $\{b, c\}$ — это $\{a, b, c\}$ и т.д.

Рис. 5.5.
Диаграмма $\wp(A)$ Рис. 5.6.
Диаграмма у-множества
с отношением « x — делитель y ».

Глядя на диаграмму $\wp(A)$, можно сделать вывод, что в интерпретации теории множеств операции $\sup \{x, y\}$ соответствует операция объединения, а операции $\inf \{x, y\}$ — пересечения. Эта аналогия послужила основанием для выбора наименования операции нахождения точной верхней грани — «объединение» (обозначается \vee) и точной нижней грани — «пересечение» (обозначается \wedge) в теории решеток. Таким образом обозначения $\inf \{x, y\}$ и $x \wedge y$, $\sup \{x, y\}$ и $x \vee y$ равнозначны.

4. Множество $X = \{1, 2, 3, 5, 6, 10, 15, 30\}$ с заданным на нем отношением « x — делитель y » (рис. 5.6) образует решетку, в которой операции нахождения точной нижней грани x и y соответствует нахождение НОД (x, y) (наибольший общий делитель), а операции нахождения точной верхней грани x и y соответствует нахождение НОК (x, y) (наименьшее общее кратное).

5.4. Изоморфизм. Двойственность

⇨ **Определение 5.18.** Функция $\phi: P \rightarrow Q$, заданная на у-множестве P и принимающая значения в у-множестве Q , называется *сохраняющей порядок*, или *изотонной*, если из $x \leq y$ следует, что $\phi(x) \leq \phi(y)$.

Например, если $P = \{1, 2, 3\}$, такое что $1 \leq 2 \leq 3$, и $Q = \{a, b, c\}$, такое что $a \leq b \leq c$, то отображение $\phi(1) = a$, $\phi(2) = b$, $\phi(3) = c$ является изотонной функцией.

⇨ **Определение 5.19.** Изотонная функция, допускающая изотонную обратную функцию, называется *ϕ -изоморфизмом*. Иными словами, изоморфизм есть взаимно однозначное соответствие между двумя у-множествами, удовлетворяющее условию (1) и условию (1'):

$$\text{из } \phi(x) \leq \phi(y) \text{ следует, что } x \leq y. \quad (1')$$

⇨ **Определение 5.20.** Два у-множества P и Q называются *изоморфными* (обозначение: $P \cong Q$), если между ними существует изоморфизм.

* **Пример.** Нетрудно заметить, что диаграммы множеств $\wp(A)$ (рис. 5.5) и X (рис. 5.6) имеют совершенно одинаковую структуру, хотя состоят из разных элементов. Значит, между ними можно установить взаимно однозначное соответствие (самостоятельно определите изотонную функцию ϕ , допускающую изотонную обратную функцию). Очевидно, что соответствие будет сохранять порядок каждого упорядоченного множества, т.е. эти у-множества изоморфны.

⇨ **Определение 5.21.** Изоморфизм у-множества P с самим собой называется *автоморфизмом*.

Из свойств **P1** — **P3** следует **принцип двойственности**.

Теорема 5.3. Отношение, обратное для отношения порядка, само является упорядоченностью.

Действительно, если $x \leq y$ (« x меньше y »), то $y \geq x$ (« y больше x »). Например, если $x \leq y$ есть отношение « x делит y », то обратное ему отношение $y \geq x$ есть « y делится на x ».

⇨ **Определение 5.22.** Двойственным для u -множества X называется множество X' , определяемое на тех же элементах отношением, обратным к упорядоченности в X . При этом: $X \equiv X'$.

Из теоремы 5.3 следует, что каждое свойство и каждая теорема об u -множествах имеет двойственный аналог, и если некоторое утверждение справедливо для всех u -множеств, то двойственное ему утверждение также справедливо для всех u -множеств. Это свойство u -множеств обычно и называется *принципом двойственности*.

Согласно этому принципу, утверждение ψ справедливо в u -множестве $\langle X, \leq \rangle$, тогда и только тогда, когда двойственное ему утверждение справедливо в u -множестве $\langle X', \geq \rangle$. Для каждого утверждения относительно решетки можно получить двойственное ему утверждение, заменив в нем операцию \vee на \wedge и наоборот. Если в утверждении присутствуют **0** и **1** решетки, то в двойственном утверждении их также следует поменять местами. Например, для утверждения «множество $\langle X, \leq \rangle$ имеет нуль» двойственным будет утверждение «множество $\langle X', \geq \rangle$ имеет единицу».

Согласно принципу двойственности, все свойства решеток, которые будут рассмотрены в следующей главе, формулируются в виде двух утверждений, двойственных друг другу.

⇨ **Определение 5.23.** Функция $\varphi: P \rightarrow Q$ называется *антиизотонной* (антитонной), если:

из $x \leq y$ следует, что $\varphi(x) \geq \varphi(y)$, (2)

а взаимно однозначное соответствие φ , удовлетворяющее условию (2) и (2'):

из $\varphi(x) \leq \varphi(y)$ следует $x \geq y$, (2')

называется *дуальным изоморфизмом*.

* **Пример.**

На рис. 5.7 прямая $y = x$ есть автоморфизм $\mathbf{R} \rightarrow \mathbf{R}$, который является тождественным отображением. Прямая $y = -x$ есть дуальный автоморфизм; это отображение биективно и антитонно: если $x_1 \leq x_2$, то $y_1 \geq y_2$.

Системы $\langle X', \geq \rangle$, дуально изоморфные $\langle X, \leq \rangle$, являются *двойственными по отношению к X* .

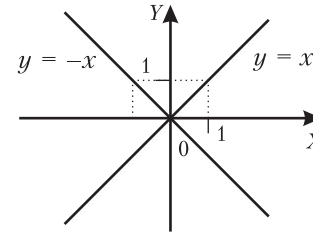


Рис. 5.7.

Аutomорфизм и
дуальный автоморфизм.

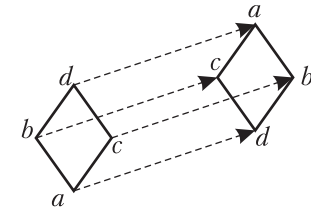


Рис. 5.8.

Дуальный изоморфизм
(самодвойственное множество).

* **Пример.** Множества E и E' на рис. 5.9. двойственны друг другу. Отображение φ является изоморфизмом: прямое и обратное отображения биективны и изотонны. Отображение ψ на рис. 5.9, б не является изоморфизмом, оно не сохраняет порядок, например, $b \leq d$, но $\psi(b) \not\leq \psi(d)$.

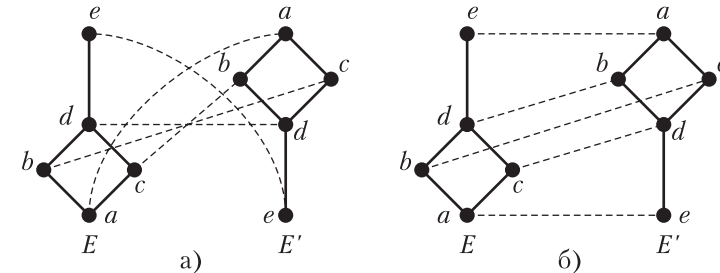


Рис. 5.9.

а) Изотонное отображение, изоморфизм.
б) Неизотонное отображение.

⇨ **Определение 5.24.** u -множество, дуально изоморфное самому себе, называется *самодвойственным*. В самодвойственном множестве для любого x образ $\varphi(\varphi(x))$ образа $\varphi(x)$ совпадает с x : $\varphi(\varphi(x)) = x$. Такие самодвойственные (дуальные) автоморфизмы называются *инволюциями*.

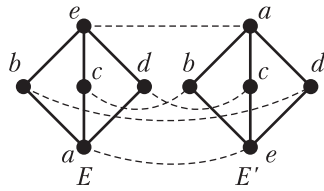
* **Примеры.**

1. Множество на рис. 5.8 является самодвойственным. Действительно, отображение $\varphi(a) = d, \varphi(b) = c, \varphi(c) = b, \varphi(d) = a$ является дуальным автоморфизмом. Повторное применение этого отображения дает те же самые элементы, т. е. выполняется свойство самодвойственности: $\varphi(\varphi(x)) = x$.
2. Свойством самодвойственности обладает множество-степень $\wp(P)$ всех подмножеств некоторого множества P , упорядоченное

отношением включения. Отображение, ставящее в соответствие каждому подмножеству его дополнение до множества P , взаимно однозначно и обращает включение. Таким образом, множество-степень $\wp(P)$ является самодвойственным (см. рис. 5.5).

3. На рис. 5.9, а) показаны множества E и E' , двойственные друг другу. На рис. 5.9, б) показано, что множество E не является самодвойственным. Действительно, отображение ψ не является дуальным изоморфизмом: $b \leq d$, однако $\psi(b) = c$ и $\psi(d) = b$ несравнимы. Нетрудно убедиться, что для этих множеств не существует дуального изоморфизма.

4. Множество на рис. 5.10 не является самодвойственным. Действительно, условие $\varphi(\varphi(x)) = x$ выполняется не для всех элементов при этом отображении:



$$\begin{array}{ll} \varphi(a) = e, & \varphi(\varphi(a)) = \varphi(e) = a, \\ \varphi(b) = d, & \varphi(\varphi(b)) = \varphi(d) = c, \\ \varphi(c) = b, & \varphi(\varphi(c)) = \varphi(b) = d, \\ \varphi(d) = c, & \varphi(\varphi(d)) = \varphi(c) = b, \\ \varphi(e) = a, & \varphi(\varphi(e)) = \varphi(a) = e. \end{array}$$

Рис. 5.10. Несамодвойственное множество.

5.5. Градуированные множества

Теорема 5.4. Любая конечная цепь из n элементов изоморфна ординальному числу n (цепи целых чисел $1, \dots, n$). Иными словами, существует взаимно однозначное соответствие φ между n -элементной цепью X и множеством $\{1, 2, \dots, n\}$, такое, что $x_1 \leq x_2$ тогда и только тогда, когда $\varphi(x_1) \leq \varphi(x_2)$.

Доказательство. Пусть φ отображает наименьший элемент $x \in X$ в 1, наименьший элемент из оставшихся — в 2 и т. д. Тогда каждому элементу цепи будет соответствовать натуральное число. \asymp

↪ **Определение 5.25.** *Длиной* $l[P]$ у-множества P называется точная верхняя грань длин цепей в P . Длина конечной цепи n по определению полагается равной $n - 1$ (это очевидно, если посмотреть на диаграмму цепи). Если $l[P]$ конечно, то говорят, что у-множество P имеет конечную длину.

↪ **Определение 5.26.** *Высотой*, или *размерностью*, $h[x]$ элемента x называется точная верхняя грань длин цепей $0 < x_0 < x_1 < \dots < x_l = x$ между 0 и x . Если P имеет наибольший элемент I , то, очевидно, что $h[I] = l[P]$. Понятно также, что $h[x] = 1$ тогда и только тогда, когда x покрывает 0 . Такие элементы x называются *атомами*, или *точками*, у-множества P .

* **Примеры.** На рис. 5.11 высота множества M_3 равна 2, а высота множеств N_5 , L_7 , 2^3 и P_6 равна 3.

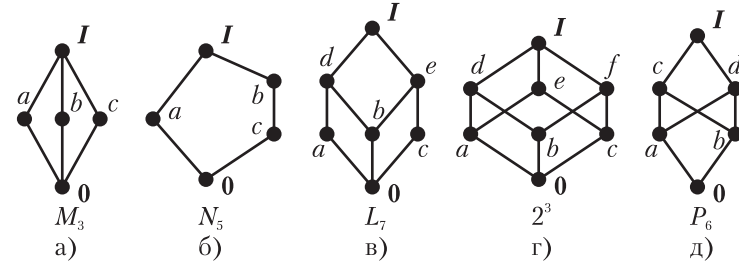


Рис. 5.11. Диаграммы у-множеств.

Понятие высоты тесно связано с понятием градуированного множества.

↪ **Определение 5.27.** *Градуированным* у-множеством называется у-множество P с заданной на нем функцией $g: P \rightarrow \mathbb{Z}$, принимающей значение в цепи целых чисел, и такой, что
если $x > y$, то $g[x] > g[y]$, (строгая изотонность); **G1.**
если x покрывает y , то $g[x] = g[y] + 1$. **G2.**

Утверждение. Во всяком градуированном у-множестве имеет место цепное условие Жордана–Дедекинда: все максимальные цепи между двумя фиксированными точками имеют одинаковую длину.

Теорема 5.5. В у-множестве P с 0 и конечными цепями тогда и только тогда выполняется цепное условие Жордана–Дедекинда, когда P градуируется функцией высоты $h[x]$.

Такие множества, в которых выполняется условие Жордана–Дедекинда, называют еще *дедекиндовыми* множествами.

Доказательство. Если P градуируется функцией $h[x]$, то условие Жордана–Дедекинда выполняется очевидным образом: длина максимальной цепи, соединяющей точки a и b , такие, что $b > a$, равна $h[b] - h[a]$. Обратное, если имеет место условие Жордана–Дедекинда, то $h[x]$ будет длиной максимальной цепи от 0 до x , откуда следует выполнимость для $h[x]$ условий **G1** и **G2**. \asymp

* **Пример.** Рассмотрим диаграммы на рис. 5.11. Среди множеств, изображенных на рис. 5.11, множество N_5 выделяется своей «несимметричностью»: длина левой цепи между 0 и I равна двум, а правой цепи — трем. Поскольку на диаграммах Хассе изображаются только максимальные цепи, условие Жордана–Дедекинда не выполняется в данном множестве, оно является не градуированным (не дедекиндовым) множеством. Все остальные множества — градуированные.

Глава 6.

РЕШЕТКИ

Исторически теория решеток появилась позже формализации Джорджем Булем пропозициональной логики высказываний, которое привело к понятию булевой алгебры. Именно исследования по аксиоматизации булевых алгебр побудили Чарльза Пирса и Эрнста Шрёдера ввести понятие решетки в конце девятнадцатого века. Независимо от них, Ричард Дедекинд в своих исследованиях по идеалам алгебраических чисел пришел к тому же самому понятию. Однако эти работы не привлекли внимания математической общественности в то время. И только исследования Гарриетта Биркгофа в середине тридцатых годов дали толчок развитию теории решеток. В серии блестящих работ он показал важность теории решеток, которая служит каркасом для обобщения и унификации многих результатов в различных математических дисциплинах. Собрав и обобщив свои результаты, а также достижения многих других математиков, работающих в этой области, Г. Биркгоф в 1940 г. издал монографию «*Lattice Theory*», создав фактически основы общей теории решеток, что позволило выделить ее в самостоятельную дисциплину. В дальнейших изданиях (1948, 1967 гг.) Г. Биркгоф отразил развитие этой теории, и в настоящее время его монография (на русском языке см. [Биркгоф, 1984]) является настоящей энциклопедией классической теории решеток.

6.1. Основные определения

↪ **Определение 6.1.** Решеткой¹ называется у-множество L , в котором любые два элемента x и y имеют точную нижнюю грань, называемую *пересечением* (обозначается $x \wedge y$), и точную верхнюю грань, называемую *объединением* (обозначается $x \vee y$). Решетка L называется *полной*, если любое ее подмножество X имеет в L точные верхнюю и нижнюю грани.

Полагая $X = L$, мы видим, что любая непустая полная решетка содержит наименьший элемент 0 и наибольший элемент 1 . Действительно, если каждые два элемента имеют точную верхнюю грань, то в решетке имеется только один максимальный элемент, который будет и универсальной верхней гранью, т.е. единицей у-множества. Аналогично, существование точной нижней грани для любых двух элементов обеспечивает существование универсальной нижней грани — нуля у-множества. Очевидно, что у-множество, двойственное решетке, само является решеткой, а у-

¹ По-английски *lattice*, по-немецки *Verband*; в нашей литературе решетки иногда именуют структурами.

множество, двойственное полной решетке, будет полной решеткой с взаимной заменой объединений и пересечений. Из определения следует также, что любая конечная решетка является полной.

Утверждение 6.1. Любая цепь является решеткой, в которой $x \wedge y$ совпадает с меньшим, а $x \vee y$ — с большим из элементов x, y .

Это утверждение очевидно, так как в любой цепи либо $x \leq y$, либо $y \leq x$, поэтому либо $x \wedge y = x$, либо $x \wedge y = y$. Двойственно для объединения: либо $x \vee y = x$, либо $x \vee y = y$.

* Примеры.

1. В главе 5 на рис. 5.11 изображены диаграммы Хассе у-множеств, среди которых множества $M_3, N_3, L_7, 2^3$ являются решетками. Не всякое у-множество с 0 и 1 является решеткой. У-множество P_6 является дедекиндовым у-множеством с 0 и 1 , однако, оно не образует решетку, так как в нем не для всяких двух элементов существует объединение и пересечение: для элементов c и d не существует пересечения, а для элементов a, b — объединения.

2. У-множество рациональных чисел не является полной решеткой, так как в нем отсутствуют универсальные грани 0 и 1 . В у-множестве действительных чисел условия полноты будут выполняться, если присоединить к ним в качестве универсальных граней $-\infty$ и $+\infty$.

↪ **Определение 6.2.** Подрешеткой решетки L называется подмножество $X \subset L$ такое, что если $a \in X, b \in X$, то $a \wedge b \in X$ и $a \vee b \in X$.

Пустое подмножество и любое одноэлементное подмножество являются подрешетками. Подрешетка решетки сама является решеткой с теми же операциями объединения и пересечения. Вообще, если $a \leq b$ в решетке L , то (замкнутый) интервал $[a, b]$, состоящий из всех элементов $x \in L$, которые удовлетворяют условию $a \leq x \leq b$, всегда будет подрешеткой. Для цепи и ее элементов $a \leq b$ можно определить понятия *полуоткрытых интервалов*: $(a, b] = \{x \mid a < x \leq b\}$ и $[a, b) = \{x \mid a \leq x < b\}$, а также *открытый интервал* $(a, b) = \{x \mid a < x < b\}$. Если эти множества непусты, они также являются подрешетками.

* **Пример.** В решетке на рис. 6.1 подмножество $Y = \{\emptyset, \{b\}, \{c\}, \{b, c\}\}$ является подрешеткой. Действительно $\{b\} \in Y, \{c\} \in Y, \{b\} \wedge \{c\} = \emptyset \in Y, \{b\} \vee \{c\} = \{b, c\} \in Y, \{b\} \wedge \{b, c\} = \{b\} \in Y, \{c\} \wedge \{b, c\} = \{c\} \in Y$ и т.д. Это подмножество образует замкнутый интервал $[\emptyset, \{b, c\}]$. Подмножество $Z = \{\emptyset, \{a\}, \{a, b\}, \{a, c\}, \{c\}\}$ не является подрешеткой, так как $\{a, b\} \vee \{a, c\} = \{a, b, c\} \notin Z$. Это

подмножество не является также интервалом. Подрешетками будут также подмножества: $\{\emptyset, \{a\}\}$, $\{\{c\}, \{a, c\}\}$, $\{\{a\}, \{a, b\}\}$, и т.д., все цепи, например, $\{\emptyset, \{b\}, \{b, c\}\}$, а также все элементы решетки.

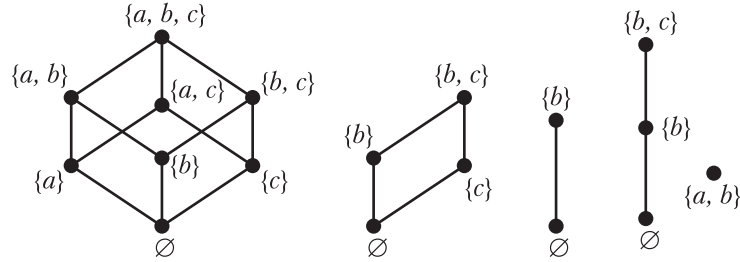


Рис. 6.1. Решетка и ее подрешетки.

↪ **Определение 6.3.** Выпуклым подмножеством в u -множестве P называется подмножество, которое вместе с любыми своими элементами a и b , где $a \leq b$, содержит весь интервал $[a, b]$.

На рис. 6.1 подмножество $\{\emptyset, \{b\}, \{c\}, \{b, c\}\}$ — выпуклое, а подмножество $\{\emptyset, \{b\}, \{b, c\}\}$ — нет. Подмножество S решетки L является *выпуклой подрешеткой*, если для любых $a, b \in S$ $[a \wedge b, a \vee b] \subset S$.

↪ **Определение 6.4.** Свойство подмножеств множества S называется свойством замыкания, если:

- 1) S обладает этим свойством;
- 2) любое пересечение подмножеств, обладающих этим свойством, само обладает им.

Понятие «свойство замыкания» равносильно понятию «операция замыкания».

↪ **Определение 6.5.** Операцией замыкания на множестве S называется отображение $X \rightarrow X'$ на подмножествах этого множества такое, что

- | | | |
|---|--------------------|-----------|
| $X \subset X'$ | (экстенсивность); | C1 |
| $X' = X''$ | (идемпотентность); | C2 |
| Если $X \subset Y$, то $X' \subset Y'$ | (изотонность). | C3 |

Подмножество $X \subset S$, по определению, замкнуто относительно данной операции замыкания, если оно совпадает со своим «замыканием» X' . Теперь подрешетку можно определить как любое подмножество решетки, замкнутое относительно операций объединения и пересечения.

6.2. Решетки как алгебры

Решетку можно определить как алгебраическую систему: $L = \langle P, \vee, \wedge, \leq \rangle$, с двумя бинарными операциями и отношением порядка, заданными на множестве P . Решеточные операции \vee и \wedge обладают важными алгебраическими свойствами. В этом разделе мы исследуем свойства операций \vee и \wedge и покажем, что операции, обладающие этими свойствами, определяют отношение порядка на множестве P , что позволяет рассматривать решетки как алгебры с двумя операциями.

Лемма 6.1. В любом u -множестве для операций пересечения и объединения выполняются (при определенных в них выражениях) следующие законы:

- | | | |
|--|--------------------|-----------|
| $x \wedge x = x, x \vee x = x$ | (идемпотентность); | L1 |
| $x \vee y = y \vee x, x \wedge y = y \wedge x$ | (коммутативность); | L2 |
| $x \wedge (y \wedge z) = (x \wedge y) \wedge z,$ | | |
| $x \vee (y \vee z) = (x \vee y) \vee z$ | (ассоциативность); | L3 |
| $x \wedge (x \vee y) = x, x \vee (x \wedge y) = x$ | (поглощение). | L4 |

Кроме того, неравенство $x \leq y$ равносильно каждому из условий: $x \wedge y = x$ и $x \vee y = y$ (условие совместимости).

Доказательство. **L1** и **L2** выполняются очевидно. Ассоциативный закон **L3** также очевиден: $x \wedge (y \wedge z) = \inf \{x, \inf \{y, z\}\} = \inf \{\inf \{x, y\}, z\} = (x \wedge y) \wedge z$. Закон поглощения **L4** выполним в силу того, что $x \wedge (x \vee y) = \inf \{x, \sup \{x, y\}\}$. Если $x \leq y$, то $\sup \{x, y\} = y$, и тогда $\inf \{x, y\} = x$, а если $y \leq x$, то $\sup \{x, y\} = x$, и тогда $\inf \{x, x\} = x$. Условие совместимости: $x \wedge y = x$, если $x \leq y$, и $x \vee y = y$, если $x \leq y$, — выполняется также очевидно. \simeq

Из условия совместимости следуют важные свойства универсальных граней **0** и **1**.

Лемма 6.2. Если u -множество P имеет **0**, то $\mathbf{0} \wedge x = \mathbf{0}$ и $\mathbf{0} \vee x = x$ для всякого $x \in P$, и если u -множество P имеет **1**, то $x \wedge \mathbf{1} = x$ и $x \vee \mathbf{1} = \mathbf{1}$ для всякого $x \in P$.

Доказательство не представляет труда.

Лемма 6.3. Во всякой решетке операции объединения и пересечения изотонны:

если $y \leq z$, то $x \wedge y \leq x \wedge z$ и $x \vee y \leq x \vee z$.

Доказательство. Согласно **L1** — **L4**, если $y \leq z$, то $x \wedge y = (x \wedge x) \wedge (y \wedge z) = (x \wedge y) \wedge (x \wedge z)$. Учитывая, что $x \wedge x = x$ и $y \wedge z = y$, по условию совместимости получаем $x \wedge y \leq x \wedge z$. Второе неравенство доказывается двойственно. \simeq

Лемма 6.4. Во всякой решетке имеют место следующие *неравенства дистрибутивности*:

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z), \quad (6.1)$$

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z). \quad (6.1')$$

Доказательство. Очевидно, что $x \wedge y \leq x$ и $x \wedge y \leq y \leq y \vee z$, откуда $x \wedge y \leq x \wedge (y \vee z)$. Аналогично: $x \wedge z \leq x$ и $x \wedge z \leq z \leq y \vee z$, откуда $x \wedge z \leq x \wedge (y \vee z)$. Таким образом, $x \wedge (y \vee z)$ является верхней гранью для $x \wedge y$ и $x \wedge z$ и, следовательно, выполняется (6.1). (6.1') доказывается двойственно. \simeq

Лемма 6.5. Элементы любой решетки удовлетворяют *неравенству модулярности*:

$$\text{если } x \leq z, \text{ то } x \vee (y \wedge z) \leq (x \vee y) \wedge z. \quad (6.2)$$

Доказательство. $x \leq x \vee y$ и $x \leq z$, значит $x \leq (x \vee y) \wedge z$. Аналогично, $y \wedge z \leq y \leq x \vee y$ и $y \wedge z \leq z$, следовательно, $y \wedge z \leq (x \vee y) \wedge z$, отсюда $x \vee (y \wedge z) \leq (x \vee y) \wedge z$. \simeq

Дадим следующие определения.

☞ **Определение 6.6.** Система с одной бинарной идемпотентной, коммутативной и ассоциативной операцией называется *полурешеткой*. У-множество P , в котором любые два элемента имеют пересечение, является полурешеткой относительно бинарной операции \wedge . Такие полурешетки называются *\wedge -полурешетками*, или *нижними полурешетками*. У-множество P , в котором любые два элемента имеют объединение, является полурешеткой относительно бинарной операции \vee . Такие полурешетки называются *\vee -полурешетками*, или *верхними полурешетками*.

✱ **Пример.** На рис. 6.2 приведены диаграммы верхней и нижней полурешеток. В у-множестве P_1 любые два элемента имеют объединение, однако элементы a и b не имеют пересечения, поэтому P_1 является верхней полурешеткой; в у-множестве P_2 любые два элемента имеют пересечение, однако элементы c и d не имеют объединения, поэтому это нижняя полурешетка.

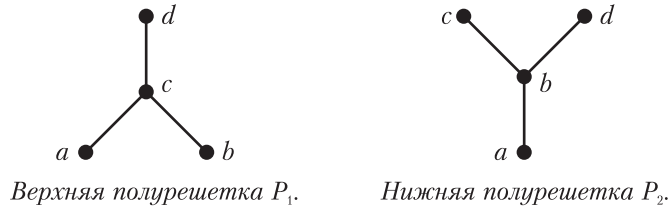


Рис. 6.2. Полурешетки.

Теперь докажем важную лемму, которая связывает полурешетку как алгебру с понятием у-множества. Эта лемма утверждает, что если задана алгебра на множестве P с одной бинарной операцией, удовлетворяющей свойствам идемпотентности, коммутативности и ассоциативности, то эта операция задает отношение порядка на P , т.е. множество, на котором задана эта операция, является у-множеством. Таким образом, мы можем ничего не знать о существовании каких-либо отношений на множестве P , но задание операции со свойствами **L1**, **L2**, **L3** определяет отношение порядка на нем.

Лемма 6.6. Если в полурешетке с бинарной операцией \circ положить

$$x \leq y \text{ тогда и только тогда, когда } x \circ y = x,$$

то она становится у-множеством, в котором $\inf \{x, y\} = x \circ y$.

Поясним смысл леммы. В лемме задано некоторое множество с некоторой бинарной операцией \circ , и, поскольку указано, что множество образует полурешетку, то это означает, что операция \circ является идемпотентной, коммутативной и ассоциативной. Далее мы вводим некоторое (пока абстрактное) отношение \leq на множестве таким образом, что если $x \circ y = x$, то $x \leq y$, и наоборот, если $x \leq y$, то $x \circ y = x$, т.е. эти два условия равнозначны. Нужно доказать, что отношение \leq является отношением порядка, и операция \circ имеет смысл нахождения точной нижней грани x и y .

Доказательство.

1. Сначала докажем, что отношение \leq является отношением порядка, т.е. удовлетворяет свойствам рефлексивности, антисимметричности и транзитивности: **P1**, **P2**, **P3**.

По предположению леммы, $x \leq y$ тогда и только тогда, когда $x \circ y = x$. Из закона идемпотентности $x \circ x = x$ следует рефлексивность отношения: $x \leq x$. В силу коммутативности $x \circ y = y \circ x$ получаем антисимметричность: если $x \leq y$, то по условию $x \circ y = x$, и если $y \leq x$, то $y \circ x = y$. Тогда, если выполняются одновременно $x \leq y$ и $x \leq y$, то $x = x \circ y = y \circ x = y$, т.е. отношение \leq антисимметрично. Применяя ассоциативный закон, из $x \leq y$ и $y \leq z$ получим $x \leq z$. Действительно, если $x \leq y$ и $y \leq z$, то $x = x \circ y$ и $y = y \circ z$, т.е. $x = x \circ y = x \circ (y \circ z) = (x \circ y) \circ z = x \circ z$, откуда $x \leq z$, т.е. доказана транзитивность \leq . Отсюда следует, что \leq является отношением порядка.

2. Теперь докажем, что $x \circ y = \inf \{x, y\}$ для любых x, y . Докажем сначала, что $x \circ y \leq x$ и $x \circ y \leq y$. Если $x \leq y$, то $x \circ y = x$ по определению, и, следовательно, $x \circ y \leq y$, а в силу рефлексивности $x \leq x$ справедливо и $x \circ y \leq x$. Наконец, если x и y несравнимы, то, в силу того, что операция \circ всюду определена, найдется $z \leq x$ и $z \leq y$. Тогда $z \circ (x \circ y) = (z \circ x) \circ y = z \circ y = z$, откуда $z \leq x \circ y$, и, следовательно, $x \circ y = \inf \{x, y\}$.

Справедлива и двойственная лемма относительно объединения. \asymp

Теперь мы можем доказать теорему о том, что любая решетка может рассматриваться как алгебра.

Теорема 6.3. Любая алгебра $L = \langle P, \vee, \wedge \rangle$ с двумя бинарными операциями, удовлетворяющими условиям **L1** — **L4**, является решеткой, и обратно.

Доказательство. Согласно лемме 6.6, любая система L , операции которой удовлетворяют условиям **L1** — **L4**, является u -множеством, в котором $x \wedge y = \inf \{x, y\}$, так что $x \leq y$ означает, что $x \wedge y = x$. Рассмотрим теперь операцию $x \vee y$. Если $x \leq y$, то $x \wedge y = x$. Подставим $x \wedge y$ вместо x в $x \vee y$; получим $x \vee y = (x \wedge y) \vee y = y$ (последнее равенство выполнимо в силу закона поглощения **L4**). В силу двойственности справедливо и обратное утверждение: если $x \vee y = y$, то $x \leq y$. Следовательно, неравенство $x \leq y$ равносильно также и равенству $x \vee y = y$. По принципу двойственности получаем, что $x \vee y = \sup \{x, y\}$ и, значит, L является решеткой. \asymp

✱ **Пример.**

Пусть на множестве $L = \{a, b, c, d\}$ заданы бинарные операции \otimes и \oplus :

\otimes	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

\oplus	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

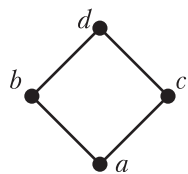


Рис. 6.3.

Решетка $L = \{a, b, c, d\}$.

Непосредственно из таблиц видно, что обе операции идемпотентны (см. значения на диагонали таблиц) и коммутативны (таблицы симметричны). В ассоциативности операций также нетрудно убедиться. Будем полагать, что $x \leq y$ всякий раз, когда $x \otimes y = x$. Тогда из первой строки табл. 6 получим: $a \leq b$, $a \leq c$, $a \leq d$; далее: $b \leq d$, так как $b \otimes d = b$, и $c \leq d$, так как $c \otimes d = c$. Имеем также:

$b \otimes c = c \otimes b = a$, откуда следует, что a является точной нижней гранью b и c , и, учитывая первую строку, универсальной нижней гранью. Тогда, построив диаграммы двух цепей: $a \leq b$, $b \leq d$, и $a \leq c$, $c \leq d$, получим диаграмму на рис. 6.3, где операция \otimes является пересечением, а \oplus — объединением любых двух элементов. Таким образом, множество L является решеткой.

6.3. Дистрибутивные решетки

Можно выделить решетки, обладающие дополнительными свойствами, и определить типы решеток, согласно этим свойствам. Так, например, для любой решетки выполняются неравенства дистрибутивности (6.1) и (6.1'), однако существуют и такие, для которых выполнимы строгие равенства.

⇨ **Определение 6.7.** Решетка называется *дистрибутивной*, если в ней для всех x, y, z выполняются тождества:

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z), & \mathbf{L6'} \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z). & \mathbf{L6''} \end{aligned}$$

Следует отметить, что выполнимость **L6'** для отдельных элементов решетки не влечет выполнимости для них **L6''** (свойство **L6''** для тех же элементов может не выполняться, если решетка недистрибутивна). Однако выполнимость одного из свойств для **всех** элементов решетки влечет выполнимость и другого. Тогда для проверки дистрибутивности решетки достаточно установить тождество **L6'** (или **L6''**) для всех элементов, — второе будет следовать по теореме 6.4.

Теорема 6.4. Если в решетке для всех элементов выполняется тождество **L6'**, то выполняется тождество **L6''** и наоборот.

Доказательство. Покажем, что из **L6'** следует **L6''**. Из **L6''** будет следовать **L6'** по принципу двойственности. Для всех x, y, z :

$$\begin{aligned} (x \vee y) \wedge (x \vee z) &= \\ &= [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] = & \text{согласно } \mathbf{L6'} \\ &= x \vee [z \wedge (x \vee y)] = & \text{по } \mathbf{L4}, \mathbf{L2} \\ &= x \vee [(z \wedge x) \vee (z \wedge y)] = & \text{по } \mathbf{L6'} \\ &= [x \vee (z \wedge x)] \vee (z \wedge y) = & \text{по } \mathbf{L3} \\ &= x \vee (z \wedge y). & \text{по } \mathbf{L4} \asymp \end{aligned}$$

Лемма 6.7. Любая цепь является дистрибутивной решеткой.

Доказать самостоятельно.

6.4. Модулярность

⇨ **Определение 6.8.** Решетка называется *модулярной*, если в ней выполняется модулярный закон **L5**:

$$\text{если } x \leq z, \text{ то } x \vee (y \wedge z) = (x \vee y) \wedge z. \quad \mathbf{L5}$$

Заметим, что по принципу двойственности, если $z \leq x$, то $x \wedge (y \vee z) = (x \wedge y) \vee z$, что совпадает с **L5**, т.е. закон модулярности является самодвойственным.

Модулярный закон может быть получен из **L6''**, если $x \leq z$. Таким образом, модулярный закон **L5** имеет место в любой дистрибутив-

ной решетке. Отсюда следует, что *если решетка дистрибутивна, то она и модулярна*.

✱ **Примеры.**

1. Рассмотрим решетку N_5 («пентагон») на рис. 6.4. Докажем, что она немодулярна. Все цепи в решетке дистрибутивны, следовательно, для любых двух элементов, лежащих на одной цепи, условие модулярности выполняется. Возьмем элементы $a \leq b$ и элемент c , не лежащий с ними на одной цепи. Проверим выполнимость свойства **L5**: $a \vee (c \wedge b) = (a \vee c) \wedge b$. Получим: $a \vee (c \wedge b) = a \vee \mathbf{0} = a$, $(a \vee c) \wedge b = \mathbf{I} \wedge b = b$. Так как $a \neq b$, то закон модулярности не выполняется. Рассмотрим, удовлетворяется ли свойство дистрибутивности: $a \vee (c \wedge b) = (a \vee c) \wedge (a \vee b)$, но $a \vee \mathbf{0} \neq \mathbf{I} \wedge b$, следовательно, решетка N_5 не дистрибутивна.

Отсюда следует вывод: *если решетка немодулярна, то она недистрибутивна*.

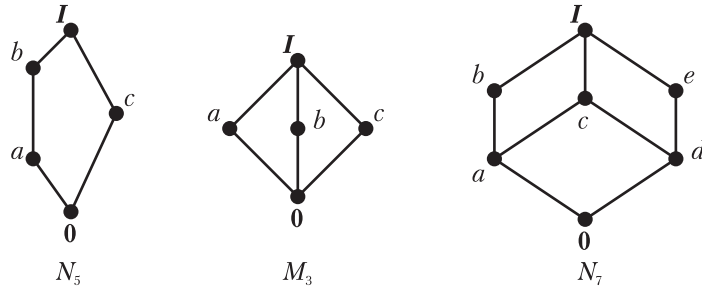


Рис. 6.4. Решетки N_5 (пентагон), M_3 (ромб), N_7 .

2. Рассмотрим решетку M_3 («ромб») на рис. 6.4. Все цепи $\{0, a, \mathbf{I}\}$, $\{0, b, \mathbf{I}\}$, $\{0, c, \mathbf{I}\}$ дистрибутивны, следовательно, и модулярны. Возьмем три элемента, не лежащие на одной цепи: $a \leq \mathbf{I}$ и c . Условие модулярности для них выполняется: $a \vee (c \wedge \mathbf{I}) = (a \vee c) \wedge \mathbf{I}$, так как $a \vee c = \mathbf{I} \wedge \mathbf{I}$, т.е. $\mathbf{I} = \mathbf{I}$. Нетрудно убедиться в том, что условие модулярности в M_3 будет выполняться для любых трех элементов, два из которых находятся в отношении порядка, и, следовательно, решетка M_3 модулярна. Проверим выполнение свойства дистрибутивности для элементов a, b, c (все остальные тройки элементов в этой решетке дистрибутивны): $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Равенство невыполнено, так как $a \vee (b \wedge c) = a \vee \mathbf{0} = a$, но $(a \vee b) \wedge (a \vee c) = \mathbf{I} \wedge \mathbf{I} = \mathbf{I}$, и $a \neq \mathbf{I}$. Отметим, что выполнено только неравенство дистрибутивности: $a \leq \mathbf{I}$. Таким образом, решетка M_3 модулярна, но не дистрибутивна. Все элементы a, b, c несравнимы, следовательно, для них не определен закон модулярности, но дистрибу-

тивный закон должен выполняться для всех элементов, в том числе для a, b, c .

Отсюда следует вывод: *решетка может быть модулярной, но недистрибутивной*.

Обобщая выводы, полученные нами при исследовании дистрибутивных и модулярных решеток, можно сформулировать следующую теорему.

Теорема 6.6.

- а) Решетка L модулярна тогда и только тогда, когда она не содержит пентагонов.
- б) Модулярная решетка L дистрибутивна тогда и только тогда, когда она не содержит ромбов.
- в) Решетка L дистрибутивна тогда и только тогда, когда она не содержит ни пентагонов, ни ромбов.

Доказательство. а). Если L модулярна, то всякая ее подрешетка тоже модулярна и, следовательно, L не содержит подрешеток, изоморфных N_5 . Если L немодулярна, то она содержит три элемента x, y, z такие, что $x \leq z$, и $x \vee (y \wedge z) < (x \vee y) \wedge z$. Тогда элементы $y, x \vee y, y \wedge z, (x \vee y) \wedge z, x \vee (y \wedge z)$ образуют пентагон (см. рис. 6.5.). Действительно, $y \wedge z \leq x \vee (y \wedge z) < (x \vee y) \wedge z \leq x \vee y$. Далее, $(x \vee (y \wedge z)) \vee y = (x \vee y) \vee ((y \wedge z) \vee y) = x \vee y$. Двойственно, $((x \vee y) \wedge z) \wedge y = z \wedge y$. Равенство $y \wedge z = x \vee (y \wedge z)$ невозможно, так как тогда было бы $x \leq y \wedge z$, откуда $(x \vee y) \wedge z = x \vee (y \wedge z)$, что противоречит условию.

С доказательством пункта б) можно познакомиться в [Гретцер Г., 1982]; пункт в) следует из а) и б). ∞

Основным свойством модулярных решеток является принцип транспозиции.

Теорема 6.7 (принцип транспозиции). В любой модулярной решетке отображения $\phi_a: x \rightarrow x \wedge a$ и $\psi_b: y \rightarrow y \vee b$ являются взаимно обратными изоморфизмами между интервалами $[b, a \vee b]$ и $[a \wedge b, a]$.

Доказательство. Если $x \in [b, a \vee b]$, то $\phi_a(x) \in [a \wedge b, a]$ в силу изотонности ϕ_a . Согласно **L5**, $(x \wedge a) \vee b = x \wedge (a \vee b)$, так как $x \in [b, a \vee b]$. Это означает, что $\psi_b(\phi_a(x)) = x$. В силу принципа двойственности получаем, что $\phi_a(\psi_b(y)) = y$ для всех $y \in [a \wedge b, a]$. ∞

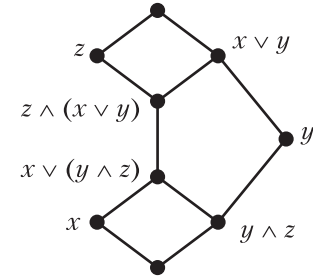


Рис. 6.5.
К доказательству
теоремы 6.6.

Следствие. В любой модулярной решетке, если $a \neq b$ и оба элемента покрывают c , то $a \vee b$ покрывает и a , и b (**M1**), двойственно, если $a \neq b$ и c покрывает оба элемента, то a и b оба покрывают $a \wedge b$ (**M2**).

✱ **Пример.** Для решетки N_7 на рис. 6.4 не выполняется условие **M2**: элементы b, e покрываются элементом I , однако, ни b , ни e не покрывает $b \wedge e = 0$. Отсюда следует, что решетка N_7 немодулярна. Нетрудно проверить, что условие **M1** удовлетворяется в этой решетке. Такие решетки, в которых выполняется одно из условий **M1** или **M2**, называются полумодулярными: если в решетке выполняется условие **M1**, то решетка полумодулярна сверху, а если условие **M2** — то полумодулярна снизу. Решетка N_7 полумодулярна сверху.

6.5. Модулярные решетки с дополнениями

↪ **Определение 6.9.** Дополнением элемента x в решетке с 0 и I называется элемент y такой, что $x \wedge y = 0$ и $x \vee y = I$. Дополнение x будем обозначать x' .

↪ **Определение 6.10.** Решетка называется *решеткой с дополнениями*, если все ее элементы имеют дополнения.

✱ **Примеры.**

1. Решетка на рис. 6.1 является решеткой с дополнениями. Дополнение каждого элемента соответствует его теоретико-множественному дополнению до множества $\{a, b, c\}$: дополнение элемента \emptyset есть $\{a, b, c\}$, дополнение $\{a\}$ есть $\{b, c\}$ и т.д. В общем случае любое множество-степень $\wp(U)$ является решеткой с дополнениями.

2. Решетка на рис. 5.11, изоморфная решетке $\wp(A)$, также является решеткой с дополнениями. Для каждого элемента x существует дополнение x' такое, что $\text{НОД}(x, x') = 1$, т.е. **нулю** решетки, $\text{НОК}(x, x') = 30$, т.е. **единице** решетки. Например, 1 есть дополнение 30 (и наоборот), 2 есть дополнение 15 (и наоборот): $\text{НОД}(2, 15) = 1$, $\text{НОК}(2, 15) = 30$ и т.д., т.е. дополнениями друг друга являются взаимно простые числа.

↪ **Определение 6.11.** Решетка L называется *решеткой с относительными дополнениями*, если каждый ее замкнутый интервал является решеткой с дополнениями.

Давая определение подрешетки, мы определили замкнутый интервал $[a, b]$ решетки как интервал, состоящий из всех элементов $x \in L$, таких что $a \leq x \leq b$. Такой интервал решетки всегда будет подрешеткой. Элемент x' является относительным дополнением элемента $x \in [a, b]$, если $x \wedge x' = a$ и $x \vee x' = b$.

✱ **Примеры.** На рис. 6.4 решетка N_5 — немодулярная решетка с дополнениями: дополнением 0 является I , дополнение a — c , допол-

нение b — c , c имеет два дополнения: a и b . Однако это решетка без относительных дополнений: в интервале $[0, b]$ элемент a не имеет дополнения. Решетка M_3 является подрешеткой с дополнениями. Решетка N_7 — решетка без дополнений: элемент c не имеет дополнения.

Для дистрибутивных решеток имеет место следующая теорема.

Теорема 6.8. Если в дистрибутивной решетке для фиксированного c $c \vee x = c \vee y$ и $c \wedge x = c \wedge y$, то $x = y$.

Доказательство.

$$\begin{aligned} x &= x \wedge (c \vee x) = && \text{(закон поглощения)} \\ &= x \wedge (c \vee y) = && \text{(по условию теоремы)} \\ &= (x \wedge c) \vee (x \wedge y) = && \text{(дистрибутивность)} \\ &= (c \wedge y) \vee (x \wedge y) = && \text{(L2 и по условию } c \wedge x = c \wedge y) \\ &= (c \vee x) \wedge y = (c \vee y) \wedge y = y. \end{aligned}$$

Согласно этой теореме в любом замкнутом интервале $[a, b]$ дистрибутивной решетки элемент c может иметь самое большее одно относительное дополнение. \asymp

Теорема 6.9. Любая модулярная решетка с дополнениями является решеткой с относительными дополнениями.

Доказательство. Пусть M — произвольная модулярная решетка с дополнениями. Рассмотрим интервал $[0, b] \subset M$. Если $0 \leq x \leq b$ в M , то $x \wedge (x' \wedge b) = (x \wedge x') \wedge b = 0 \wedge b = 0$, так как M — решетка с дополнениями, а так как M — модулярна, то $x \vee (x' \wedge b) = (x \vee x') \wedge b = I \wedge b = b$. Следовательно, $B = [0, b]$ является модулярной подрешеткой с дополнениями решетки M . Если взять теперь $[a, b] \subset B$, то это будет модулярная решетка с дополнениями в B . Следовательно, по определению, M является модулярной решеткой с относительными дополнениями. \asymp

Напомним, что в u -множестве P конечной длины с 0 *атомом* называется элемент x , покрывающий 0 (его высота $h[x] = 1$).

Теорема 6.10. В решетке L конечной длины с относительными дополнениями каждый элемент a является объединением содержащихся в нем атомов.

Доказательство. Если $a > 0$, то либо a является атомом, либо $a > b > 0$ для некоторого $b \in L$. Пусть c будет относительным дополнением элемента b в $[0, a]$. Индукцией по длине интервала $[0, a]$ доказывается, что элементы b и c оба являются объединениями атомов. Тогда это справедливо и для $a = b \vee c$. \asymp

Следствие. В модулярной решетке конечной длины с дополнениями каждый элемент является объединением содержащихся в нем атомов.

6.6. Булевы решетки

↪ **Определение 6.12.** Булевой решеткой называется дистрибутивная решетка с дополнениями.

Теорема 6.11. В булевой решетке любой элемент x имеет одно и только одно дополнение x' . При этом:

$$x \wedge x' = 0, \quad x \vee x' = I; \quad \text{L7}$$

$$(x')' = x; \quad \text{(инволюция)} \quad \text{L8}$$

$$(x \wedge y)' = x' \vee y', \quad (x \vee y)' = x' \wedge y'. \quad \text{(законы де Моргана)} \quad \text{L9}$$

Доказательство. По теореме 6.8, если в дистрибутивной решетке $c \vee x = c \vee y$ и $c \wedge x = c \wedge y$, то $x = y$, т.е. каждый элемент дистрибутивной решетки с дополнениями имеет не более одного дополнения. L7 является определением дополнения. Докажем L8. Дополнение элемента x в дистрибутивной решетке единственно, следовательно, соответствие $x \rightarrow x'$ однозначно. Но, по определению, если x' является дополнением x , то x является дополнением x' , следовательно, обратное соответствие также однозначно, т.е. $(x')' = x$. L8 доказано.

Докажем L9. Если x и y имеют дополнения x' и y' соответственно, то элемент $x \wedge y$ имеет своим дополнением $(x \wedge y)'$, а элемент $x \vee y - (x \vee y)'$. В силу единственности дополнения для доказательства первого равенства L9 достаточно показать, что

$$(x \wedge y) \vee (x' \vee y') = I \text{ и } (x \wedge y) \wedge (x' \vee y') = 0.$$

$$\text{Действительно, } (x \wedge y) \vee (x' \vee y') = (x' \vee y' \vee x) \wedge (x' \vee y' \vee y) = I \wedge I = I.$$

$$(x \wedge y) \wedge (x' \vee y') = (x \wedge y \wedge x') \vee (x \wedge y \wedge y') = 0 \vee 0 = 0.$$

Второе равенство L9 доказывается двойственно. \simeq

Лемма 6.7. В булевой решетке $x \wedge a = 0$ тогда и только тогда, когда $x \leq a'$.

Доказательство. Действительно, если $x \leq a'$ то $x \wedge a \leq a' \wedge a = 0$, и, если $x \wedge a = 0$, то $x = x \wedge I = x \wedge (a \vee a') = (x \wedge a) \vee (x \wedge a') = 0 \vee (x \wedge a') = x \wedge a'$, т.е. $x = x \wedge a'$, откуда следует, что $x \leq a'$. \simeq

Из леммы 6.7 следует, что при $a \leq b$, $b' \leq a'$, т.е. взаимно однозначное соответствие $x \rightarrow x'$ обращает порядок (антиизотонно). Соответствие $x' \rightarrow (x')'$ также антиизотонно, следовательно, $x \rightarrow x'$ является дуальным изоморфизмом. Следовательно, любая булева решетка дуально изоморфна самой себе, т.е. самодвойственна.

Поскольку дополнения в булевой решетке единственны, ее можно рассматривать как алгебру.

↪ **Определение 6.13.** Булевой алгеброй $B = \langle L, \vee, \wedge, ', 0, I \rangle$ называется алгебра с двумя бинарными операциями \vee и \wedge , одной унарной операцией $'$ и двумя нульарными операциями 0 и I ,

удовлетворяющими условиям L1 – L9. (Нульарные операции выделяют элементы $0, I$ множества L , эти элементы называются выделенными элементами).

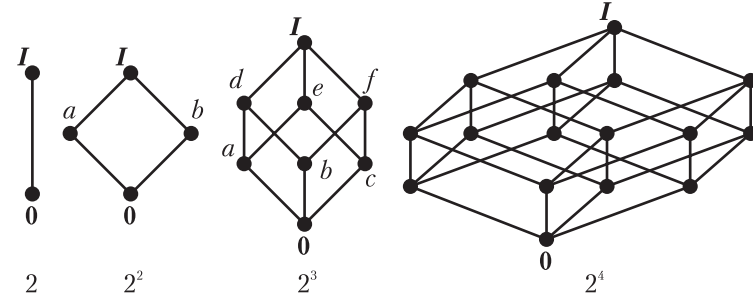


Рис. 6.6. Булевы решетки.

На рис. 6.6 показаны булевы решетки $2, 2^2, 2^3, 2^4$.

Любое поле множеств и, в частности, множество всех подмножеств некоторого множества является булевой алгеброй. Любая подалгебра булевой алгебры сама является булевой алгеброй. Прямое произведение булевых алгебр является булевой алгеброй.

6.7. Квазипорядки

↪ **Определение 6.14.** Отношение квазипорядка (предпорядка) (обозначим его \angle) на множестве S определяется как отношение, удовлетворяющее условиям

рефлексивности: $x \angle x$, P1
 транзитивности: если $x \angle y$ и $y \angle z$, то $x \angle z$, P3
 но не обязательно условию антисимметричности P2.

Пара $\langle S, \angle \rangle$ называется квазиупорядоченным (псевдоупорядоченным) множеством.

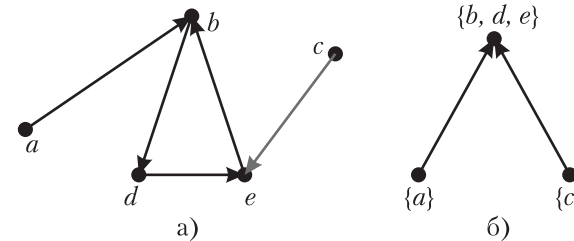


Рис. 6.7.

а) Квазипорядок S . б) Фактор-множество $[S/\sim]$.

Квазиупорядоченное множество изображается в виде ориентированного графа, (см., например, рис. 6.7, а). На графе существование отношения $x \angle y$ означает, что либо $x = y$, либо существует путь из x в y в направлении стрелок. На рис. 6.7, а) показано, что имеется путь из b в e : $b \rightarrow d, d \rightarrow e$, т.е. $b \angle e$. С другой стороны, имеется путь из e в b : $e \rightarrow b$, т.е. $e \angle b$. Таким образом, $b \angle e$ и $e \angle b$, однако, $e \neq b$, т.е. антисимметричность в данном случае не выполняется. Аналогично для d, e и d, b .

Рассмотрим основную лемму о квазиупорядоченных множествах, согласно которой любое квазиупорядоченное множество можно преобразовать в упорядоченное. По лемме, если для каких-то двух элементов выполняется $x \angle y$ и $y \angle x$, и при этом $x \neq y$, то эти элементы полагаются эквивалентными. Множество классов эквивалентности образует у-множество. Например, на рис. 6.7 элементы b, d, e будут эквивалентны и образуют один класс эквивалентности. Два других класса эквивалентности будут образованы одноэлементными подмножествами $\{a\}$ и $\{c\}$. Теперь любые два элемента будут находиться в отношении порядка $x \angle y$ только в том случае, если они принадлежат разным классам эквивалентности. В данном примере: $a \angle b, a \angle d, a \angle e, c \angle b, c \angle d, c \angle e$, и a несравнимо с c . Тогда фактор-множество $[S/\sim]$ есть у-множество, где каждый элемент является одним из классов эквивалентности. На рис. 6.7, б) показано у-множество классов эквивалентности $\{a\}, \{c\}, \{b, d, e\}$.

Докажем эту лемму.

Лемма 6.8. В квазиупорядоченном множестве $Q = \langle S, \angle \rangle$ положим $x \sim y$, если $x \angle y$ и $y \angle x$. Тогда:

- I. отношение \sim является отношением эквивалентности на S ;
- II. если E и F — два класса эквивалентности отношения \sim , то либо $x \angle y$ для всех $x \in E, y \in F$, либо подобное соотношение невозможно ни при каких $x \in E, y \in F$;
- III. фактор-множество S/\sim становится у-множеством, если положить $E \leq F$ в случае, если $x \angle y$ для некоторых (а значит и для всех) $x \in E, y \in F$.

Доказательство.

I. Отношение $x \angle x$ выполняется для всякого $x \in S$ по **P1**, следовательно, отношение \sim рефлексивно. Согласно определению, из $x \sim y$ и $y \sim z$ следует $x \angle y$ и $y \angle z$, откуда $x \angle z$ по **P3**. Аналогично, из $x \sim y$ и $y \sim z$ следует $z \angle y$ и $y \angle x$, поэтому $z \angle x$. Следовательно, если $x \sim y$ и $y \sim z$, то $x \sim z$, т.е. отношение \sim транзитивно. Отношение \sim симметрично по определению. Следовательно, это отношение эквивалентности.

II. В двух классах эквивалентности E и F , если $x \angle y$ для некоторых $x \in E, y \in F$, то $x_1 \angle x \angle y \angle y_1$ для всех $x_1 \in E, y_1 \in F$, и, следовательно, $x_1 \angle y_1$ в силу транзитивности. Это означает, что только элементы, принадлежащие разным классам эквивалентности, могут находиться в отношении порядка, либо эти элементы несравнимы.

III. В фактор-множестве $[S/\sim]$ класс $E \sim E$ (так как $x \sim x$) для всех E . Если $E \leq F$, и $F \leq G$, то $x \angle y \angle z$ для всех $x \in E, y \in F, z \in G$, следовательно, $x \angle z$ согласно **P3** для \angle . Значит отношение \leq транзитивно. И, если $E \leq F$, и $F \leq E$, то для всех $x \in E, y \in F$ $x \angle y$ и $y \angle x$, откуда $x \sim y$, и значит $E = F$.

Таким образом, введение классов эквивалентности на квазиупорядоченных множествах сводит их к у-множествам, поэтому квази-порядок часто называют *предпорядком*.

Глава 7. СТРОЕНИЕ И ПРЕДСТАВЛЕНИЕ РЕШЕТОК

7.1. Операции над у-множествами

Рассмотрим проблему построения решеток из меньших компонент. Для этого используем операции над у-множествами, обобщающие арифметические операции сложения, умножения и возведения в степень. Эти операции над множествами называются *кардинальными операциями*.

↪ **Определение 7.1.** Пусть X, Y – у-множества. Кардинальная сумма $X + Y$ – это множество, элементами которого являются все элементы из X и Y , рассматриваемые как непересекающиеся множества. Порядок \leq сохраняет свой смысл отдельно в X и в Y , и ни для каких $x \in X, y \in Y$ не может быть ни $x \leq y$, ни $y \leq x$.

Диаграмма суммы двух конечных множеств $X + Y$ состоит из диаграммы для X и Y , помещенных рядом, например, диаграмма $2 + 2$ будет выглядеть так:

↪ **Определение 7.2.** Кардинальное произведение $X \times Y$ (или XY) – это декартово (прямое) произведение у-множеств X и Y .

Теорема 7.1. Прямое произведение $L \times M$ любых двух решеток является решеткой.

Доказательство. Для любых двух элементов $\langle x_1, y_1 \rangle$ и $\langle x_2, y_2 \rangle$ в $L \times M$ элемент $\langle x_1 \vee x_2, y_1 \vee y_2 \rangle$ является верхней гранью этой пары. Любая другая верхняя грань $\langle u, v \rangle$ обоих элементов $\langle x_1, y_1 \rangle$ и $\langle x_2, y_2 \rangle$ удовлетворяет неравенствам $u \geq x_i, v \geq y_i$ ($i = 1, 2$), и значит, по определению верхней грани, $u \geq x_1 \vee x_2$ и $v \geq y_1 \vee y_2$, так что $\langle u, v \rangle \geq \langle x_1 \vee x_2, y_1 \vee y_2 \rangle$. Это показывает, что $\langle x_1 \vee x_2, y_1 \vee y_2 \rangle = \langle x_1, y_1 \rangle \vee \langle x_2, y_2 \rangle$, откуда следует, что объединение, стоящее справа, существует. Двойственно: $\langle x_1 \wedge x_2, y_1 \wedge y_2 \rangle = \langle x_1, y_1 \rangle \wedge \langle x_2, y_2 \rangle$. Следовательно, $L \times M$ является решеткой. \simeq

Теорема 7.2. Прямое произведение $X \times Y$ двух дистрибутивных решеток является дистрибутивной решеткой.

Доказательство. Поскольку X и Y – решетки, то по теореме 7.1 их произведение тоже решетка, поэтому имеют место равенства:

$$\begin{aligned} \langle x_i, y_i \rangle \vee \langle x_j, y_j \rangle &= \langle x_i \vee x_j, y_i \vee y_j \rangle \text{ и} \\ \langle x_i, y_i \rangle \wedge \langle x_j, y_j \rangle &= \langle x_i \wedge x_j, y_i \wedge y_j \rangle. \end{aligned}$$

$$\begin{aligned} \text{Тогда } \langle x_i, y_i \rangle \vee (\langle x_j, y_j \rangle \wedge \langle x_k, y_k \rangle) &= \\ = \langle x_i, y_i \rangle \vee \langle x_j \wedge x_k, y_j \wedge y_k \rangle &= \\ = \langle x_i \vee (x_j \wedge x_k), y_i \vee (y_j \wedge y_k) \rangle &= \end{aligned}$$

(поскольку каждая из исходных решеток дистрибутивна, можем продолжить цепочку равенств)

$$\begin{aligned} &= \langle (x_i \vee x_j) \wedge (x_i \vee x_k), (y_i \vee y_j) \wedge (y_i \vee y_k) \rangle = \\ &= \langle (x_i \vee x_j), (y_i \vee y_j) \rangle \wedge \langle (x_i \vee x_k), (y_i \vee y_k) \rangle = \\ &= (\langle x_i, y_i \rangle \vee \langle x_j, y_j \rangle) \wedge (\langle x_i, y_i \rangle \vee \langle x_k, y_k \rangle). \end{aligned}$$

Аналогично доказывается, что

$$\begin{aligned} \langle x_i, y_i \rangle \wedge (\langle x_j, y_j \rangle \vee \langle x_k, y_k \rangle) &= \\ = (\langle x_i, y_i \rangle \wedge \langle x_j, y_j \rangle) \vee (\langle x_i, y_i \rangle \wedge \langle x_k, y_k \rangle). \end{aligned}$$

Следствие. Поскольку цепь является дистрибутивной решеткой, то, очевидно, что прямое произведение цепей есть дистрибутивная решетка.

* Примеры.

1. Прямое произведение цепи на себя часто называют *векторной решеткой*, а отношение частичного порядка на ней – *отношением доминирования*. На рис. 7.1 показана дистрибутивная векторная решетка.

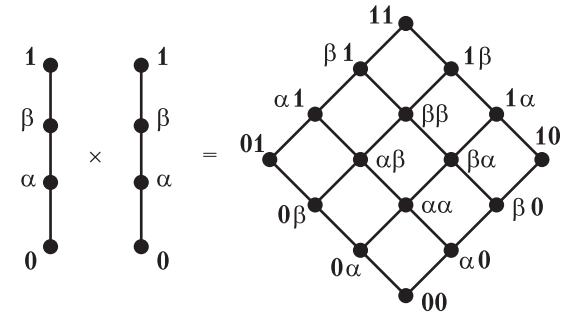


Рис. 7.1. Дистрибутивная векторная решетка.

2. Пусть $X = \{0, 1\}$, $Y = \{0, 1, 2\}$ – цепи. На рис. 7.2 представлены диаграммы у-множеств $X, Y, X \times Y, X \times X \times Y$. Декартово произведение цепей $X \times Y$ имеет плоскую диаграмму и образует дистрибутивную решетку. Декартово произведение цепи X и решетки $X \times Y$ с плоской диаграммой имеет пространственную диаграмму.

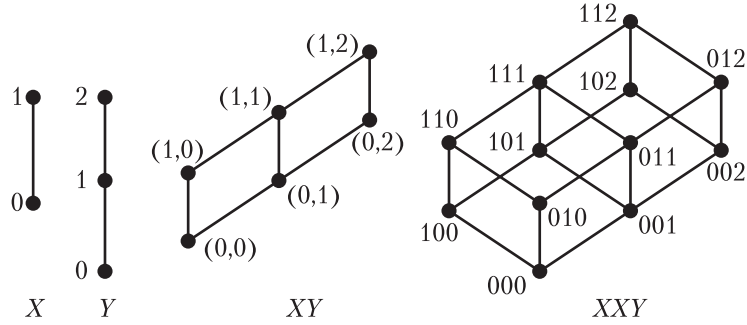


Рис. 7.2. Декартово произведение цепей.

7.2. Степень множеств

↪ **Определение 7.3.** Кардинальной степенью Y^X : $X \rightarrow Y$ с основанием Y и показателем X называется множество всех изотонных функций $y = f(x)$, заданных на X и принимающих значения в Y , упорядоченных отношением $f(x) \leq g(x)$ для всех $x \in X$.

Исследуем свойства степени множеств.

* **Пример.** Пусть $E = \{A, B\}$, $L = \{\alpha, \beta, \gamma\}$. Множество функциональных отображений $F: E \rightarrow L$ имеет мощность $\text{card}L^E = \text{card}L^{\text{card}E} = 3^2 = 9$ (рис. 7.3). Перечислим все функции (запись A/α означает, что α – образ элемента A):

$$F_1 = \{A/\alpha, B/\alpha\}, F_2 = \{A/\alpha, B/\beta\}, F_3 = \{A/\alpha, B/\gamma\},$$

$$F_4 = \{A/\beta, B/\alpha\}, F_5 = \{A/\beta, B/\beta\}, F_6 = \{A/\beta, B/\gamma\},$$

$$F_7 = \{A/\gamma, B/\alpha\}, F_8 = \{A/\gamma, B/\beta\}, F_9 = \{A/\gamma, B/\gamma\}.$$

Пусть $L = \{\alpha, \beta, \gamma\}$ – цепь, тогда на L определены операции объединения \vee и пересечения \wedge . В этом случае на множестве всех функциональных отображений L^E индуцируются операции с теми же свойствами. Для операции пересечения индуцируется операция \otimes следующим образом:

$$F_1 \otimes F_2 = \{A/\alpha, B/\alpha\} \wedge \{A/\alpha, B/\beta\} = \{A/(\alpha \wedge \alpha), B/(\alpha \wedge \beta)\} = \{A/\alpha, B/\alpha\} = F_1.$$

Выполняя данную операцию для всех $F_i \in L^E$, получаем таблицу для индуцированной операции \otimes в L^E (табл. 7.1).

Аналогично можно получить таблицу для операции \oplus , индуцируемой в L^E операцией объединения \vee на L . Все свойства операций \wedge и \vee : идемпотентность, коммутативность, ассоциативность, дистрибутивность, – сохраняются для индуцированных операций \otimes и \oplus . (Проверить выполнимость этих законов для двух индуциро-

ванных операций предоставляется читателю.) В результате множество всех функциональных отображений L^E образует решетку (рис. 7.4).

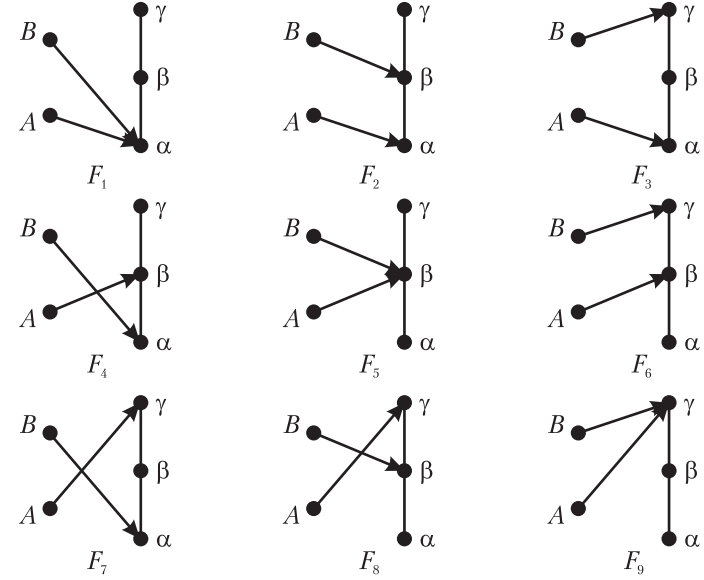
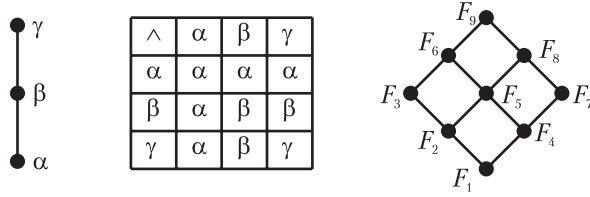


Рис. 7.3. Множество функциональных отображений.

Таблица 7.1.

\otimes	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9
F_1	F_1	F_1	F_1	F_1	F_1	F_1	F_1	F_1	F_1
F_2	F_1	F_2	F_2	F_1	F_2	F_2	F_1	F_2	F_2
F_3	F_1	F_2	F_3	F_1	F_2	F_3	F_1	F_2	F_3
F_4	F_1	F_1	F_1	F_4	F_4	F_4	F_4	F_4	F_4
F_5	F_1	F_2	F_2	F_4	F_5	F_5	F_4	F_5	F_5
F_6	F_1	F_2	F_3	F_4	F_5	F_6	F_4	F_5	F_6
F_7	F_1	F_1	F_1	F_4	F_4	F_4	F_7	F_7	F_7
F_8	F_1	F_2	F_2	F_4	F_5	F_5	F_7	F_8	F_8
F_9	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9

Рис. 7.4. Степень множеств L^E .

Рассмотренный пример позволяет обобщить полученный результат следующей теоремой.

Теорема 7.3. Кардинальная степень L^E индуцирует на множестве функциональных отображений $E \rightarrow L$ множество операций с теми же свойствами, которыми обладают операции, определенные на L . Тогда

- 1) если L – \vee -множество, то L^E – \vee -множество;
- 2) если L – нижняя/верхняя полурешетка, то L^E – нижняя/верхняя полурешетка;
- 3) если L – решетка, то L^E – решетка.

При этом если L – дистрибутивная решетка, то L^E – дистрибутивная решетка, если L – булева решетка, то L^E – булева решетка.

Доказательство.

Пункт 1) выполнен по определению кардинальной степени (см. определение 7.3).

2). Рассмотрим L^E , где L имеет структуру \vee -полурешетки. Положим $x_1, x_2, x_3, y_1, y_2, y_3 \in L, A_1, \dots, A_k \in E$. Пусть $F_i = \{A_1/x_1, \dots, A_k/y_1\}$, $F_j = \{A_1/x_2, \dots, A_k/y_2\}$, $F_l = \{A_1/x_3, \dots, A_k/y_3\}$. Тогда для любых двух элементов $F_i, F_j \in L^E$ элемент $\{A_1/(x_1 \vee x_2), \dots, A_k/(y_1 \vee y_2)\}$ будет верхней гранью этой пары. Любая другая верхняя грань $\langle u, v \rangle$ обоих элементов $\langle x_1, y_1 \rangle$ и $\langle x_2, y_2 \rangle$ удовлетворяет неравенствам $u \geq x_i, v \geq y_i$ ($i = 1, 2$), и значит, по определению верхней грани, $u \geq x_1 \vee x_2$ и $v \geq y_1 \vee y_2$, так что $\langle u, v \rangle \geq \langle x_1 \vee x_2, y_1 \vee y_2 \rangle$. Это показывает, что $\{A_1/(x_1 \vee x_2), \dots, A_k/(y_1 \vee y_2)\} = \{A_1/x_1, \dots, A_k/y_1\} \vee \{A_1/x_2, \dots, A_k/y_2\}$, откуда следует, что объединение $F_i \vee F_j$ существует. Следовательно, L^E – \vee -полурешетка.

Двойственно: $F_i \wedge F_j = \{A_1/(x_1 \wedge x_2), \dots, A_k/(y_1 \wedge y_2)\} = \{A_1/x_1, \dots, A_k/y_1\} \wedge \{A_1/x_2, \dots, A_k/y_2\}$.

Следовательно, если L имеет структуру решетки, то L^E – решетка.

Проверим дистрибутивность L^E , если L – дистрибутивная решетка. Тогда

$$\begin{aligned} F_i \vee (F_j \wedge F_l) &= \{A_1/(x_1 \vee (x_2 \wedge x_3)), \dots, A_k/(y_1 \vee (y_2 \wedge y_3))\} = \\ &= \{A_1/((x_1 \vee x_2) \wedge (x_1 \vee x_3)), \dots, A_k/((y_1 \vee y_2) \wedge (y_1 \vee y_3))\} = \end{aligned}$$

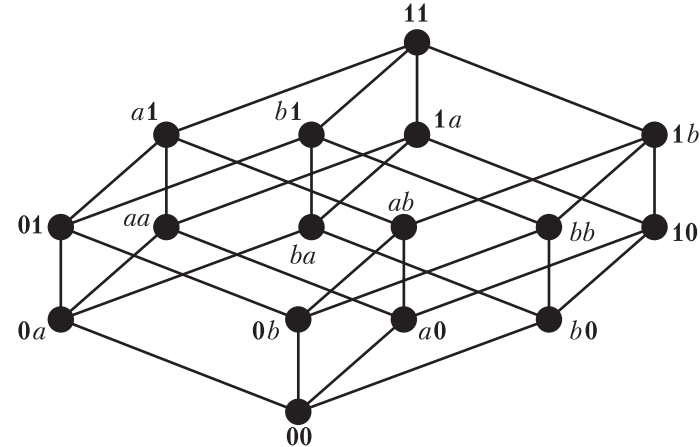
$= (F_i \vee F_j) \wedge (F_i \vee F_l)$ – закон дистрибутивности выполнен.

Предположим, что L – булева решетка. Положим $F_i' = \{A_1/x_1', \dots, A_k/y_1'\}$, где F_i', x_1', y_1' – дополнения F_i, x_1, y_1 соответственно. Тогда $F_i \wedge F_i' = \{A_1/(x_1 \wedge x_1'), \dots, A_k/(y_1 \wedge y_1')\} = \{A_1/0, \dots, A_k/0\}$. Аналогично, $F_i \vee F_i' = \{A_1/(x_1 \vee x_1'), \dots, A_k/(y_1 \vee y_1')\} = \{A_1/1, \dots, A_k/1\}$. Отображение $F_i' = \{A_1/x_1', \dots, A_k/y_1'\}$ является дополнением отображения $F_i = \{A_1/x_1, \dots, A_k/y_1\}$. Таким образом, L^E также обладает структурой булевой решетки с дополнениями. \bowtie

Следствие. Если L – обычный предпорядок, то L^E – обычный предпорядок;

Если L имеет структуру предпорядка, то в этом предпорядке можно определить множество классов эквивалентности и тогда эти классы сами собой образуют частичный или полный порядок. Удаляя транзитивно замыкающие дуги на графе классов эквивалентности, получим диаграмму Хассе. Например, если классы эквивалентности предпорядка образуют верхнюю полурешетку, то L^E также образует верхнюю полурешетку для классов эквивалентности, в которых также выполняется отношение предпорядка.

* **Пример.** Пусть $E = \{A, B\}$ и $L = \{0, a, b, 1\}$ имеет структуру булевой решетки с нулем 0 и единицей 1 . Структура функциональных отображений для L^E изображена на рис.7.5. Она имеет $\text{card} L^E = \text{card} L^{\text{card} E} = 4^2 = 16$ элементов¹. На рисунке обозначение xy – это отображение $\{A/x, B/y\}$, например: $00 - \{A/0, B/0\}$, $ab - \{A/a, B/b\}$ и. т.д.

Рис. 7.5. Решетка функциональных отображений 4^2 .

¹ Диаграммы Хассе для 16-элементных булевых решеток $2^2 \times 2^2$, 2^4 , 4^2 , $(2^2)^2$ имеют одинаковую структуру, но различаются своими элементами.

Пусть теперь $L = \{0, a, b, 1\}$ – цепь, $E = \{A, B\}$. Тогда L^E также имеет 16 элементов, диаграмма его совпадает с диаграммой дистрибутивной векторной решетки, представленной на рис 7.1. Различие заключается в том, что сами элементы решетки имеют другой смысл. Для диаграммы L^E обозначение xy на рисунке следует понимать как функциональное отображение $\{A/x, B/y\}$, например, $a0$ есть обозначение для $\{A/a, B/0\}$ и т.д. Полученная решетка L^E является обобщением нечеткого множества первого уровня в смысле Заде.

7.3. Нечеткие множества

7.3.1. Основные понятия

Рассмотрим конечное множество $E = \{x_1, x_2, \dots, x_n\}$ и $L = \{0, 1\}$. Тогда $L^E = 2^E$ есть множество всех характеристических функций подмножеств множества E , включая \emptyset , и оно образует булеву решетку. Элементами этой решетки будут характеристические вектора подмножеств множества E (см. п. 4.6 главы 4). Каждый элемент характеристического вектора показывает, принадлежит ли данный элемент множества E данному подмножеству, или нет. Однако, как мы показали выше, множество E можно отобразить в любую решетку. Тогда мы приходим к новому понятию.

↪ **Определение 7.4.** Пусть E – универсальное множество и L – решетка. Пусть $\alpha \in L$. Нечеткое подмножество $A \subseteq E$, или, что эквивалентно, $A \in L^E$, – это такое подмножество, что каждому элементу $x \in E$ можно поставить в соответствие элемент $\alpha \in L$. Эти элементы обозначают $\mu_A(x)$ и называют *функцией принадлежности*.

В случае, если решетка L есть замкнутый интервал $[0, 1]$ на множестве действительных чисел, представляющий собой цепь, возведение его в степень произвольного множества E дает множество нечетких подмножеств в смысле Заде. Тогда функция принадлежности $\mu_A(x)$ принимает значения из интервала $[0, 1]$ и определяет степень, с которой элемент x принадлежит нечеткому множеству A . В частности, если $\mu_A(x) = 0$, то элемент x не принадлежит нечеткому множеству A , если $\mu_A(x) = 1$, то элемент x принадлежит нечеткому множеству A со степенью 1, если $\mu_A(x) = 0,6$, то элемент x принадлежит нечеткому множеству A со степенью 0,6 и т.д.

Таким образом, *нечеткое множество в смысле Заде* есть отображение $[0, 1]^E: E \rightarrow [0, 1]$.

✱ **Пример 1.** Пусть множество E есть множество чисел, обозначающих *возраст* человека, например, в пределах от 0 до 100. Рассмотрим такие понятия, как *молодой* и *старый*. Очевидно, трудно установить какую-то точную границу, где кончается возраст *молодости* и

наступает возраст *старости*. Мы можем указать эти границы приблизительно, и, опросив, например, некоторое количество людей, установить, с какой *степенью* можно отнести тот или иной возраст к категории *молодой* или *старый*. Результаты этих опросов можно будет изобразить в виде графиков функций принадлежности $\mu_{\text{молодой}}$ и $\mu_{\text{старый}}$ (рис. 7.6). Значения функции принадлежности из интервала $[0, 1]$ показывают, с какой степенью тот или иной возраст принадлежит возрасту *молодых* или *старых*. Например, возраст *40 лет* со степенью 0,48 отнесен к понятию *молодой* и со степенью 0,36 – к понятию *старый*.

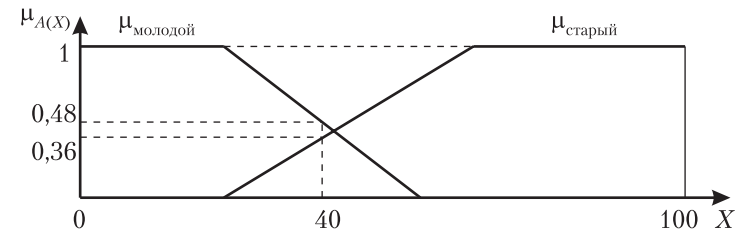


Рис. 7.6. Функции принадлежности нечетких множеств.

✱ **Пример 2.** Пусть $E = \{a, b, c\}$, и пусть $A, B \in [0, 1]^E$: $A = \{a/0,2, b/0,6, c/0,8\}$, $B = \{a/0,1, b/0,4, c/0,9\}$ – два нечетких множества. Элемент a принадлежит множеству A со степенью 0,2, множеству B со степенью 0,1, и т.д.

Приведенное выше определение 7.4 является обобщением понятия нечеткого множества, введенного Заде. Рассмотрим обобщение свойств нечетких множеств и операций на них, если L – решетка.

7.3.2. Операции над нечеткими множествами

↪ **Определение 7.5.** Если \leq – отношение порядка на решетке L , E – некоторое множество, $A \in L^E$, $B \in L^E$ – нечеткие множества, то говорят, что A включено в B ($A \subseteq B$), если

$$\forall x_i \in E: \mu_A(x_i) \leq \mu_B(x_i).$$

Таким образом, два нечетких множества сравнимы, если сравнимы соответствующие значения функций принадлежности и между двумя нечеткими подмножествами существует отношение доминирования. Например, если $A = \{a/0,2, b/0,6, c/0,8\}$, $B = \{a/0,3, b/0,8, c/0,9\}$, то $A \subseteq B$.

↪ **Определение 7.6.** Два нечетких множества A и B равны тогда и только тогда, когда

$$\forall x_i \in E: \mu_A(x_i) = \mu_B(x_i).$$

Понятие дополнения в теории нечетких множеств Заде и в теории решеток – разные. В случае, если L – булева решетка, L^E – также булева решетка. Тогда дополнение нечеткого множества A определяется как нечеткое множество B , такое что

$$\forall x_i \in E: \mu_A(x_i) \wedge \mu_B(x_i) = \mathbf{0} \text{ и } \mu_A(x_i) \vee \mu_B(x_i) = \mathbf{1},$$

где $\mathbf{0}$ – нуль, а $\mathbf{1}$ – единица булевой решетки L .

Учитывая, что не все решетки имеют дополнения своих элементов, и, в частности решетка $[0, 1]$ не имеет дополнений, для нечетких множеств в смысле Заде вводится *псевдодополнение*, которое называют дополнением.

↪ **Определение 7.7.** Дополнение нечеткого множества $A \in [0, 1]^E$ есть нечеткое подмножество B со значениями функции принадлежности, такими что

$$\forall x_i \in E: \mu_B(x_i) = 1 - \mu_A(x_i).$$

Например, если $A = \{a/0,2, b/0,6, c/0,8\}$, то дополнение A – нечеткое множество $B = \{a/0,8, b/0,4, c/0,2\}$.

↪ **Определение 7.8.** Операция *пересечения* на решетке L индуцирует операцию пересечения нечетких множеств как

$$\forall x_i \in E: \mu_{A \cap B}(x_i) = \mu_A(x_i) \wedge \mu_B(x_i).$$

Для нечетких множеств в смысле Заде это определение совпадает с

$$\mu_{A \cap B}(x_i) = \min\{\mu_A(x_i), \mu_B(x_i)\}.$$

Например, если $A = \{a/0,2, b/0,6, c/0,8\}$, $B = \{a/0,1, b/0,4, c/0,9\}$, то $A \cap B = \{a/0,1, b/0,4, c/0,8\}$.

↪ **Определение 7.9.** Операция *объединения* на решетке L индуцирует операцию объединения нечетких множеств как

$$\forall x_i \in E: \mu_{A \cup B}(x_i) = \mu_A(x_i) \vee \mu_B(x_i).$$

Для нечетких множеств в смысле Заде это определение совпадает с

$$\mu_{A \cup B}(x_i) = \max\{\mu_A(x_i), \mu_B(x_i)\}.$$

Например, если $A = \{a/0,2, b/0,3, c/0,8\}$, $B = \{a/0,1, b/0,4, c/0,9\}$, то $A \cup B = \{a/0,2, b/0,4, c/0,9\}$.

Таким образом, если L обладает структурой дистрибутивной решетки с операциями \wedge и \vee , в частности, представляет собой интервал $[0, 1] \subset \mathbf{R}$, то степень L^E индуцирует также дистрибутивную векторную решетку относительно операций \cap и \cup в множестве нечетких подмножеств.

Для нечетких множеств в смысле Заде можно также определить следующие операции.

↪ **Определение 7.10.** Алгебраическое произведение нечетких множеств A и B (обозначается AB) определяется как арифметическое произведение их функций принадлежности:

$$\mu_{AB}(x) = \mu_A(x) \mu_B(x).$$

↪ **Определение 7.11.** Алгебраическая сумма нечетких множеств A и B (обозначается $A + B$) определяется как

$$\mu_{A+B}(x) = \mu_A(x) + \mu_B(x) - \mu_A(x) \mu_B(x),$$

где $+$ и $-$ есть операции арифметического сложения и вычитания соответственно.

Операции кардинальной степени и произведения множеств обладают следующими свойствами:

$$(E_1 \times E_2)^{E^3} = E_1^{E^3} \times E_2^{E^3}, \\ (E_1^{E^2})^{E^3} = E_1^{E^2 \times E^3}.$$

Эти свойства позволяют получить некоторые новые дополнительные обобщения и результаты. Рассмотрим степень произведения множеств, например, $(L_1 \times L_2)^E$, где L_1, L_2 – решетки (полурешетки). Тогда $L_1 \times L_2$ также обладает структурой решетки (полурешетки), а множество $(L_1 \times L_2)^E$ – множество нечетких подмножеств с двуместной функцией принадлежности. Например, если $L_1 = \{a, b, c\}$ – нижняя полурешетка, $L_2 = \{\alpha, \beta\}$ – решетка $\mathbf{2}$, то $L_1 \times L_2$ также обладает структурой нижней полурешетки (рис.7.7).

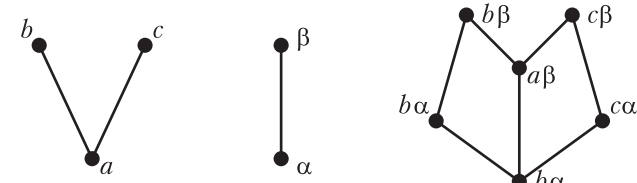


Рис. 7.7. Произведение $L_1 \times L_2$.

Возьмем множество $E = \{A, B, C\}$ и возведем полученную структуру $L_1 \times L_2$ в степень E . Тогда: $(L_1 \times L_2)^E$ имеет $6^3 = 218$ элементов, которые образуют множество нечетких подмножеств, имеющее структуру нижней полурешетки с элементами: $\{A/(x_1, y_1), B/(x_2, y_2), C/(x_3, y_3)\}$, где $x_i = a, b, c$; $i = 1, 2, 3$; $y_j = \alpha, \beta$; $j = 1, 2$.

Предположим, что $\mu_A(x_i)$ принимает свои значения в L_r , $i = 1, 2, \dots, n$, так что каждое $x_i \in L_r$. Тогда множество нечетких подмножеств можно записать как

$$L_1^{\{x_1\}} \times L_2^{\{x_2\}} \times \dots \times L_n^{\{x_n\}}, \quad (*)$$

где $\{x_i\}$ ($i = 1, \dots, n$) – обычные одноточечные подмножества E . Тогда любой элемент вида $(*)$ называется *нечетким неоднородным*

подмножеством. Если $L_1 = L_2 = \dots = L_n$, то $L_1^{\{x_1\}} \times L_2^{\{x_2\}} \times \dots \times L_n^{\{x_n\}} = L^E$, и мы снова приходим к понятию нечеткого подмножества в том же смысле, как и раньше.

Если L_1, L_2, L_3 — решетки, то $L_3^{(L_2^{L_1})}$ — тоже решетка, и один элемент ее — это нечеткое множество 2-го порядка.

Можно пойти дальше и определить нечеткие подмножества более высоких порядков ($n > 2$).

✱ **Пример.** Пусть $L_1 = \{A, B, C\}$, $L_2 = \{a, b\}$, $L_3 = \{a, b\}$. Исследуем представление: $L_3^{(L_2^{L_1})}$. Построим сначала $L_2^{L_1}$. Это будут нечеткие множества:

$$\begin{aligned} F_1 &= \{A/a, B/a, C/a\}, & F_2 &= \{A/a, B/b, C/b\}, \\ F_3 &= \{A/a, B/b, C/a\}, & F_4 &= \{A/a, B/b, C/b\}, \\ F_5 &= \{A/b, B/a, C/a\}, & F_6 &= \{A/b, B/a, C/b\}, \\ F_7 &= \{A/b, B/b, C/a\}, & F_8 &= \{A/b, B/b, C/b\}. \end{aligned}$$

Запишем $F_1 - F_8$ следующим образом: $L_2^{L_1} = \{\sim Faaa, \sim Faab, \sim Faba, \sim Fabb, \sim Fbaa, \sim Fbab, \sim Fbba, \sim Fbbb\}$. Каждый из этих элементов — нечеткое множество 1-го порядка. Возведем теперь L_3 в степень $L_2^{L_1}$. Эта степень содержит $2^8 = 256$ элементов, например:

$$\begin{aligned} \sim\sim F_1 &= \{\sim Faaa/a, \sim Faab/a, \sim Faba/a, \sim Fabb/a, \sim Fbaa/a, \sim Fbab/a, \\ &\sim Fbba/a, \sim Fbbb/a\}, \\ \sim\sim F_2 &= \{\sim Faaa/a, \sim Faab/a, \sim Faba/a, \sim Fabb/a, \sim Fbaa/a, \sim Fbab/a, \\ &\sim Fbba/a, \sim Fbbb/b\}, \\ \sim\sim F_3 &= \{\sim Faaa/a, \sim Faab/a, \sim Faba/a, \sim Fabb/a, \sim Fbaa/a, \sim Fbab/a, \\ &\sim Fbba/b, \sim Fbbb/a\}, \text{ и т.д.} \end{aligned}$$

Следует обратить внимание, что $L_3^{(L_2^{L_1})} \neq (L_3^{L_2})^{L_1}$. Вторая степень дает нам нечеткость другого типа.

7.4. Решеточные многочлены

☞ **Определение 7.12.** Индивидуальные переменные x, y, z, \dots являются многочленами веса 1. Если p, q — решеточные многочлены весов n, m соответственно, то $p \vee q, p \wedge q$ называются решеточными многочленами веса $n + m$.

Теорема 7.4. В любой решетке L подрешетка F_2 , порожденная двумя элементами x и y , состоит из элементов $x, y, x \wedge y = v, x \vee y = u$, для которых операции \vee и \wedge задаются, как показано на рис.7.8.

Доказательство. Согласно **L4**, $x \wedge u = x$, а из **L3**, **L1** следует, что $x \vee u = x \vee (x \vee y) = (x \vee x) \vee y = x \vee y = u$. В силу **L4**, $u \vee v = x \vee y \vee (x \wedge y) = x \vee y = u$. Остальные случаи доказываются аналогично, на основании симметричности между x и y и двойственности. ☞

Решетку F_2 называют свободной решеткой с двумя порождающими x и y . Она содержит четыре элемента и является булевой решеткой.

Решеточные многочлены от трех и более переменных могут быть устроены очень сложно, однако у них есть несколько простых свойств.

Теорема 7.5. В любой \vee -полурешетке каждый многочлен от x_p, x_2, \dots, x_r эквивалентен объединению $\vee_s x_i$ некоторого непустого множества этих переменных.

Доказательство. Согласно **L2**, **L3** каждый такой многочлен эквивалентен объединению некоторых переменных x_2, \dots, x_r в указанном порядке, возможно, с повторениями. Тогда, на основании **L1** можно заменить повторяющиеся вхождения одного и того же символа одним вхождением этого символа. ☞

Теорема 7.6. В любой дистрибутивной решетке каждый многочлен эквивалентен некоторому объединению пересечений и, двойственно, пересечению объединений:

$$p(x_p, x_2, \dots, x_r) = \vee_{a \in A} \{\wedge_{S_a} x_i\} = \wedge_{\delta \in D} \{\vee_{T_\delta} x_i\},$$

где S_a, T_δ — непустые множества индексов, \vee, \wedge — объединение и пересечение конечного числа членов.

Доказательство. Каждый элемент x_i можно записать таким образом, считая A (или D) семейством множеств, состоящим из единственного одноэлементного множества $\{x_i\}$. С другой стороны, используя **L1** — **L3**, получаем: $\vee_{a \in A} \{\wedge_{S_a} x_i\} \vee \vee_{b \in B} \{\wedge_{S_b} x_i\} = \vee_{A \cup B} \{\wedge_{S_c} x_i\}$.

Вследствие дистрибутивности решетки имеем: $\vee_{a \in A} \{\wedge_{S_a} x_i\} \wedge \wedge_{b \in B} \{\wedge_{S_b} x_i\} = \vee_{A \times B} \{\wedge_{S_{ab}} x_i\}$. ☞

7.5. Гомоморфизмы и идеалы

7.5.1. Гомоморфизм решеток

☞ **Определение 7.13.** Изотонное отображение $\phi: L \rightarrow M$ решетки L в решетку M называется \vee -гомоморфизмом, если

$$\phi(x \vee y) = \phi(x) \vee \phi(y) \quad \forall x, y \in L, \quad (1)$$

\wedge -гомоморфизмом, если

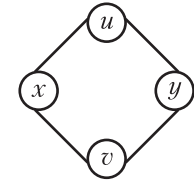


Рис. 7.8.
Решетка
с двумя
порождающими

$$\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y) \quad \forall x, y \in L, \quad (1')$$

и просто гомоморфизмом (морфизмом), если выполняется (1) и (1').

Таким образом, гомоморфизм решеток — это функциональное отображение, сохраняющее решеточные операции, т.е. переводящее объединение — в объединение, пересечение — в пересечение.

↪ **Определение 7.14.** Гомоморфизм называют:

- 1) *изоморфизмом*, если он является взаимно однозначным соответствием (биекцией);
- 2) *наложением*, или *эпиморфизмом*, если он отображает L на M , т.е. если отображение $\varphi: L \rightarrow M$ является сюръекцией;
- 3) *вложением*, или *мономорфизмом*, если различные элементы L отображаются в различные элементы M (однозначное соответствие), т.е. отображение $\varphi: L \rightarrow M$ является инъекцией;
- 4) *эндоморфизмом*, если $L = M$;
- 5) *автоморфизмом*, если $L = M$ и отображение — изоморфизм.

✱ **Пример.** Рассмотрим отображение φ множества $L = \{a, b, c, d, e\}$ на множество $M = \{A, B, C\}$ (рис. 7.9, а).

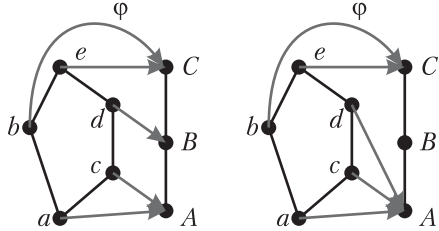


Рис. 7.9. а) — \vee -гомоморфизм, б) — гомоморфизм.

Проверим, является ли оно изотонным. Рассмотрим все цепи максимальной длины и их образы.

Для цепи $a \leq b \leq e$ выполнено $\varphi(a) \leq \varphi(b) \leq \varphi(e)$, так как $A \leq C \leq C$. Для цепи $a \leq c \leq d \leq e$ свойство изотонности также выполнено, так как

$$a \leq c, \varphi(a) = A, \varphi(c) = A, A \leq A, c \leq d, \varphi(c) = A, \varphi(d) = B, A \leq B, \\ d \leq e, \varphi(d) = B, \varphi(e) = C, B \leq C, b \leq e, \varphi(b) = C, \varphi(b) = C, C \leq C.$$

Отображение φ изотонно. Проверим, является ли оно \vee -гомоморфизмом. В силу изотонности отображения, оно сохраняет операции \vee и \wedge , поэтому достаточно проверить сохранение этих операций для несравнимых элементов:

$$\varphi(b \vee c) = \varphi(e) = C; \varphi(b) \vee \varphi(c) = C \vee A = C, \\ \varphi(b \vee d) = \varphi(e) = C; \varphi(b) \vee \varphi(d) = C \vee B = C.$$

Отображение φ сохраняет \vee , следовательно, является \vee -гомоморфизмом. Однако оно не является \wedge -гомоморфизмом, так как $\varphi(b \wedge d) = \varphi(a) = A$, но $\varphi(b) \wedge \varphi(d) = C \wedge B = B$, т.е. свойство сохранения \wedge не выполнено. Поэтому отображение φ не является гомоморфизмом. На рис. 7.9, б показано отображение, которое является гомоморфизмом.

7.5.2. Понятие идеала

При гомоморфизме решетки L в решетку M множество элементов из L , переходящих в один и тот же элемент M , не может быть произвольным. Если φ — гомоморфизм решеток и $\varphi(a) = \varphi(b)$, то, поскольку φ сохраняет операции, в силу идемпотентности

$$\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b) = \varphi(a)$$

и

$$\varphi(a \vee b) = \varphi(a) \vee \varphi(b) = \varphi(b),$$

т.е. образы объединения a и b совпадают с образом a и, следовательно, с b . Иными словами, множество элементов из L , отображаемых гомоморфизмом в один и тот же элемент в M , всегда образует подрешетку, (т.е. a, b отображается в один элемент вместе с $a \wedge b$ и $a \vee b$). Но эта подрешетка не произвольна. Например, если решетка содержит нулевой и единичный элементы, то они, очевидно, образуют подрешетку. Если эти граничные элементы переходят при гомоморфизме в один и тот же элемент, то их образ будет одновременно и нулевым и единичным элементом, а это означает, что он будет образом всех элементов. Следовательно, это уже не будет решетка, содержащая хотя бы два элемента.

Утверждение. В общем случае, если $a \leq b$ и $\varphi(a) = \varphi(b)$, то образ любого $a \leq x \leq b$ будет совпадать с $\varphi(a)$ и $\varphi(b)$.

Действительно, если $a \leq x \leq b$, то $x = x \vee a$ и $x = x \wedge b$. Так как $x = a \vee (x \wedge b)$ и $\varphi(x) = \varphi(a) \vee (\varphi(x) \wedge \varphi(b))$, то при $\varphi(a) = \varphi(b)$ $\varphi(x) = \varphi(a) \vee (\varphi(x) \wedge \varphi(a)) = \varphi(a)$ по закону поглощения. Такая подрешетка, которая при гомоморфизме отображается в один и тот же элемент, является *выпуклой подрешеткой*.

Выпуклые подрешетки, которые при гомоморфизме могут отображаться в нулевой и единичный элементы, играют особенно важную роль. Например, если к решетке добавлен новый элемент, который меньше всех остальных, то отобразив новый элемент в нулевой, мы получим тот же гомоморфизм, что и раньше. Если этот гомоморфизм отображает a в нулевой элемент и $x \leq a$, то (так как $0 \leq x$) в силу выпуклости, элемент x также переходит в нулевой элемент.

Подрешетка решетки, содержащая вместе с любым элементом a все элементы x , такие, что $x \leq a$, называется *идеалом* решетки, а подрешетка, содержащая вместе с любым элементом a все элементы x , такие, что $a \leq x$, называется *двойственным идеалом* решетки, или *фильтром*.

⇨ **Определение 7.15.** Подмножество J решетки называется *идеалом*, если

- 1) J замкнуто относительно объединения, т.е. если $a \in J$ и $b \in J$, то и $a \vee b \in J$;
- 2) Из $a \in J$ и $x \leq a$ следует, что $x \in J$ (J непусто).

⇨ **Определение 7.16.** Подмножество D называется *двойственным (дуальным) идеалом*, если

- 1) D замкнуто относительно пересечения;
- 2) Из $b \in D$ и $b \leq y$ следует, что $y \in D$ (D не вся решетка).

Любой элемент решетки определяет идеал, состоящий из элементов, которые не больше его. Например, если $a \leq c$ и $b \leq c$, то $a \vee b \leq c$. Если $x \leq a$, то по транзитивности $x \leq c$, а $a \wedge b \leq a$. Отсюда следует замкнутость относительно объединения и пересечения. Полученный идеал обозначим J_c . Элементы, которые не менее c , образуют двойственный идеал D_c .

✱ **Пример.** На рис. 7.10 задано отображение элемента $c \in L$ в $\mathbf{0}$ и элемента f в $\mathbf{1}$ решетки **2**. Для того, чтобы продолжить это отображение до гомоморфизма, необходимо отобразить элементы d, b, a в $\mathbf{0}$, а элемент e — в $\mathbf{1}$ решетки **2**. Тогда элементы $\{a, b, d, c\}$ образуют идеал J_c , а элементы $\{f, e\}$ — двойственный идеал D_f . Если к решетке добавить элемент h , то для продолжения гомоморфизма необходимо отобразить этот элемент в $\mathbf{0}$. Элемент g не принадлежит ни идеалу, ни двойственному идеалу.

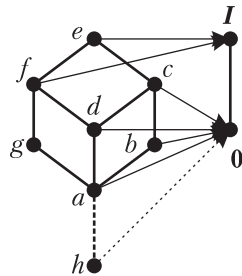


Рис. 7.10. Идеал и двойственный идеал.

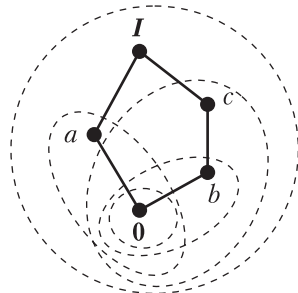


Рис. 7.11. Идеалы решетки N_5 .

Можно показать, что в конечной решетке имеется столько идеалов и двойственных идеалов, сколько она содержит элементов. На рис. 7.11 для решетки N_5 показано пять идеалов, включая всю решетку в целом.

7.5.3. Примарные идеалы

Условия, определяющие идеал и двойственный идеал решетки, двойственны друг другу. Поэтому, если решетку L разбить на две части A и B так, чтобы для части A выполнялось условие (2) определения идеала: из $a \in A$ и $x \leq a$ следует, что $x \in A$ (A непусто), то для части B будет выполняться условие (2) двойственного идеала. Таким образом, A будет идеалом L , а B — двойственным идеалом, и при этом A и B будут дополнять друг друга до полного множества, образующего решетку L .

Условие (2) определения идеала выполняется в том и только том случае, если для B выполняется условие (2) определения двойственного идеала. Действительно, если (2) выполняется для A и некоторый элемент $b \in B$, то при $y \leq b$ элемент y не может принадлежать A , так как тогда оно содержало бы и b , следовательно, $y \in B$. С другой стороны, если (2) выполняется для B и $a \in A$, то всякий элемент $x \leq a$ принадлежит A , поскольку в противном случае элемент a также принадлежал бы и B .

Такое разбиение решетки на подмножества, являющиеся дополнениями друг друга и образующие идеал и двойственный идеал, называют *сечением* решетки. Подмножество A называют *нижним сегментом*, B — *верхним сегментом*.

В общем случае нижний сегмент не является идеалом, а верхний — двойственным идеалом, так как они могут быть пустым множеством и всей решеткой или не удовлетворять условию (2). Но если нижний сегмент удовлетворяет определению идеала, то он называется *примарным идеалом*, или *простым идеалом*, а верхний сегмент *двойственным*, или *дуальным примарным идеалом (фильтром)*.

Примарный и двойственный ему идеалы можно получить, определив гомоморфизм f решетки L в решетку из двух элементов (в решетку **2**), где под действием f в нуль переходят элементы нижнего сегмента, а в единицу — элементы верхнего сегмента, образующие двойственный примарный идеал (см. рис. 7.12). Это обусловлено свойством гомоморфизма сохранять упорядоченность. Если элементы a и b принадлежат верхнему сегменту, то пересечение их $a \wedge b$ также принадлежит верхнему сегменту и отображается в $\mathbf{1}$: $f(a \wedge b) = f(a) \wedge f(b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. Если же a и b принадлежат нижнему сегменту, то $f(a \vee b) = f(a) \vee f(b) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$, т.е. их

объединение отображается в $\mathbf{0}$. Следовательно нижний сегмент является идеалом, а верхний — двойственным идеалом.

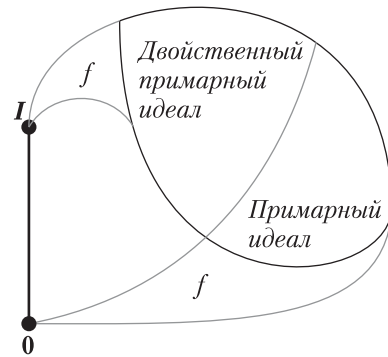


Рис. 7.12. Сечение решетки

$a \wedge b \in J$ либо $a \in J$, либо $b \in J$. Иными словами, если пересечение каких-либо двух элементов принадлежит примарному идеалу, то в нем должен содержаться какой-либо из этих элементов.

Примарный идеал можно рассматривать как нижнюю \wedge -полурешетку, следовательно, в нем содержится пересечение каких-либо элементов a и b . При этом верхняя полурешетка будет двойственным примарным идеалом, который замкнут относительно пересечения. Таким образом, если a и b принадлежат двойственному идеалу D , то $a \wedge b \in D$ также. Следовательно, если $a \wedge b$ не принадлежит D , то он не содержит либо a , либо b , либо a и b вместе.

2. Если для элемента решетки существует дополнение, то любой примарный идеал содержит либо элемент, либо его дополнение.

Если L — решетка с дополнениями, значит это решетка с $\mathbf{0}$ и \mathbf{I} . $\mathbf{0}$ будет элементом идеала J , а \mathbf{I} — двойственного идеала D . Если некоторый элемент a вместе со своим дополнением a' принадлежит одному из идеалов, то так как $a \vee a' = \mathbf{I}$, а $a \wedge a' = \mathbf{0}$, то такой идеал должен быть всей решеткой. Но двойственный идеал не может быть всей решеткой (всем множеством), а примарный идеал — пустым множеством, следовательно, примарный идеал может содержать либо элемент, либо его дополнение.

* Примеры.

Рассмотрим идеалы и примарные идеалы недистрибутивных решеток из пяти элементов (рис. 7.13). Каждый идеал состоит из элементов, которые не больше данного элемента. Этот элемент является объединением всех элементов идеала. Следовательно, в каждой из двух решеток из 5 элементов существует по 5 идеалов.

Это свойство сегментов полностью определяет примарный идеал. Иначе говоря, примарный идеал можно получить, лишь отображая решетку в решетку из двух элементов: примарный идеал образуют элементы, которые при гомоморфизме переходят в нулевой элемент. Рассмотрим некоторые свойства примарных идеалов.

1. Идеал J решетки является примарным идеалом тогда и только тогда, если при

Рассмотрим рис. 7.13, а. Из элементов a, b, c по крайней мере два принадлежат либо J , либо D . Допустим, $a, b \in J$. Если $a \in J$, то любой элемент $x \leq a$ также принадлежит J , т.е. $\mathbf{0} \in J$. Вместе с a, b их объединение принадлежит J , т.е. $a \vee b = \mathbf{I} \in J$. С другой стороны, элемент $c \in J$, так как $c \leq \mathbf{I}$. Следовательно, существует только один примарный идеал, совпадающий со всей решеткой.

Во второй решетке (рис. 7.13, б) существуют два примарных идеала: $[\mathbf{0}, a]$ и $[\mathbf{0}, b, c]$.

Рассмотрим $[\mathbf{0}, a]$. $\mathbf{0} \vee a = a$, $\mathbf{0} \wedge a = \mathbf{0}$. Для a существует единственный элемент $\mathbf{0} \leq a$, следовательно $[\mathbf{0}, a]$ — примарный идеал. Рассмотрим $[\mathbf{0}, b, c]$. $\mathbf{0} \vee b = b$, $\mathbf{0} \wedge b = \mathbf{0}$, $b \vee c = c$, $b \wedge c = b$. Других элементов, меньших b и c нет, кроме нуля, следовательно, $[\mathbf{0}, c]$ — примарный идеал.

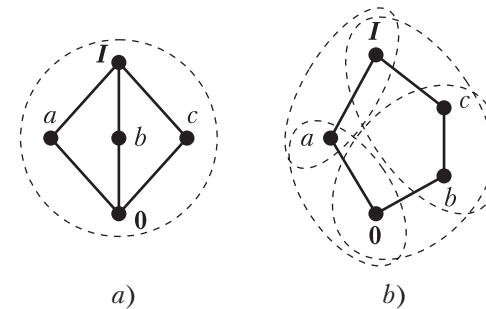


Рис. 7.13. Примарные идеалы.

Наиболее «естественным» представлением решетки является, наверное, дистрибутивная булева решетка множества-степени, т.е. множества всех подмножеств некоторого множества, упорядоченного отношением включения. Для множества из трех элементов это булев гиперкуб (булева решетка 2^3), в котором операции объединения и пересечения совпадают с их теоретико-множественными интерпретациями. Очевидно, было бы полезно научиться строить гомоморфизм, отображающий заданную решетку в решетку подмножеств некоторого множества так, чтобы различные элементы исходной решетки переходили бы в различные подмножества, т.е. строить мономорфизм. Однако такого универсального гомоморфизма не существует, так как решетка подмножеств любого множества дистрибутивна, и, следовательно, может служить представлением только дистрибутивных решеток, для которых данная задача разрешима. Действительно, любую дистрибутивную решетку можно представить некоторой подрешеткой подмножеств определенным образом выбранного множества. Этот результат известен

под названием *теоремы Стоуна*, которую мы здесь приведем без доказательства.

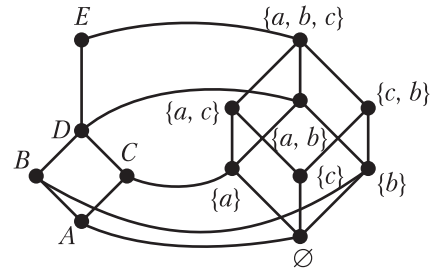


Рис. 7.14. К теореме Стоуна.

Теорема 7.7 (Стоуна о представлении). Для любой дистрибутивной решетки существует мономорфизм, отображающий ее в решетку всех подмножеств некоторого множества, причем так, что дополнение переходит в дополнение.

✱ **Пример.** На рис. 7.14 показан мономорфизм решетки в решетку подмножеств множества $A = \{a, b, c\}$.

Глава 8.

ГРАФЫ

8.1. Основные понятия и определения

С понятием графа обычно связывается его графическое представление, при котором он изображается как множество точек, некоторые из которых соединены линиями. Однако граф отличается от геометрических конфигураций (скажем, фигур, которые также состоят из точек-вершин и линий-сторон) тем, что в графе несущественны расстояния между точками, форма соединяющих линий и углы между ними. Важно лишь, соединена ли данная пара точек линией, или нет. Поэтому граф иногда называют *топологическим объектом*, т. е. объектом, свойства которого не изменяются при растягивании, сжатии, искривлении (но без разрывов и склеиваний). По этой же причине (важно лишь наличие или отсутствие соединения) граф – объект дискретный и может быть задан двумя дискретными множествами: множеством точек, которые будем называть *вершинами*, и множеством линий, соединяющих некоторые вершины. Линии будем называть *ребрами*.

Существуют два основных вида графов – *ориентированные*, в которых линии имеют направление от одной вершины к другой, и *неориентированные*, в которых линии не имеют направления.

↪ **Определение 8.1.** *Неориентированным графом* $G = (V, E)$ называется объект, заданный парой множеств (V, E) , где V – множество *вершин*, $E \subseteq V \times V$ – множество *ребер*.

↪ **Определение 8.2.** *Ориентированным графом (орграфом)* называется граф $D = (V, E)$, где V – множество *вершин*, $E \subseteq V \times V$ – множество *ориентированных ребер*, или *дуг*.

↪ **Определение 8.3.** Граф называется *простым*, если каждую пару вершин соединяет не более, чем одно ребро. Граф называется *мультиграфом*, если хотя бы одну пару вершин соединяет более, чем одно ребро. Ребра мультиграфа, соединяющие одну и ту же пару вершин, называются *кратными*.

В простом графе ребро однозначно определяется парой вершин, которые оно соединяет. В неориентированном графе порядок вершин в паре не важен, поэтому ребра простого неориентированного графа определяются как множество неупорядоченных пар вершин $(v_i, v_j) \in V \times V$. В ориентированном графе упорядоченная пара $(v_i, v_j) \in V \times V$ указывает направление дуги: от вершины v_i к вершине v_j . Она имеет начало (вершину v_i , из которой дуга выходит) и конец (вершину v_j , в которую она заходит). В мультиграфе каждое ребро должно иметь свое собственное имя. Вершины, соединяемые

ребром, не обязательно различны. Ребро, соединяющее вершину v_i с самой собой, т. е. пара (v_i, v_i) , называется *петлей*.

✱ **Примеры.**

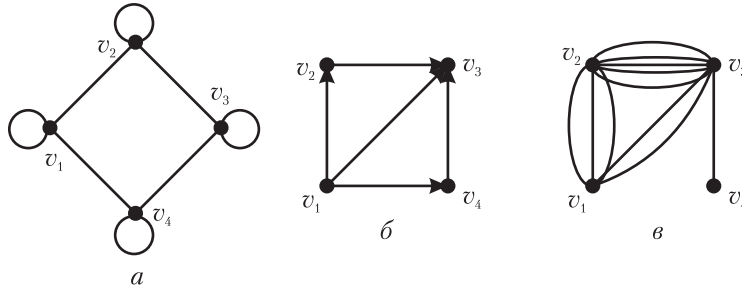


Рис. 8.1. Примеры графов:

а) простой неориентированный граф с петлями G ;

б) ориентированный граф D ;

в) неориентированный мультиграф M .

Граф может вовсе не иметь ребер: $E = \emptyset$. Такой граф называется *пустым*, или *0-графом*.

Для простого графа существует другой крайний случай, когда все вершины соединены между собой ребрами. Такой граф называется *полным*, причем различают два вида полных графов – с петлями и без петель. Полный граф с n вершинами имеет $(n^2 - n)/2$ ребер (число сочетаний из n по 2), если петли не учитываются, и $(n^2 - n)/2 + n = (n^2 + n)/2$ ребер, если добавить n петель. Полный граф с n вершинами без петель обозначается K_n . Понятно, что в мультиграфе ограничений на число ребер нет.

8.2. Неориентированные графы

8.2.1. Матрица смежности

Неориентированный граф задает два отношения между своими элементами: отношение *смежности* и отношение *инцидентности*. *Смежность* – отношение между вершинами: две вершины называются смежными, если они соединены ребром. Это отношение – обычное бинарное отношение на множестве V , которое для простого графа может быть задано квадратной бинарной (т. е. состоящей из нулей и единиц) *матрицей смежности* $A(G) = (a_{ij})$, которая определяется следующим образом:

$$a_{ij} = \begin{cases} 1, & \text{если } (u_i, u_j) \in E, \\ 0, & \text{если } (u_i, u_j) \notin E. \end{cases}$$

Отношение смежности в неориентированном графе всегда симметрично, поскольку порядок вершин в паре (v_i, v_j) не важен. Наличие рефлексивности и транзитивности зависит от конкретных свойств графа. Матрица смежности пустого графа заполнена только нулями, а матрица смежности полного графа с петлями – только единицами. Для мультиграфа матрица смежности уже не является бинарной: в ней $a_{ij} = k$, где k – число кратных ребер, соединяющих вершины v_i и v_j .

✱ **Примеры.**

Матрицы смежности для графов, приведенных на рис. 8.1.

$$A(G) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, A(D) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, A(M) = \begin{pmatrix} 0 & 3 & 2 & 0 \\ 3 & 0 & 4 & 0 \\ 2 & 4 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

8.2.2. Матрица инцидентности

Инцидентность – это отношение между вершинами и ребрами: ребро инцидентно каждой из вершин, которое оно соединяет. Оно задается *матрицей инцидентности* C , в которой строки помечаются именами вершин, а столбцы – именами ребер графа. *Матрица инцидентности* графа определяется как $(n \times m)$ -матрица $C(G) = (c_{ij})$, у которой

$$c_{ij} = \begin{cases} 1, & \text{если вершина } v_i \text{ инцидентна ребру } e_j, \\ 0, & \text{если вершина } v_i \text{ не инцидентна ребру } e_j. \end{cases}$$

Это прямоугольная бинарная матрица, в которой число строк равно числу вершин графа n , а число столбцов – числу ребер m .

Число ребер, инцидентных вершине v_i графа (орграфа, мультиграфа), называется *степенью* этой вершины и обозначается $\deg(v_i)$. Степень вершины можно определить по матрицам инцидентности и смежности. Степень вершины v_i равна числу единиц в i -й строке матрицы инцидентности или матрицы смежности.

Сумма степеней всех вершин равна удвоенному числу ребер, поскольку каждое ребро участвует в степенях двух вершин, т. е. считается в этой сумме два раза. Поскольку эта сумма четна, то и число вершин с нечетными степенями тоже четно.

Вершина, степень которой равна 1, называется *концевой*, или *висячей*.

Граф называется *однородным* степени k , если степени всех его вершин равны k .

↪ **Определение 8.4.** Граф $G' = (V', E')$ называется *частью* графа $G = (V, E)$, если $V' \subseteq V$, а E' – подмножество множества всех ребер G , оба конца которых принадлежат V' .

↪ **Определение 8.5.** Граф $G' = (V', E')$ называется *подграфом* графа $G = (V, E)$, если $V' \subset V$, а E' – множество всех ребер G , оба конца которых принадлежат V' . Множество вершин $V' \subset V$ называют *порождающим множеством* подграфа V' , а сам подграф – *порожденным* вершинами V' .

Всякий подграф графа G является частью G , но не всякая часть – подграф (см. рис. 8.2). Подграф полностью определяется множеством V' своих вершин и может быть построен так: в исходном графе G выбираем множество вершин V' и удаляем все ребра, хотя бы один конец которых не принадлежит V' . Часть графа – это подграф, из которого, возможно, удалены некоторые ребра. Например, часть графа G на рис. 8.2, б содержит вершины v_3, v_4, v_5, v_6 , но не содержит ребер $(v_3, v_4), (v_4, v_5), (v_5, v_6), (v_3, v_6)$, в то время, как его подграф на рис. 8.2, в содержит все ребра, соединяющие эти вершины.

↪ **Определение 8.6.** Часть графа, образованная вершиной v_i и всеми вершинами, смежными с ней, называется *звездой* вершины v_i .

↪ **Определение 8.7.** Полный подграф, порожденный заданным множеством вершин, называется *кликой*.

✱ **Пример.**

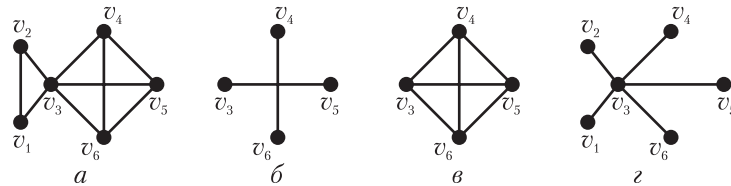


Рис. 8.2.

а) Граф G ; б) Часть графа G ;
в) Подграф графа G , клика; г) Звезда вершины v_3 .

↪ **Определение 8.8.** Подграф G' графа G называется *максимальным* по некоторому свойству, если G' обладает этим свойством, а любой подграф графа G , содержащий G' , не обладает им. Подграф G' графа G называется *минимальным* по некоторому свойству, если G' обладает этим свойством, а любой подграф графа G , содержащийся в G' , не обладает им.

Например, подграф на рис. 8.2, в является максимальной кликой; подграф этого подграфа, порожденный вершинами v_3, v_4, v_5 , также будет кликой, но не максимальной, а минимальной кликой будет подграф, порожденный двумя вершинами, например, v_3 и v_4 .

8.3. Ориентированные графы

Для орграфа его бинарная матрица смежности A в общем случае несимметрична: элемент $a_{ij} = 1$, если и только если имеется дуга $e = (v_i, v_j)$. Число единиц в этой матрице равно числу дуг графа. (Заметим, что в матрице смежности неориентированного графа петле соответствует одна единица, стоящая на главной диагонали, а остальным ребрам – по две единицы, соответствующие элементам, симметричным относительно главной диагонали.) Если же матрица смежности орграфа D оказывается симметричной, то это означает, что для каждой дуги (v_i, v_j) в нем имеется противоположно направленная дуга (v_j, v_i) . Такая матрица совпадает с матрицей смежности неориентированного графа, полученного из D заменой каждой пары противоположно ориентированных дуг (v_i, v_j) и (v_j, v_i) на одно неориентированное ребро (v_i, v_j) . Поэтому симметричный орграф всегда можно заменить простым неориентированным графом, имеющим ту же матрицу смежности. Однако свойство симметричности может выполняться не для всех дуг орграфа; тогда на рисунке изображаются обе противоположно направленные дуги.

Понятие инцидентности для орграфов сохраняется, однако в матрице инцидентности C различают начало и конец дуги.

Матрицей инцидентности орграфа D называется $(n \times m)$ -матрица $C(D) = (c_{ij})$, у которой

$$c_{ij} = \begin{cases} 1, & \text{если вершина } v_i \text{ является концом дуги } e_j, \\ -1, & \text{если вершина } v_i \text{ является началом дуги } e_j, \\ 0, & \text{если вершина } v_i \text{ не инцидентна дуге } e_j. \end{cases}$$

✱ **Пример.**

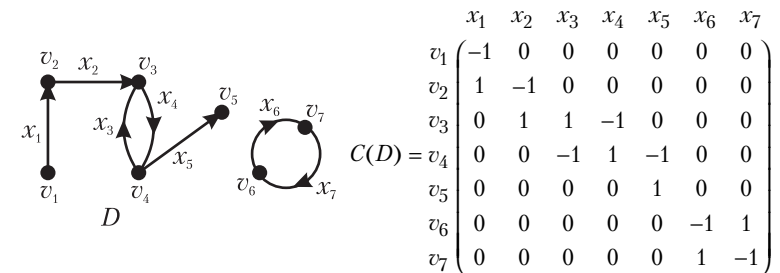


Рис. 8.3. Орграф и его матрица инцидентности.

В каждом столбце матрицы инцидентности находится ровно две единицы: 1 и -1. Вершина v_6 на рис. 8.3. имеет петлю. Чтобы

отобразить ее в матрице инцидентности, вводится дополнительная фиктивная вершина v_7 и петля делится на две дуги: x_6 и x_7 .

Необходимость учитывать ориентацию дуг в орграфе приводит к расщеплению понятия «степень вершины» на две части. *Полустепенью захода* $\deg^+(v_i)$ вершины v_i называется число дуг, входящих в v_i ; *полустепенью исхода* $\deg^-(v_i)$ – число дуг, выходящих из нее. Полустепень исхода v_i равна числу единиц в i -й строке матрицы смежности, полустепень захода v_i – числу единиц в i -м столбце матрицы смежности. Полустепени захода и исхода легко определяются и по матрице инцидентности: сумма положительных единиц в i -й строке определяет полустепень захода вершины v_i , а отрицательных – исхода. Общая сумма дает степень вершины: $\deg(v_i) = \deg^+(v_i) + \deg^-(v_i)$.

Понятие подграфа для орграфа остается тем же. Понятие звезды, как и степень, расщепляется на две части. *Полузвезда захода* вершины v_i – это подграф, определяемый вершиной v_i и всеми вершинами, из которых дуги заходят в вершину v_i . *Полузвезда исхода* вершины v_i – это подграф, определяемый вершиной v_i и всеми вершинами, в которые из v_i идут дуги.

✱ **Пример.**

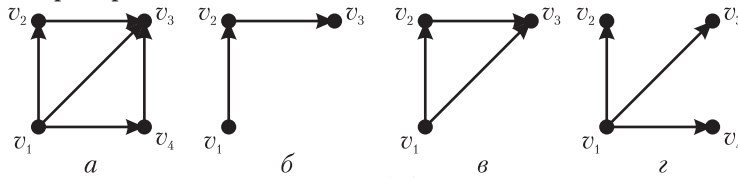


Рис. 8.4.

- а) ориентированный граф D ; б) часть графа D ;
в) подграф графа D , порожденный вершинами v_1, v_2, v_3 ;
г) полузвезда исхода вершины v_1 .

Итак, графы и орграфы могут быть заданы тремя способами:

- непосредственным заданием множеств вершин V и дуг E (например, списком);
- матрицей смежности или матрицей инцидентности (правда, мультиграф матрицей смежности не может быть задан однозначно, поскольку эта матрица не содержит имен ребер);
- рисунком (см. примеры).

Когда два графа одинаковы? Для первых двух способов задания ответ прост: когда совпадают их описания – списки вершин и ребер или матрицы. Визуально, по рисунку, определить, одинаковы ли графы, сложнее. Один и тот же граф можно изобразить разными рисунками, по-разному расположив вершины и придав ребрам разную геометрическую форму и длину.

Например, графы D_1 и D_2 на рис. 8.5 геометрически одинаковы. Однако они отличаются нумерацией вершин, из-за чего матрицы смежности и списки дуг у них будут различны. Например, дуга (v_1, v_3) есть в первом графе, но отсутствует во втором: вместо него появилась дуга (v_4, v_2) . Поэтому множества дуг этих графов различны и, согласно определению 8.2, различны сами графы.

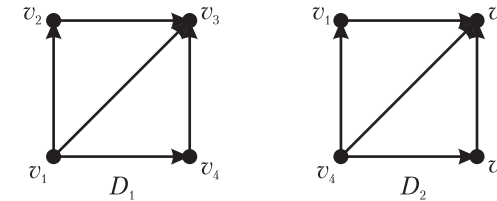


Рис. 8.5. Изоморфизм графов.

Графы, которые отличаются только нумерацией вершин (и которые, следовательно, при некоторой другой нумерации можно сделать одинаковыми), называются *изоморфными*. Изоморфизм графов с небольшим числом вершин иногда можно непосредственно увидеть на рисунке, однако, в общем случае проблема установления изоморфизма графов оказывается сложной в вычислительном отношении задачей.

8.4. Графы и бинарные отношения

Между простыми (без кратных ребер) графами и бинарными отношениями существует взаимно однозначное соответствие. Всякий граф с множеством вершин $V = \{v_1, \dots, v_n\}$ определяет бинарное отношение на множестве V – отношение смежности. Матрица смежности этого графа – это матрица бинарного отношения смежности. Верно и обратное – всякое бинарное отношение ρ на произвольном множестве $M = \{m_1, \dots, m_n\}$ можно представить графом G , вершины которого соответствуют элементам M , а ребро (m_i, m_j) в этом графе существует, если и только если выполняется $m_i \rho m_j$. Бинарная матрица отношения ρ одновременно является матрицей смежности графа G , а сам граф называют графом отношения ρ .

По матрице смежности графа можно определить свойства отношения ρ . Граф рефлексивного отношения содержит петли во всех вершинах и, соответственно, единицы во всех элементах главной диагонали матрицы смежности. Симметричному отношению соответствует граф с симметрической матрицей смежности. Как было отмечено выше, такой орграф равносильен простому неориентированному графу. Граф транзитивного отношения обладает следующим свойством: если существуют ребра (v_i, v_j) и (v_j, v_k) , то

существует ребро (v_i, v_k) . Граф отношения эквивалентности представляет собой совокупность полных подграфов.

Поскольку любой граф представляет некоторое отношение, можно определить операции объединения и пересечения над графами так же, как над отношениями. Дополнению ρ' отношения ρ (т. е. отношению, которое истинно, когда ρ ложно) соответствует дополнение графа G до полного графа, т. е. граф G' , в котором имеются те и только те дуги, которых нет в G . Обратному отношению ρ^{-1} соответствует граф G^{-1} , который получен из графа G изменением ориентации всех его дуг на противоположные.

8.5. Пути и связность в неориентированных графах

8.5.1. Основные определения

➤ **Определение 8.9.** *Путь P_i в неориентированном графе – это последовательность ребер $(v_{i0}, v_{i1}), (v_{i1}, v_{i2}), \dots, (v_{i,n-1}, v_{in})$, такая, что любые два соседние ребра различны и имеют общую инцидентную им вершину. Вершина v_{i0} называется *началом* пути, вершина v_{in} – *концом* пути.*

Путь можно задать также последовательностью вершин, не указывая ребер, например: $v_{i0}, v_{i1}, v_{i2}, \dots, v_{i,n-1}, v_{in}$. В мультиграфе при задании пути нужно указывать имена ребер. Число ребер в пути P называется его *длиной* и обозначается $l(P)$.

Очевидно, что, если в неориентированном графе существует путь из v_{i0} в v_{in} , то существует путь из v_{in} в v_{i0} , – это тот же путь, пройденный в обратном направлении.

Путь называется *циклическим*, или просто *циклом*, если $v_{i0} = v_{in}$. Цикл называется *простым*, если любая вершина графа встречается в нем не более одного раза. Цикл называется *полным*, если в него входят все вершины графа.

Одно и то же ребро может встречаться в пути несколько раз. Путь называется *цепью*, если каждое ребро встречается в нем не более одного раза, и *простой цепью* (или простым путем), если любая вершина графа встречается в нем не более, чем один раз. Простая цепь – это цепь, которая не пересекает сама себя.

Если конец пути P_1 совпадает с началом пути P_2 , то, приписав справа к последовательности ребер P_1 последовательность ребер P_2 , получим новый путь, ведущий из начала P_1 в конец P_2 . Этот путь будем обозначать $P_1 P_2$.

* Пример.

В качестве примера рассмотрим пути и циклы в графе на рис. 8.6. Путь $(v_1, v_2), (v_2, v_5), (v_5, v_7), (v_7, v_6), (v_6, v_8)$ образует

простую цепь. Эту цепь можно задать последовательностью вершин: $v_1, v_2, v_5, v_7, v_6, v_8$. Ни одна вершина в ней не повторяется. Путь $v_1, v_2, v_5, v_7, v_6, v_8, v_7$ не является простой цепью – он содержит цикл v_7, v_6, v_8, v_7 . Путь $v_1, v_2, v_5, v_4, v_3, v_2, v_5, v_7$ не является цепью, так как ребро (v_2, v_5) содержится в нем два раза. Этот путь содержит также цикл v_2, v_5, v_4, v_3, v_2 . Наконец, последовательность $(v_1, v_2), (v_2, v_1)$ не считается циклом, поскольку $(v_1, v_2) = (v_2, v_1)$, так как ребра не ориентированы.

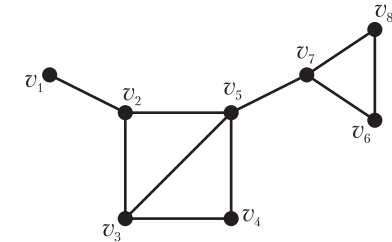


Рис. 8.6. Пути и циклы в неориентированном графе.

➤ **Определение 8.10.** Вершины v_i и v_j называются *связанными*, если существует путь с началом в v_i и концом в v_j . В этом случае говорят также, что вершина v_j *достижима* из вершины v_i . Каждая вершина по определению связана сама с собой путем нулевой длины.

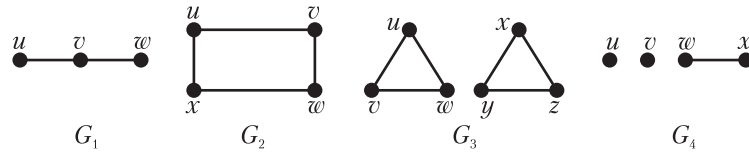
Связанность – это бинарное отношение на множестве вершин. Оно рефлексивно (каждая вершина связана сама с собой по определению), симметрично (для каждого пути имеется обратный путь) и транзитивно. Транзитивность означает, что если есть путь из v_i в v_j и путь из v_j в v_k , то есть путь из v_i в v_k . Это очевидно: чтобы получить такой путь, достаточно к последовательности ребер, ведущей из v_i в v_j , приписать справа последовательность ребер, ведущую из v_j в v_k .

Таким образом, отношение связанности является отношением эквивалентности на множестве вершин графа G и разбивает это множество на непересекающиеся подмножества – классы эквивалентности. Все вершины одного класса связаны между собой, вершины из разных классов между собой не связаны. Подграф, образованный всеми вершинами одного класса, называется *компонентой связности* графа G . Можно дать и другое определение компоненты связности.

➤ **Определение 8.11.** Неориентированный граф называется *связным*, если все его вершины связаны между собой. Максимальный связный подграф графа G называется *компонентой связности* графа G .

Связный граф состоит из одной компоненты связности.

* Пример.

Рис. 8.7. Графы G_1 и G_2 – связные, G_3 и G_4 – несвязные.

Теорема 8.1. Если две вершины связаны между собой, то существует связывающая их простая цепь.

Доказательство. Действительно, если путь, связывающий две вершины, не является простой цепью, то в нем имеется вершина v , инцидентная более чем двум ребрам этого пути. Пусть e_i – первое из этих ребер, e_j – последнее ($j > i + 1$). Тогда из данного пути можно удалить участок от $i + 1$ -го ребра до $j - 1$ -го. Полученная последовательность останется путем: в ней ребра e_i и e_j станут соседними, и при этом они имеют общую вершину v . Если полученный путь не является простой цепью, то процесс повторяется до получения простой цепи. \asymp

↪ **Определение 8.12.** Вершина графа называется *точкой сочленения*, если ее удаление увеличивает число связных компонент графа. Граф называется *разделимым*, если он содержит хотя бы одну точку сочленения, и *неразделимым*, если он не содержит таких точек. Максимальные неразделимые подграфы графа называются его *блоками*.

Например, в графе G на рис. 8.6 вершины v_5 , v_2 , v_7 – точки сочленения.

Теорема 8.2. Вершина v_i является точкой сочленения связного графа G , если и только если существуют такие вершины v_j и v_k , отличные от v_i , что любой путь между ними проходит через v_i .

Доказательство. Пусть v_i – точка сочленения. Ее удаление дает новый граф G' , содержащий несколько связных компонент. Выберем вершины v_j и v_k так, чтобы они лежали в разных компонентах. Тогда в G' между ними пути нет. Но в G (в силу его связности) между ними есть пути (по крайней мере один). Значит, именно удаление v_i разорвало эти пути, и, следовательно, все они проходят через v_i .

Пусть теперь существуют вершины v_j и v_k , указанные в условии теоремы. Тогда удаление v_i разрывает все пути между ними, граф становится несвязным, и, следовательно, v_i – точка сочленения. \asymp

Разделимые графы называют еще 1-связными. Вообще, k -связным называют граф, для нарушения связности которого надо удалить не менее k вершин. Можно сказать, что число связности k характеризует надежность связности. Если граф изображает, например, сеть коммуникаций, то это число говорит о том, что при повреждении любых $k - 1$ узлов сеть все еще обеспечивает связь между любыми оставшимися узлами.

8.5.2. Расстояния. Диаметр, радиус, центр

↪ **Определение 8.13.** В неориентированном графе *расстоянием* $d(v_i, v_j)$ между вершинами v_i и v_j называется минимальная из длин простых цепей, связывающих эти вершины.

Поскольку по определению каждая вершина связана сама с собой, то $d(v_i, v_i) = 0$.

Расстояние $d(v_i, v_j)$ удовлетворяет аксиомам метрики:

1. $d(v_i, v_j) \geq 0$, причем $d(v_i, v_j) = 0$, если и только если $v_i = v_j$;
2. $d(v_i, v_j) = d(v_j, v_i)$;
3. $d(v_i, v_j) + d(v_j, v_k) \geq d(v_i, v_k)$ (неравенство треугольника).

Выполнение первых двух свойств очевидно. Доказательство третьего также несложно. Пусть P_{ij} – кратчайшая цепь из v_i в v_j , P_{jk} – кратчайшая цепь из v_j в v_k . Тогда путь $P_{ij}P_{jk}$, длина которого равна $l(P_{ij}P_{jk}) = l(P_{ij}) + l(P_{jk}) = d(v_i, v_j) + d(v_j, v_k)$, ведет из v_i в v_k . Следовательно, $d(v_i, v_k)$ либо равно $d(v_i, v_j) + d(v_j, v_k)$, либо меньше этой суммы, если существует более короткий путь из v_i в v_k . Следовательно, аксиома 3 выполняется.

↪ **Определение 8.14.** *Диаметром* $d(G)$ графа G называется максимальное из расстояний между его вершинами: $d(G) = \max_{v_i, v_j \in G} d(v_i, v_j)$. *Максимальным удалением* от вершины

v_i называется величина $r(v_i) = \max_{v_j \in G} d(v_i, v_j)$. Вершина v

называется *центром* графа G , если $r(v)$ минимально среди других вершин графа: $r(v) = \min_{v_j \in G} r(v_j)$. Максимальное удаление

$r(v)$ от центра v называется *радиусом* графа G и обозначается $r(G)$.

Число центров и соотношения между радиусом и диаметром в графе могут быть различными. В полном неориентированном графе диаметр и радиус равны единице, и все вершины – центры. Если граф G – простая цепь с нечетным числом $2n + 1$ вершин, то $n + 1$ -я от начала вершина – единственный центр, $d(G) = 2n$, $r(G) = n$. Если же граф G – простая цепь с четным числом $2n$ вершин, то n -я и $n + 1$ -я от начала вершины – два центра, $d(G) = 2n - 1$, $r(G) = n - 1$.

* Пример.

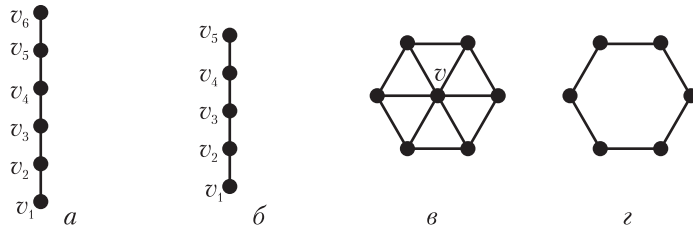


Рис. 8.8. Примеры графов.

Диаметр графа на рис. 8.8, а равен 5, радиус — 3; в графе два центра: вершины v_3, v_4 . Диаметр графа на рис. 8.8, б равен 4, радиус — 2; вершина v_3 — центр графа. В графе на рис. 8.8, в, топологически эквивалентном окружности (вернее, тележному колесу), диаметр $d(G) = 2$, радиус $r(G) = 1$, т. е. диаметр, как и в круге, в два раза больше радиуса; вершина v — центр. В графе на рис. 8.8, г $d(G) = 3$, радиус $r(G) = 3$, и все вершины — центры.

8.5.3. Эйлеров обход

↪ **Определение 8.15.** *Эйлеровым обходом, или эйлеровым циклом, в неориентированном графе (мультиграфе) называется цикл, который содержит все ребра графа в точности по одному разу. Граф называется эйлеровым, если в нем существует эйлеров обход.*

Не всякий граф — эйлеров. Это установил великий математик Л. Эйлер, занимаясь задачей о кёнигсбергских мостах. В городе Кёнигсберге во времена Эйлера было семь мостов (см. рис. 8.9). Задача заключается в том, чтобы, выйдя с любого участка суши, пройти каждый мост по одному разу и вернуться в исходную точку. Эйлер свел эту задачу к задаче нахождения обхода графа на рис. 8.10 и показал, что она не имеет решения. Необходимые и достаточные условия существования эйлерова обхода он сформулировал в следующей теореме.

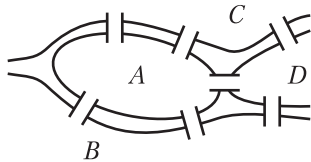


Рис. 8.9. Кёнигсбергские мосты.

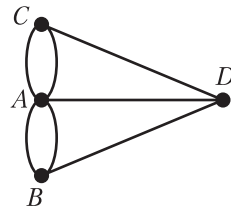


Рис. 8.10. Граф к задаче о кёнигсбергских мостах.

Теорема 8.3. (Л. Эйлер, 1736 г.). Неориентированный граф является эйлеровым тогда и только тогда, когда он связан и все степени его вершин четны.

Доказательство.

Необходимость. Пусть G — эйлеров граф. Эйлеров обход этого графа, проходя через каждую его вершину, входит в нее по одному ребру, а выходит по другому. Это означает, что каждая вершина инцидентна четному числу ребер эйлерова цикла, а поскольку такой цикл содержит все ребра графа G , то отсюда следует четность степеней всех вершин.

Достаточность. Предположим теперь, что степени вершин графа G четны. Пусть цепь P_1 начинается из произвольной вершины v_1 . Будем продолжать ее, насколько возможно, выбирая каждый раз новое ребро. Так как степени всех вершин четны, то, попав в очередную отличную от v_1 вершину, мы всегда будем иметь в распоряжении еще не пройденное ребро. Поэтому цепь P_1 можно продолжить путем добавления этого ребра. Таким образом, построение цепи P_1 закончится в вершине v_1 , то есть P_1 непременно будет циклом. Если окажется, что P_1 содержит все ребра графа G , то это будет требуемый эйлеров цикл. В противном случае, удалив из графа G все ребра цикла P_1 , рассмотрим граф G_1 , полученный в результате такой операции. Поскольку P_1 и G имели вершины только четных степеней, то, очевидно, и G_1 будет обладать тем же свойством. Кроме того, в силу связности графа G , графы P_1 и G_1 должны иметь хотя бы одну общую вершину v_2 . Теперь, начиная с вершины v_2 , построим цикл P_2 в графе G_1 подобно тому, как строили цикл P_1 . Обозначим через P_1', P_1'' части цикла P_1 от v_1 до v_2 и от v_2 до v_1 соответственно. Получим новый цикл $P_3 = P_1' \cup P_2 \cup P_1''$, который, начинаясь в v_1 , проходит по ребрам цепи P_1' до v_2 , а затем обходит все ребра цикла P_2 и, наконец, возвращается в v_1 по ребрам цепи P_1'' (рис. 8.11).

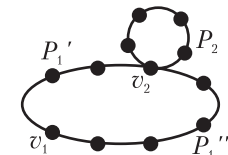


Рис. 8.11. Граф к доказательству теоремы Эйлера.

Если цикл P_3 не эйлеров, т. е. содержит еще не все ребра графа, то, проделав аналогичные построения, получим еще больший цикл, и т. д. Этот процесс закончится построением эйлерова цикла. ▀

* Примеры.

На рис. 8.12 показан эйлеров граф. Помимо задачи о кёнигсбергских мостах, известен ряд других старинных занимательных задач и головоломок, решение которых сводится к выяснению вопроса, является ли граф эйлеровым. В одной из них требуется

обрисовать фигуру, именуемую саблями (знаком) Магомета (рис. 8.13), не отрывая карандаша от бумаги и не повторяя линий.

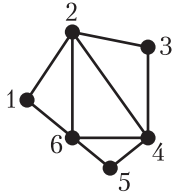


Рис. 8.12. Эйлеров граф.

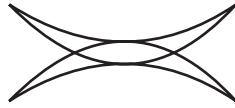


Рис. 8.13. Сабля Магомета.

8.5.4. Гамильтонов цикл

↪ **Определение 8.16.** Цикл в неориентированном графе называется *гамильтоновым*, если он содержит все вершины графа в точности по одному разу. Граф называется *гамильтоновым*, если в нем существует гамильтонов цикл.

Задача нахождения гамильтонова цикла, поставленная английским математиком Гамильтоном, при всем сходстве ее формулировки с задачей об эйлеровом обходе, оказывается гораздо более сложной. Простые критерии существования гамильтонова цикла неизвестны. В то же время интерес к ее решению велик, поскольку она имеет естественную прикладную интерпретацию. Если рассматривать граф как транспортную сеть, вершины которой – города, а ребра – пути между городами, то задача о гамильтоновом цикле оказывается частным случаем известной «задачи о коммивояжере»: объехать все города, побывав в каждом ровно один раз и вернуться в исходный город. Более сложная постановка этой задачи связана со случаем, когда разные пути имеют разную цену в стоимости или длительности; тогда требуется найти обход всех городов с минимальной ценой.

8.6. Пути и связность в ориентированных графах

В ориентированных графах ряд понятий совпадает с аналогичными для неориентированных графов. Однако, в литературе часто одни и те же понятия имеют различные названия. В основном мы будем придерживаться одинаковой терминологии как для ориентированных, так и для неориентированных графов.

↪ **Определение 8.17.** *Путь* P_i в ориентированном графе – это последовательность дуг $(v_{i0}, v_{i1}), (v_{i1}, v_{i2}), \dots, (v_{i_{n-1}}, v_{in})$, такая, что конец любой дуги совпадает с началом следующей. Вершина v_{i0} называется *началом* пути, вершина v_{in} – *концом* пути.

Другое обозначение пути – последовательность вершин $v_0, v_1, \dots, v_{n-1}, v_n$, которые соединены дугами в направлении стрелок. В дальнейшем мы именно так и будем обозначать путь в орграфе.

Понятия цикла, цепи, простой цепи, длины пути и цикла, гамильтонова цикла без изменения переносятся на орграфы. (Цикл в орграфе называют иначе *контуром*).

На рис. 8.14 изображено несколько орграфов. В орграфе D_7 u, v, w – простая цепь, а u, v, y, x, v, w – цепь, не являющаяся простой, поскольку вершина v встречается в ней дважды. Путь u, v, y, x, u является простым циклом, но не является гамильтоновым (полным) циклом. Путь u, v, w, x, u в графе D_4 является циклом; он является также простым, гамильтоновым и эйлеровым циклом. В графе D_6 путь u, v, u является циклом, но не является полным циклом, так как он содержит не все вершины графа.

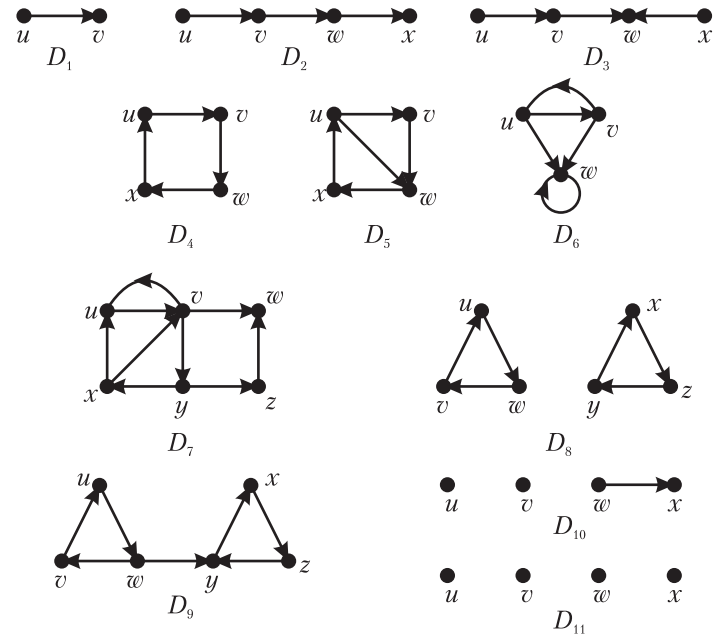


Рис. 8.14. Примеры орграфов.

Другие понятия, и, прежде всего, связность и достижимость, существенно изменяются для орграфов.

↪ **Определение 8.18.** Вершина v_j *достижима* из вершины v_i , если существует путь с началом в v_i и концом в v_j . По определению полагаем, что любая вершина достижима из себя самой.

Для орграфов верно утверждение, аналогичное теореме 8.1.

Теорема 8.1'. Если вершина v_j достижима из вершины v_i , то существует простой путь из v_i в v_j .

Для сетей коммуникаций теорема 8.1' имеет следующую прозрачную интерпретацию: если некоторое лицо имеет возможность отправить сообщение другому лицу через цепочку посредников, то сможет это сделать так, что ни один посредник не передаст это сообщение дважды.

↪ **Определение 8.19.** *Полупуть* в ориентированном графе – это последовательность дуг, такая, что любые две соседние дуги различны и имеют общую инцидентную им вершину. Иначе говоря, полупуть – это путь, который проходится без учета ориентации дуг. Говорят, что вершины u и v в орграфе *соединимы*, если v можно достичь из u , не обязательно следуя по дугам в направлении их ориентации, т. е., если между ними существует полупуть.

Отношение достижимости между вершинами в орграфах несимметрично: если v_j достижима из v_i , то v_i не обязательно достижима из v_j . Однако полупуть из v_j в v_i в этом случае существует всегда. Возможен случай, когда между вершинами нет пути ни в одну, ни в другую сторону, но есть полупуть. Например, на рис. 8.14 в графе D_3 не существует пути из вершины u в вершину x , однако существует полупуть u, v, w, x .

В связи с несимметричностью отношения достижимости, расстояние между двумя вершинами орграфа $d(u, v)$ не удовлетворяет всем аксиомам метрики (см. определение 8.13). В частности, оно не обязательно симметрично: в общем случае $d(u, v) \neq d(v, u)$. В качестве примера рассмотрим орграф D_7 на рис. 8.14: $d(x, v) = 1$, $d(v, x) = 2$. При отсутствии пути между двумя вершинами расстояние считается либо неопределенным, либо бесконечным. Например, в графе D_7 расстояние $d(w, u)$ не определено. (Иногда в таких случаях расстояние между двумя вершинами в орграфах определяется как длина полупути между ними.)

Неравенство треугольника имеет место в том случае, если вершина v достижима из u и w достижима из v . Действительно, пусть $d(u, v) = s$, $d(v, w) = t$ и $u, u_2, u_3, \dots, u_s, v$ – кратчайший путь из u в v , а $v, v_2, v_3, \dots, v_t, w$ – кратчайший путь из v в w . Тогда $u, u_2, u_3, \dots, u_s, v, v_2, v_3, \dots, v_t, w$ – путь длины $s + t$ из u в w , и мы заключаем, что $d(u, v) \leq d(u, v) + d(v, w)$.

8.6.1. Виды связности орграфов

В орграфах существуют различные виды связности, которые описываются следующим определением.

↪ Определение 8.20.

1. Орграф $D = (V, E)$ называется *сильно связным*, или *сильным*, если любые две его вершины достижимы друг из друга (т. е. если между ними существуют пути в обе стороны).

Например, орграфы D_4, D_5 на рис. 8.14 сильно связны, тогда как другие орграфы – нет. Например, в орграфе D_9 вершины x, y, z не достижимы из вершин u, v, w .

Если сеть коммуникаций сильно связна, то каждое лицо может передать сообщение любому другому лицу.

2. Орграф называется *односторонне связным*, или *односторонним*, если для любой пары вершин хотя бы одна достижима из другой, т. е. если существует путь между ними хотя бы в одну сторону.

Например, орграфы D_1, D_2, D_9 на рис. 8.14 односторонне связны. Орграф D_3 не односторонний, так как вершины u и x недостижимы друг для друга.

Сеть коммуникаций является односторонне связной, если для каждой пары ее членов по крайней мере один может послать сообщение другому.

3. Орграф называется *слабо связным*, или *слабым*, если каждая пара вершин соединима, т. е., если между любой парой вершин существует полупуть. Например, орграф D_3 на рис. 8.14 слабо связан, тогда как орграф D_8 – нет, так как вершины u и x не соединимы.

4. Орграф называется *несвязным*, если между некоторой парой вершин нет полупути (т. е. если он не является слабо связным).

Примеры несвязных графов на рис. 8.14: D_8, D_{10}, D_{11} .

Отметим, что эти четыре свойства упорядочены по включению: граф, обладающий одним из этих свойств, обладает всеми свойствами, которые в этом определении «ниже» него. Так, сильно связный граф обладает свойствами 2 – 4 и т. д.

8.6.2. Критерии связности

Проверка сильной, слабой или односторонней связности путем непосредственного использования определений может оказаться очень трудоемкой, поскольку в орграфе с n вершинами имеется $n(n-1)/2$ пар вершин. В этом параграфе будут приведены критерии принадлежности к каждому из трех классов орграфов: сильных, односторонних и слабых.

В сильно связном графе любая вершина v_i входит по крайней мере в один цикл, образованный путями из v_i в некоторую другую

вершину v_j и обратно из v_j в v_i . Циклы, проходящие через v_i и другие вершины графа, не обязательно все различны. В частности, сильно связный граф, содержащий n вершин, может представлять собой один простой цикл, проходящий через все вершины.

Теорема 8.4. Оргграф сильно связан тогда и только тогда, когда в нем имеется полный цикл, т. е. цикл, проходящий через все вершины.

Доказательство. Пусть $u_1, u_2, \dots, u_p, u_1$ — полный цикл. Тогда любая пара вершин u_i, u_j в нем содержится. Будем считать, что $i < j$. Тогда u_i, u_{i+1}, \dots, u_j — путь из u_i в u_j , а $u_j, u_{j+1}, \dots, u_p, u_1, \dots, u_i$ — путь из u_j в u_i . Таким образом, оргграф D сильно связан.

Обратно, предположим, что D сильно связан. Пусть вершинами в D являются u_1, u_2, \dots, u_n . Тогда имеются пути P_1 из u_1 в u_2 , P_2 из u_2 в u_3, \dots, P_{n-1} из u_{n-1} в u_n , P_n из u_n в u_1 . Полный цикл в D можно построить объединением этих путей в следующем порядке: $P_1, P_2, \dots, P_{n-1}, P_n$. ∞

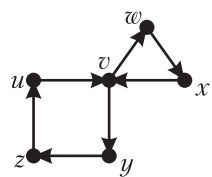


Рис. 8.15. Пример к теореме 8.4.

Для иллюстрации этой теоремы рассмотрим оргграф D на рис. 8.15. Он сильно связан, потому что последовательность v, y, z, u, v, w, x, v образует полный цикл. Чтобы использовать теорему 8.4 для проверки сильной связности оргграфа D , перенумеруем вершины u_1, u_2, \dots, u_n . Затем проверим, существует ли путь из u_1 в u_2 , из u_2 в u_3, \dots , из u_{n-1} в u_n и из u_n в u_1 .

В терминах сетей коммуникаций теорема 8.4 утверждает, что для того, чтобы каждое

лицо могло отправить сообщение любому другому лицу, необходимо (и достаточно) наличие последовательности лиц со следующими свойствами: 1) каждое из них может связаться со следующим; 2) в последовательности представлены все участники сети; 3) последнее лицо может связаться с первым.

Теорема 8.5. Оргграф D односторонне связан тогда и только тогда, когда в нем имеется полный путь.

В качестве иллюстрации этой теоремы заметим, что оргграф D_7 на рис. 8.14 односторонне связный, потому что в нем имеется полный путь x, u, v, y, z, w . Граф D_2 также односторонне связный.

Доказательство. Для доказательства теоремы предположим, что u_1, u_2, \dots, u_l — полный путь. Тогда любые вершины u_i, u_j в нем содержатся. Если $i < j$, то u_i, u_{i+1}, \dots, u_j — путь из u_i в u_j . Таким образом, D — односторонний оргграф.

Обратно, предположим, что D — односторонний оргграф. Сначала докажем предварительный результат.

Лемма 8.1. В любом подмножестве вершин одностороннего графа D существует вершина, из которой достижимы (путем использования дуг D) все другие вершины в этом множестве.

Оргграф D_9 на рис. 8.14 иллюстрирует лемму. Он является односторонне связным. Во множестве $\{u, v, x\}$ из вершины u достижимы все другие. В множестве $\{x, y\}$ таким свойством обладает вершина x , а в множестве $\{u, v, w, x, y, z\}$ — вершина u и т. д.

Доказательство леммы проведем индукцией по числу вершин k в произвольном множестве U . При $k = 1$ лемма верна, так как каждая вершина достижима сама из себя. Предположим, что она верна для всех множеств с k вершинами, и выберем некоторое множество U , содержащее $k+1$ вершину. Обозначим элементы U через v_1, v_2, \dots, v_{k+1} . По предположению индукции в $U \setminus \{v_{k+1}\}$ существует вершина v_j , из которой достижимы все v_i при $j < k+1$. Теперь, поскольку оргграф D односторонний, либо v_i достижима из v_{k+1} , либо v_{k+1} достижима из v_i . Если v_{k+1} достижима из v_i , то из v_i достижимы все вершины в U . Если v_i достижима из v_{k+1} , то из v_{k+1} достижимы все вершины в U . Это доказывает лемму.

Теперь, используя лемму, продолжим доказательство теоремы. Выберем в множестве вершин V оргграфа D вершину u_1 , из которой достижимы все другие вершины в V . Выберем в $V \setminus \{u_1\}$ вершину u_2 , из которой достижимы все другие вершины в $V \setminus \{u_1\}$. Выберем в $V \setminus \{u_1, u_2\}$ вершину u_3 , из которой достижимы все другие вершины в $V \setminus \{u_1, u_2\}$, и т. д. Далее, u_n достижима из u_1 по пути P_1 , u_3 достижима из u_2 по пути P_2 и т. д. Объединение этих путей дает полный путь оргграфа D . ∞

Оргграф D_7 на рис. 8.14 иллюстрирует доказательство теоремы 8.4. Возьмем $u_1 = y, u_2 = x, u_3 = u, u_4 = v, u_5 = z, u_6 = w$. Тогда $P_1 = \{y, x\}, P_2 = \{x, u\}, P_3 = \{u, v\}, P_4 = \{v, y, z\}, P_5 = \{z, w\}$. Полный путь задается вершинами y, x, u, v, y, z, w . (В этом оргграфе существует даже полный простой путь. Имеется ли такой путь для каждого одностороннего оргграфа?)

Теорема 8.6. Оргграф D слабо связан тогда и только тогда, когда в нем имеется полный полупуть.

Доказать самостоятельно. ∞

Для иллюстрации этой теоремы заметим, что оргграф D_3 на рис. 8.14 — слабо связный, поскольку последовательность вершин u, v, w, x образует полный полупуть. При этом он не является односторонним, так как в нем не существует полного пути. Граф D_9 является слабо связным и односторонним.

8.7. Исследование орграфов с помощью матриц

Значительную часть информации относительно орграфа D можно представить в удобной форме, используя матрицы, соответствующие орграфу D . Определим следующие операции над матрицами. Пусть $A = (a_{ij})$ и $B = (b_{ij})$ – две матрицы $n \times n$. Тогда

$A + B = (a_{ij} + b_{ij})$ – поэлементное сложение матриц A, B ,

$A \times B = (a_{ij} \times b_{ij})$ – поэлементное произведение A и B ,

$AB = (c_{ij})$, где $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$, – произведение A и B .

Транспонированной матрицей A' к матрице A является матрица (a'_{ij}) , в которой $a'_{ij} = a_{ji}$.

Определим булево преобразование $B: N \rightarrow \{0,1\}$ следующим образом:

$$B(x) = \begin{cases} 0, & \text{если } x = 0, \\ 1, & \text{если } x > 0. \end{cases}$$

Тогда преобразование $B(A)$ для матрицы $A = (a_{ij})$ означает, что элемент (i, j) в $B(A)$ равен $B(a_{ij})$. Например:

$$B \begin{pmatrix} 1 & 8 & 5 \\ 0 & 2 & 0 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

В результате получаем бинарную матрицу.

Будем обозначать через I диагональную единичную матрицу (матрицу, в которой на главной диагонали стоят единицы, а все остальные элементы равны нулю), и через J – единичную матрицу, в которой все элементы равны единице.

8.7.1. Матрицы орграфов и их связь с путями

Матрицу смежности $A(D)$ орграфа D можно использовать для подсчета числа различных путей в D . Сама матрица A задает дуги D , т. е. пути длины 1. Оказывается, что матрица A^l (l -я степень A) задает число путей длины l .

Теорема 8.7. Элемент $(i, j) = c_{ij}^{(l)}$ матрицы A^l орграфа D равен числу путей длины l из v_i в v_j .

Доказательство теоремы проведем индукцией по l . Для $l = 1$ теорема очевидна: матрица смежности задает пути длиной 1.

Пусть для некоторого l теорема верна, т. е. элемент $c_{ij}^{(l)}$ матрицы A^l равен числу путей длины l из v_i в v_j . Докажем ее для $l + 1$. Любой путь длины $l + 1$ из v_i в v_j состоит из дуги, ведущей из v_i в смежную

с ней вершину v_k , и затем пути длины l из v_k в v_j . Число путей длины $l + 1$ из v_i в v_j , проходящих на первом шаге через вершину v_k , равно $a_{ik}c_{kj}^{(l)}$ (если дуги из v_i в v_k нет, то $a_{ik} = 0$, и $a_{ik}c_{kj}^{(l)} = 0$, а если такая дуга есть, то $a_{ik}c_{kj}^{(l)} = c_{kj}^{(l)}$, так как $a_{ik} = 1$). Общее число путей длины $l + 1$ из v_i в v_j получим, если просуммируем эту

величину по всем k : $\sum_{k=1}^n c_{ik}c_{kj}^{(l)}$. Эта сумма равна элементу (i, j) произведения матриц A и A^l , т. е. элементу (i, j) матрицы A^{l+1} , что и доказывает теорему. ∞

Следствие. Элемент (i, j) матрицы $A + A^2 + \dots + A^l$ орграфа D равен числу всех путей длины $\leq l$ из v_i в v_j .

✱ **Пример.** На рис. 8.16 приведены матрицы смежности A, A^2, A^3 и A^4 , соответствующие орграфу D . Матрица A^2 показывает число путей длины два: поскольку элемент a_{11} в A^2 равен 1, в D существует путь длины 2 из u_1 в u_1 . Действительно, это цикл u_1, u_2, u_1 . Элемент $a_{13} = 1$, т. е. в D существует путь длины 2 из u_1 в u_3 : u_1, u_2, u_3 , и т. д. Элемент $a_{21} = 2$ в A^3 , следовательно, существует два пути длины 3 из u_2 в u_1 . Эти пути – u_2, u_1, u_1 и u_2, u_3, u_1 . Аналогично интерпретируются другие элементы матриц A^2, A^3, A^4 и т. д.

Нетрудно заметить, что если в графе нет циклов, матрица A^n станет нулевой через определенное (какое?) число шагов.

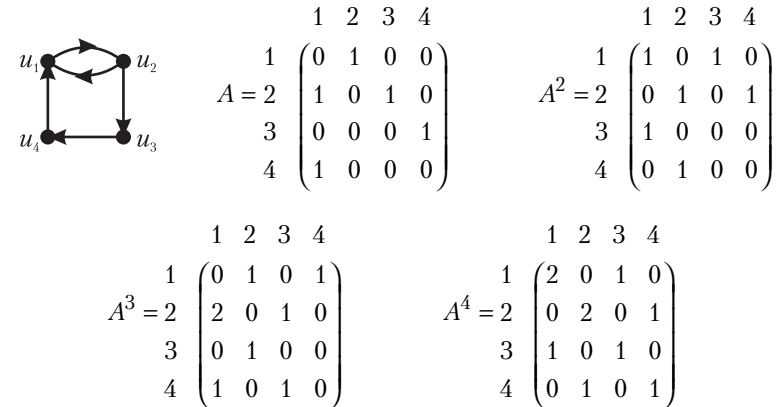


Рис. 8.16. Степени матрицы смежности орграфа D .

8.7.2. Матрица расстояний

Новая матрица, которая оказывается полезной при рассмотрении орграфов, – матрица расстояний (d_{ij}) , где d_{ij} – расстояние от u_i

до u_j , определяемое как длина кратчайшего пути из u_i в u_j . (Напомним, что величина d_{ij} не определена, если пути из u_i в u_j нет.)

Теорема 8.8. Пусть орграф D имеет матрицу смежности A и матрицу расстояний (d_{ij}) . Тогда, если величина d_{ij} , $i \neq j$ определена, то она равна наименьшему k , для которого элемент (i, j) в A^k не равен 0.

Доказать теорему предоставляется читателю самостоятельно. \simeq

Следуя этой теореме, можно построить матрицу расстояний, последовательно возводя в степень матрицу смежности орграфа. На рис. 8.16 приведены степени матрицы смежности орграфа D . Используем их для получения матрицы расстояний этого графа (см. рис. 8.17).

1. Матрица расстояний имеет нули на главной диагонали и в начале совпадает с матрицей смежности, т. е. она содержит все пути длины 1. Остальные элементы матрицы расстояний пока не определены.

2. Матрица A^2 указывает все пути длины 2. Неопределенным элементам матрицы расстояний d_{ik} присваиваем значение 2, если $a_{ik}^{(2)} \neq 0$.

3. Тем элементам d_{ik} , которые еще не определены, присваиваем значение 3, если элементы $A^3 a_{ik}^{(3)} \neq 0$.

Теперь матрица расстояний полностью определена.

$$1). d(D) = \begin{pmatrix} 0 & 1 & x & x \\ 1 & 0 & 1 & x \\ x & x & 0 & 1 \\ 1 & x & x & 0 \end{pmatrix} \quad 2). d(D) = \begin{pmatrix} 0 & 1 & 2 & x \\ 1 & 0 & 1 & 2 \\ 2 & x & 0 & 1 \\ 1 & 2 & x & 0 \end{pmatrix} \quad 3). d(D) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

Рис. 8.17. Вычисление матрицы расстояний орграфа D .

Теорема 8.9. Для того, чтобы n -вершинный орграф с матрицей смежности A имел хотя бы один цикл, необходимо и достаточно, чтобы матрица $K = A^2 + A^3 + \dots + A^n$ имела хотя бы один не нулевой диагональный элемент.

Использование матриц позволяет получить и перечисление конкретных путей. Для этого всем дугам графа D присвоим конкретные имена (например, e_1, \dots, e_m), и в матрице A заменим единицы именами соответствующих дуг, т. е. элемент $a_{ij} = 1$ заменим именем дуги, которая соединяет вершину v_i с вершиной v_j . Полученную матрицу обозначим через $H(D)$. Для того, чтобы определить произведение матриц этого вида, введем алгебру на множествах путей.

Путь будем рассматривать как слово (последовательность символов) в алфавите $\{e_1, \dots, e_m\}$. Пусть даны два множества путей M_1 и

M_2 . Сумма M_1 и M_2 определяется как их обычное теоретико-множественное объединение: $M_1 \cup M_2$, произведение $M_1 \cdot M_2$ – как множество, получаемое приписыванием справа к каждому слову из M_1 всех слов из M_2 . Например, если $M_1 = \{e_2 e_4 e_2, e_3 e_1, e_1\}$, $M_2 = \{e_3 e_1 e_4, e_2\}$, то $M_1 \cdot M_2 = \{e_2 e_4 e_2 e_3 e_1 e_4, e_2 e_4 e_2 e_2, e_3 e_1 e_3 e_1 e_4, e_3 e_1 e_2, e_1 e_3 e_1 e_4, e_1 e_2\}$. (Такую операцию называют *конкатенацией*.) Пустое множество \emptyset играет здесь роль нуля: $M_1 \cdot \emptyset = \emptyset \cdot M_2 = \emptyset$. Поэтому вместо \emptyset будем, как и в матрице A , писать 0. Очевидно, что операция конкатенации некоммукативна. Она имеет простой смысл: если M_1 – множество всех путей, ведущих из v_i в v_j , а M_2 – множество всех путей, ведущих из v_j в v_k , то $M_1 \cdot M_2$ – это множество всех путей, ведущих из v_i в v_k и проходящих через v_j .

С помощью этих операций определим произведение $Z = X \cdot Y$ квадратных матриц X и Y одинаковой размерности n , элементами которых являются множества слов (такие матрицы назовем словарными):

$$z_{ij} = \bigcup_{k=1}^n x_{ik} \cdot y_{kj}.$$

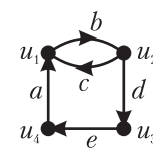
В этой формуле роль суммы элементов играет теоретико-множественное объединение, а произведения – определенная выше конкатенация. Степень матрицы H определяется по индукции формулой $H^{l+1} = H \cdot H^l$.

Теорема 8.10. Элемент $(i, j) = h_{ij}^{(l)}$ матрицы H^l орграфа D представляет собой множество всех путей длины l из v_i в v_j .

Доказательство почти дословно совпадает с доказательством теоремы 8.7. \simeq

Следствие. Элемент (i, j) матрицы $H \cup H^2 \cup \dots \cup H^l$ орграфа D равен множеству всех путей длины $\leq l$ из v_i в v_j .

* Пример.



$$H = \begin{pmatrix} 0 & b & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & e \\ a & 0 & 0 & 0 \end{pmatrix} \quad H^2 = \begin{pmatrix} bc & 0 & bd & 0 \\ 0 & cb & 0 & de \\ ea & 0 & 0 & 0 \\ 0 & ab & 0 & 0 \end{pmatrix}$$

$$H^3 = \begin{pmatrix} 0 & bcb & 0 & bde \\ bcb \cup dea & 0 & cbd & 0 \\ 0 & eab & 0 & 0 \\ abc & 0 & abd & 0 \end{pmatrix}$$

Рис. 8.18. Матрица путей в орграфе.

8.7.3. Матрица достижимости

Матрица достижимости $R(D) = (r_{ij})$ определяется следующим образом:

$$r_{ij} = \begin{cases} 1, & \text{если } u_j \text{ достижима из } u_i, \\ 0, & \text{если } u_j \text{ не достижима из } u_i. \end{cases}$$

Всякая вершина достижима сама из себя, поэтому $r_{ii} = 1$ для всех i . На рис. 8.19 представлены матрицы смежности, расстояний и достижимости для некоторых орграфов.

Матрица достижимости может быть получена при помощи матрицы смежности.

Теорема 8.11. Пусть A – матрица смежности и R – матрица достижимости орграфа D с n вершинами. Тогда

$$R = B(I + A + A^2 + \dots + A^{n-1}) = B[(I + A)^{n-1}],$$

где B – булево преобразование, а I – единичная диагональная матрица.

Доказательство. Действительно, по теореме 8.1', если v_j достижима из v_i , то существует простая цепь из v_i в v_j . Длина этого пути не превосходит $n - 1$, поскольку в простой цепи вершины не повторяются. Согласно следствию из теоремы 8.5, в этом случае элемент (i, j) матрицы $I + A + A^2 + \dots + A^{n-1}$ будет ненулевым, откуда и следует наша теорема. ∞

В следующей теореме будет показано применение матрицы достижимости как метода определения связности орграфа.

Теорема 8.12. Пусть орграф D имеет матрицу достижимости R и матрицу смежности A . Тогда

- 1) D сильно связан тогда и только тогда, когда $R = J$;
- 2) D односторонне связан тогда и только тогда, когда $B(R + R') = J$;
- 3) D слабо связан тогда и только тогда, когда $B[(I + A + A')^{n-1}] = J$, где J – единичная матрица.

8.8. Вершинные базы и сети коммуникаций

8.8.1. Сильные компоненты и вершинная база

Предположим, мы хотим передать сообщение по сети коммуникаций так, чтобы оно могло достигнуть всех ее участников. Если сеть сильно связна, достаточно передать сообщение любому одному лицу. (В действительности, по теореме 8.4, достаточно односторонней связности сети, но в этом случае надо будет передать сообщение определенному лицу.) Однако, если граф не является сильно связным, то

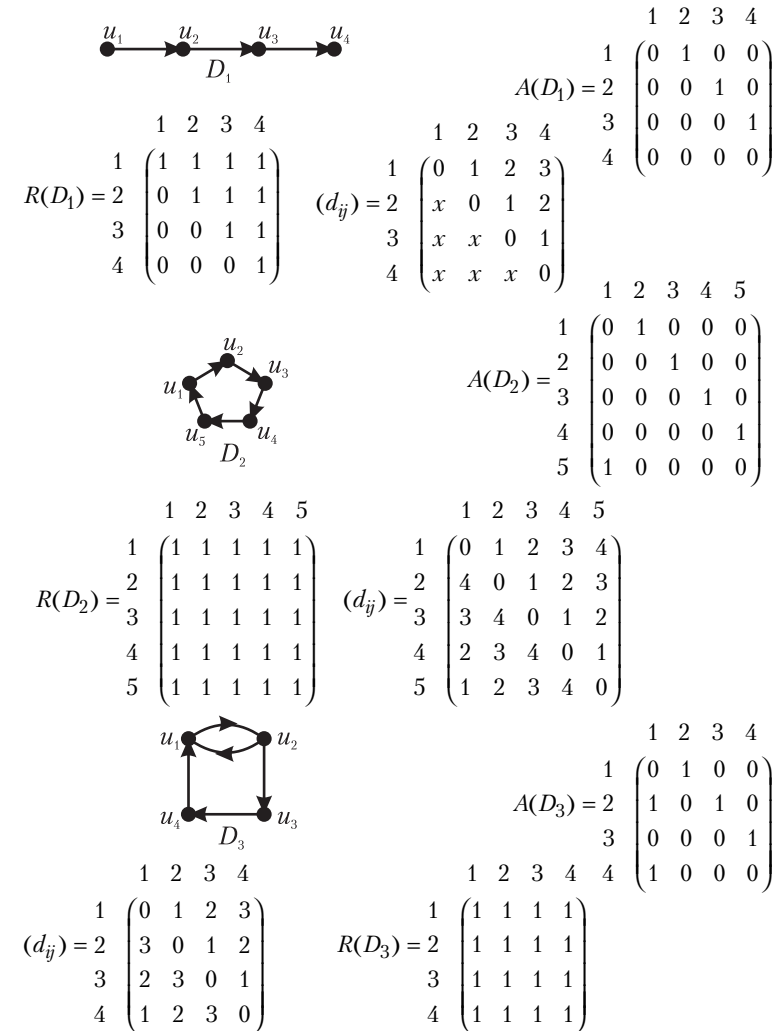


Рис. 8.19. Матрицы расстояний и достижимости для орграфов.

сообщение, переданное одному лицу, не всегда достигнет всех участников. В таком случае возникает задача нахождения множества вершин, из которых достижимы все другие вершины, причем желательно, чтобы это множество содержало наименьшее число вершин.

↪ **Определение 8.21.** Совокупность вершин B орграфа D называется его *вершинной базой* (или базой вершин), если каждая вершина, не входящая в B , достижима из некоторой вершины в B , и множество B – минимально. Здесь *минимальность* B означает, что ни из какого собственного подмножества B нельзя достичь всех оставшихся вершин D .

Для примера рассмотрим орграф, изображенный на рис. 8.20. Найдем вершинную базу с наименьшим числом элементов, исходя из ее определения. Вершина t не имеет входящих дуг, поэтому мы должны включить ее в вершинную базу. Вершины u, v, w недостижимы из p, q, r, s , но каждая из них достижима друг для друга, поэтому одна из них должна входить в любую из вершинных баз.

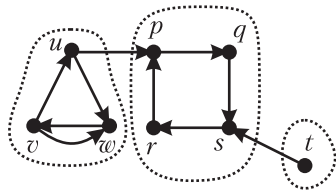


Рис. 8.20. Сильные компоненты орграфа.

В этом параграфе будет приведена процедура нахождения всех вершинных баз данного орграфа. Большинство результатов принадлежит Кёнигу. Чтобы описать процедуру Кёнига, введем некоторые предварительные определения.

↪ **Определение 8.22.** Максимальный сильно связный подграф орграфа D называется *сильно связной компонентой* D (*сильной компонентой связности*).

Например, на рис. 8.20 подграф, порожденный вершинами v, w , является сильно связным, однако он не является сильной компонентой, так как входит в сильный подграф, порожденный вершинами u, v, w , т. е. не является максимальным по свойству сильной связности. Другой сильной компонентой является подграф, порожденный вершинами p, q, r, s , – все они достижимы друг для друга, так как входят в один цикл. Одна вершина t также является сильной компонентой. Сильные компоненты обладают следующими свойствами.

поскольку подмножество $\{t, u\}$ уже обладает требуемым свойством. В действительности множества $\{t, u\}$, $\{t, v\}$ и $\{t, w\}$ образуют все вершинные базы. Как видно, все они имеют одинаковое число вершин, и это не случайно. Таким образом, поиск вершинной базы с наименьшим числом элементов заканчивается сразу, как только находится произвольная вершинная база.

Теорема 8.13. В орграфе $D = (V, E)$ каждая вершина u входит в одну и только одну сильную компоненту.

Доказательство. Вершина u входит по меньшей мере в одну сильную компоненту. В самом деле, подграф, порожденный u , является сильным (так как каждая вершина достижима сама для себя). Будем добавлять вершины до тех пор, пока будут все еще получаться сильно связанные подграфы. Такая процедура приводит к сильно связной компоненте, содержащей u . Предположим теперь, что u входит в сильные компоненты K и L . Рассмотрим подграф, порожденный вершинами из K и L . Этот подграф сильно связан, так как, если a входит в K , а b входит в L , то из a можно попасть в b через вершины из $K \cup L$, поскольку из a можно достичь u через вершины K и из u можно достичь b через вершины L . Аналогично, из b можно попасть в a через вершины $K \cup L$. Из максимальной K и L имеем, что $K \cup L = K$ и $K \cup L = L$, поэтому $K = L$. ∞

Эта теорема дает тот же самый результат, что и лемма об упорядочении квазиупорядоченного множества. Действительно, все вершины сильно связанного подграфа достижимы друг для друга, т. е. находятся в отношении сильной связности, которое является симметричным, рефлексивным и транзитивным. Следовательно, множество вершин сильно связной компоненты образуют один класс эквивалентности. Эти классы эквивалентности связаны между собой и образуют новый граф D^* , вершины которого соответствуют сильным компонентам графа D .

Орграф D^* , называемый *конденсацией* графа D , строится следующим образом. Пусть K_1, K_2, \dots, K_p – сильные компоненты D . Тогда выбираем множество вершин $V(D^*) = \{K_1, K_2, \dots, K_p\}$, и проводим дугу от K_i к K_j тогда и только тогда, когда $i \neq j$ и для некоторых вершин $u \in K_i$ и $v \in K_j$ в D имеется хотя бы одна дуга из u в v .

Конденсация D^* орграфа D не имеет циклов. Действительно, пусть в D^* существует цикл $K_{i_1}, K_{i_2}, \dots, K_{i_k}, K_{i_1}$ и u – некоторая вершина в K_{i_1} , v – некоторая вершина в K_{i_2} . Используя цикл $K_{i_1}, K_{i_2}, \dots, K_{i_k}, K_{i_1}$, легко доказать, что u достижима из v и v достижима из u . Таким образом, оказывается, что u и v входят в одну сильную компоненту и, следовательно, $K_{i_1} = K_{i_2}$ (такой вывод основан на теореме 8.6), а это противоречит определению цикла.

Поскольку новый орграф D^* , являющийся конденсацией исходного орграфа D , не содержит циклов, он будет иметь легко определяемую единственную вершинную базу B^* и из нее будет легко получить все вершинные базы орграфа D . Это свойство конденсации графа основано на следующей теореме.

Теорема 8.14. В орграфе без циклов D есть единственная вершинная база, состоящая из всех вершин, не имеющих входящих дуг.

Доказательство. Пусть B — множество всех вершин, не имеющих входящих дуг. Ясно, что любая вершина u из B должна присутствовать в каждой вершинной базе. Достаточно доказать, что всякая вершина v , не принадлежащая B , достижима из некоторой вершины множества B . Чтобы показать это, предположим, что $v \notin B$. Пусть $v = v_0$. Поскольку $v_0 \notin B$, имеется входящая в v_0 дуга (v_1, v_0) , причем $v_1 \neq v_0$. Если $v_1 \in B$, все доказано. Если нет, то значит есть входящая в v_1 дуга (v_2, v_1) , причем $v_2 \neq v_1$. Продолжая этот процесс, построим путь $v_i, v_{i-1}, \dots, v_1, v_0$, не содержащий вершин из B . Все вершины этого пути различны, поскольку, если $v_i = v_j$, $i > j$ и $v_i, v_{i-1}, \dots, v_{j+1}$ различны, то $v_i, v_{i-1}, \dots, v_{j+1}, v_j$ — цикл, что противоречит допущению об отсутствии циклов в орграфе D . Так как D имеет конечное число вершин, то построение пути $v_i, v_{i-1}, \dots, v_1, v_0$ не может продолжаться бесконечно. В конце концов мы должны достичь некоторую вершину v_i , входящую в B . Таким образом, вершина $v = v_0$ достижима из v_i . \simeq

Следствие. В орграфе без циклов существует вершина, в которую не входит ни одна дуга.

Теорема 8.15. Пусть B^* — единственная вершинная база конденсации D^* орграфа D . Тогда вершинными базами в D служат такие множества B , которые содержат по одной вершине из каждой сильной компоненты D , принадлежащей B^* .

Доказательство. Предположим, что B^* — единственная вершинная база в D^* и B содержит по одной вершине из каждой сильной компоненты B^* . Ясно, что каждая вершина в D достижима из B . Нужно показать, что B является минимальным множеством, обладающим тем свойством, что каждая вершина в D достижима из B . Для доказательства минимальности достаточно показать, что не найдется вершины $v \in B$, достижимой из другой вершины $u \in B$. Если бы это было возможно, то сильная компонента, содержащая v , была бы достижима в D^* из сильной компоненты, содержащей u , что противоречило бы минимальности B^* . Чтобы завершить доказательство, покажем, что если B служит произвольной вершинной базой, то она содержит точно по одной вершине из каждой сильной компоненты D , принадлежащей B^* . Конечно, база B должна содержать по крайней мере по одной вершине из каждой такой сильной компоненты, а также, возможно, и другие вершины. Из условия минимальности следует, что никакие другие вершины не требуются. \simeq

Следствием из теоремы 8.15 является теорема 8.16.

Теорема 8.16. Любые две вершинные базы орграфа содержат одинаковое число вершин.

Из этих теорем следует процедура (Кёнига) нахождения множества вершинных баз орграфа.

1. Находятся все сильные компоненты орграфа D .
 2. Строится конденсация D^* орграфа D .
 3. Находится множество вершин графа конденсации B^* , в которые не входит ни одна дуга (вершинная база B^* конденсации графа D^*).
 4. Из каждой сильной компоненты, входящей в B^* , выбирается по одной вершине. Это множество есть вершинная база B орграфа D .
- Рассмотрим эту процедуру для орграфа, изображенного на рис. 8.21.

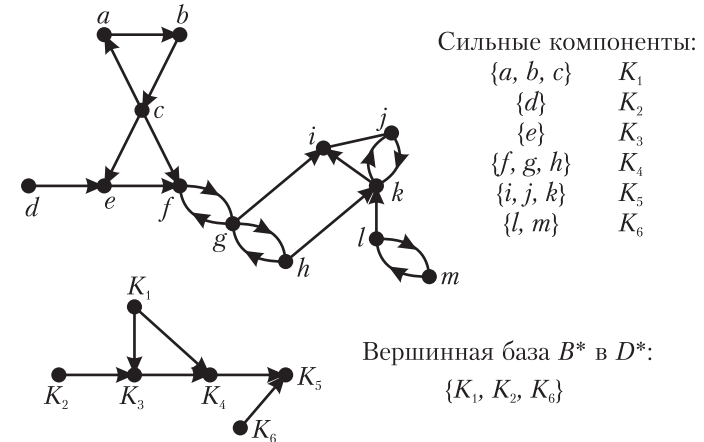


Рис. 8. 21. Орграф, его конденсация и вершинная база.

Найдем все сильные компоненты этого графа. Он содержит шесть сильных компонент (множества входящих в них вершин указаны на рисунке). Строим конденсацию D^* графа D . В качестве вершин D^* выбираем все сильные компоненты $K_1 - K_6$ и соединяем их дугами. В конденсации D^* найдется, например, дуга из K_3 в K_4 , поскольку в орграфе D имеется дуга (e, f) . Аналогично в D^* найдется дуга из K_4 в K_5 , поскольку в D есть дуга из g в i . Имеется и другая дуга (h, k) из вершины в K_4 к вершине в K_5 , однако в конденсацию графа включается только одна из них.

Теперь найдем вершинную базу в D^* . Компоненты K_1, K_2 и K_6 не имеют входящих дуг; они образуют множество $B^* = \{K_1, K_2, K_6\}$, из которого достижима каждая другая вершина в D^* . Таким образом, $B^* = \{K_1, K_2, K_6\}$ является вершинной базой для конденсации D^* .

Далее, если взять по одному элементу из каждой сильной компоненты K_1, K_2, K_6 , то получим вершинную базу для D . Например, множество $\bar{B} = \{a, d, l\}$ дает такую вершинную базу. Другая вершинная база задается множеством $\{a, d, m\}$. Из B^* получаются и другие вершинные базы: $\{b, d, l\}, \{b, d, m\}, \{c, d, l\}, \{c, d, m\}$.

Мы видим, что в D^* всегда есть единственная вершинная база B^* , состоящая, как в этом примере, из всех вершин, не имеющих входящих дуг. В свою очередь, каждую вершинную базу в D можно получить из базы в D^* , выбирая по одной вершине из каждой сильной компоненты в D , входящей в B^* . Таким образом, полученные вершинные базы составляют множество всех вершинных баз.

8.8.2. Использование матрицы достижимости для нахождения сильных компонент орграфа

Теорема 8.17. Пусть орграф D имеет матрицу достижимости $R = (r_{ij})$ и $R^2 = (s_{ij})$. Тогда:

- 1) сильная компонента, содержащая вершину u_i , определяется единичными элементами в i -й строке (или столбце) поэлементного произведения $R \times R'$, где R' — матрица, транспонированная к R ;
- 2) число вершин в сильной компоненте, содержащей u_i , равно s_{ii} .

Доказательство. Вершина u_j достижима из вершины u_i тогда и только тогда, когда $r_{ij} = 1$. В свою очередь, u_i достижима из u_j тогда и только тогда, когда $r_{ji} = 1$. Таким образом, u_i и u_j взаимно достижимы в том и только том случае, если $r_{ij} r_{ji} = 1$.

Величина s_{ii} равна $\sum_{j=1}^n r_{ij} r_{ji}$, где n — число вершин. Далее, $r_{ij} r_{ji} = 1$ тогда и только тогда, когда u_i и u_j взаимно достижимы. Таким образом, суммирование этих чисел по всем j дает число вершин u_j , взаимно достижимых для вершин u_i .

На рис. 8.22 приведены матрицы R , $R \times R'$ и R^2 для изображенного там же орграфа D . Поэлементное произведение $R \times R'$ представляет собой клеточно-диагональную матрицу. Каждая клетка соответствует одной сильной компоненте. Мы можем найти сильные компоненты, просматривая матрицу по строкам. Например, строка, соответствующая вершине u в матрице $R \times R'$, определяет сильную компоненту $\{u, v, w\}$. Элемент (u, u) в матрице R^2 , а именно 3, дает число элементов в этой сильной компоненте. Аналогично можно найти другие сильные компоненты.

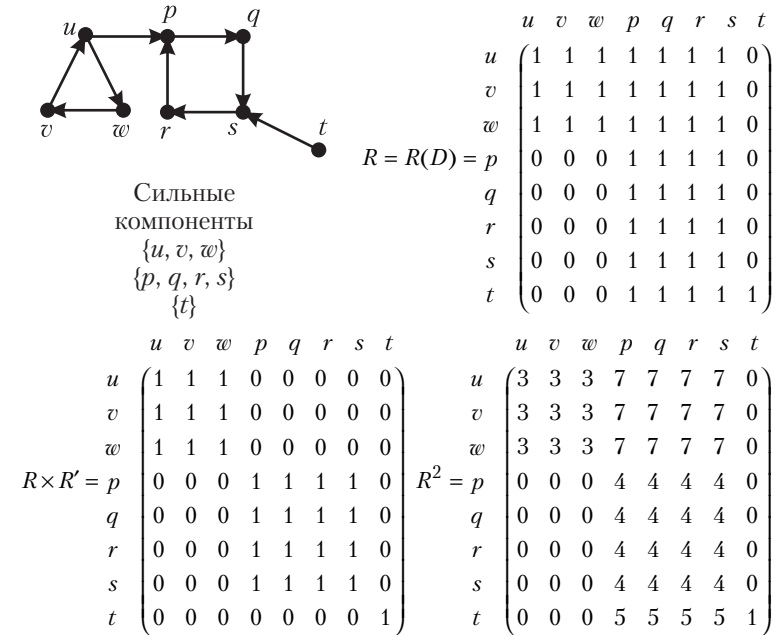


Рис. 8.22. Сильные компоненты орграфа, определяемые по матрице достижимости.

8.9. Ациклические графы

➔ **Определение 8.23.** Орграф называется *ациклическим*, если он не содержит циклов.

В общем случае орграф может содержать пути сколь угодно большой длины, поскольку каждый путь может проходить через одну вершину любое число раз. Однако это возможно, только если в графе есть циклы. В ациклическом графе длины путей ограничены, так как вершины в его путях не могут повторяться, т. е. все его пути — простые цепи. Следовательно, в ациклическом орграфе имеются пути максимальной длины, т. е. пути, которые не могут быть продолжены: нельзя добавить ребро ни к их началу, ни к их концу. Отсюда следует, что в ациклическом графе существует, по крайней мере, одна вершина, в которую не входит ни одна дуга (такую вершину называют *истоком*, или *источником*), и, по крайней мере, одна вершина, из которой не выходит ни одна дуга (такую вершину называют *стоком*).

Действительно, в ациклическом графе любой путь приводит в вершину, из которой он не может продолжиться (см. рис. 8.23). Такая вершина и есть сток. Если же продолжить этот путь от его начала против ориентации, придем в вершину, из которой нельзя выйти против ориентации инцидентных ей ребер, т. е. в вершину, не имеющую входящих ребер. Такая вершина является источником.

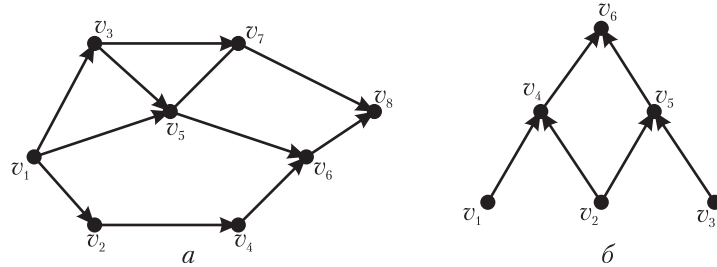


Рис. 8.23. Ациклические графы.

* Примеры.

Ациклический орграф с одним источником и одним стоком называется *двухполосным*. Двухполосный граф изображен на рис. 8.23, а. Ациклический граф на рис. 8.23, б имеет три истока и один сток.

Граф конденсации некоторого орграфа является ациклическим графом, так как он никогда не содержит циклов. Другим примером ациклического графа является представление полурешеток в виде диаграмм Хассе. Диаграмма полной решетки представляет собой двухполосный ациклический орграф.

↪ **Определение 8.24.** *Топологической сортировкой орграфа* называется такая нумерация вершин, что для любой дуги (v_i, v_j) номер ее начала меньше номера ее конца: $i < j$.

Теорема 8.18. Для орграфа топологическая сортировка существует тогда и только тогда, когда он ациклический.

Доказательство. Предположим, что для цикла топологическая сортировка возможна. Выберем в цикле произвольную вершину v_i . Цикл содержит ребра (v_i, v_j) и (v_k, v_i) , причем по определению 8.24 должно быть $i < j$ и $k < i$. При прохождении вдоль цикла номера вершин должны только возрастать и, значит, все они будут больше i . Поэтому, когда мы придем в v_k , получим $k > i$, что противоречит предположению. ∞

Для ациклического орграфа D с n вершинами топологическая сортировка осуществляется с помощью следующего алгоритма. Выберем в D какой-либо сток и присвоим ему номер n . Все инцидентные ему ребра — входящие, поэтому их начала будут иметь номера, меньшие

n , и, следовательно, для них условие определения 8.24 выполнено. Удалим выбранный сток вместе со всеми инцидентными ему дугами. Получим ациклический граф с $n - 1$ вершиной. Выберем в нем какой-либо сток и присвоим ему номер $n - 1$. Будем повторять процедуру удаления стоков и инцидентных им дуг до тех пор, пока не пронумеруем все вершины. Поскольку всякий раз удаляемые дуги будут удовлетворять условию определения 8.24, получим топологическую сортировку исходного орграфа. Пример топологической сортировки графа приведен на рис. 8.23.

8.10. Деревья

Если в ациклическом орграфе «отменить» ориентацию ребер, то в полученном неориентированном графе могут возникнуть циклы. Поэтому неориентированный ациклический граф имеет более специфический вид.

↪ **Определение 8.25.** *Связный неориентированный граф без циклов называется неориентированным деревом*. Несвязный граф, состоящий из нескольких деревьев, называется *лесом*.

Такое дерево является неориентированным ациклическим графом, поэтому в нем все пути — простые.

Понятие *ориентированного* дерева отличается от ациклического графа.

↪ **Определение 8.26.** Не содержащий циклов связный орграф, в котором только одна вершина не имеет входящих дуг, а все остальные вершины имеют по одной входящей дуге, называется *ориентированным*, или *направленным деревом*.

↪ **Определение 8.27.** Вершина, не имеющая входящих дуг, называется *корнем* дерева. Вершины, не имеющие исходящих дуг, называются *концевыми*, или *терминальными*, или *листьями*. Промежуточные вершины, лежащие между корнем и листьями, называются *транзитными*.

Ориентированные деревья часто изображают без стрелок, предварительно оговорив, что это растущее вниз (или вверх) дерево. На рис. 8.24, а изображено растущее вниз дерево, на рис. 8.24, б неориентированное дерево.

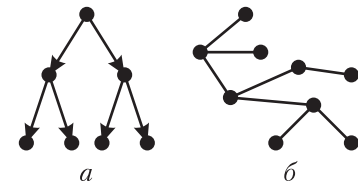


Рис. 8.24. Примеры деревьев.

Следующая теорема описывает основные свойства деревьев.

Теорема 8.19.

1. В любом дереве имеются, по крайней мере, две концевые вершины (вершины степени 1).
2. Между любыми двумя вершинами дерева имеется ровно один путь.
3. Число ребер в дереве с n вершинами равно $n - 1$.

Доказательство. 1). Поскольку в дереве все пути – простые, то в нем есть по крайней мере один максимальный путь, т. е. путь, который нельзя продолжить. Концы этого пути и являются концевыми вершинами. (Заметим, что в произвольном ациклическом орграфе тоже есть максимальные пути; их концами являются стоки. Однако сток может иметь степень, большую единицы. В этом случае продолжить из него путь нельзя не потому, что нет другого инцидентного ему ребра, а потому, что другие ребра – тоже входящие, и выйти по ним из стока нельзя.)

2). Наличие пути между любой парой вершин следует из связности дерева, а единственность этого пути – из того, что существование двух путей между парой вершин всегда создает цикл.

3). Третий пункт теоремы проще всего доказать, введя процедуру преобразования неориентированного дерева в ориентированное. Выберем в дереве произвольную вершину. Назовем ее *корнем*. Ребра, инцидентные корню, ориентируем в направлении от корня. Для каждой вершины v_i , являющейся концом одного из этих ребер, ориентируем остальные инцидентные ей ребра в направлении от v_i . Продолжаем эту процедуру до тех пор, пока не будут достигнуты концевые вершины. В силу единственности пути между вершинами ни одна вершина не будет достигнута дважды (т. е. не придется ориентировать уже ориентированные ребра), а в силу связности дерева все вершины будут достигнуты. Из этой процедуры видно, что корень не имеет входящих ребер (его полустепень захода равна 0), а каждая из остальных $n - 1$ вершин имеет одно входящее ребро. Поскольку все ребра являются входящими для какой-то вершины, то отсюда и следует п. 3 теоремы. \square

Из одного неориентированного дерева с n вершинами можно получить ровно n различных ориентированных деревьев, так как выбор разных корней всегда дает разные ордеревья. Это следует из того, что из корня достижимы все остальные вершины, сам же корень недостижим ни из какой другой вершины. Другими словами, ориентированное дерево всегда односторонне связно. Однако различные ордеревья, полученные из одного и того же дерева, могут оказаться изоморфными.

✱ **Пример.** Если исходное дерево – простая цепь, то выбор в качестве корня концов этой цепи даст две изоморфные ориентированные цепи, а если эта цепь содержит четное число вершин и, следовательно, два центра, то выбор этих центров даст два изоморфных ордеревья с двумя путями, ведущими из корня.

↪ **Определение 8.28.** Дерево, в котором каждая вершина имеет по две исходящих дуги или не имеет вовсе, называется *двоичным*, или *бинарным* деревом.

↪ **Определение 8.29.** Пусть n – количество концевых вершин в двоичном дереве, d – длина пути от корня дерева к концевой вершине и m – целое положительное число, тогда дерево называется *сбалансированным*, если:

- 1) либо $n = 2^m$ и тогда $d = m$,
- 2) либо $2^m < n < 2^{m+1}$, и тогда $d = m$ или $d = m + 1$.

На рис. 8.25, а, б деревья сбалансированные, в – несбалансированное дерево.

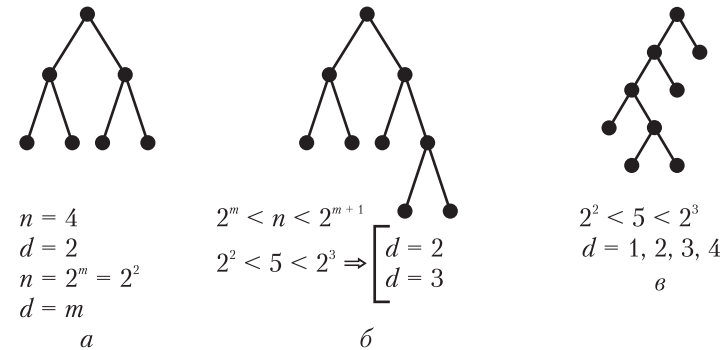


Рис. 8.25. Примеры деревьев.

Деревья отображают иерархические структуры, например, с помощью дерева можно представить иерархию служебных положений в некоторой организации, иерархию понятий некоторой предметной области, родственные отношения (генеалогическое дерево) и т. п.

Бинарные ориентированные деревья имеют большое значение в программировании для представления сложных структур данных и построения алгоритмов их обработки. Удобным способом представления арифметического выражения является польская обратная запись, где операции предшествуют операндам, в отличие от обычно используемой функциональной записи. Например, функция $f(x, y) = x + y$ в обратной записи имеет вид: $+(x, y)$ или просто $+xy$. На рис. 8.26 показано дерево арифметического выражения

$(a + b) \times (a - b)$. Для преобразования его в польскую обратную запись $\times + ab - ab$ используется алгоритм обхода дерева сверху вниз и слева направо, который показан на рис. 8.26.

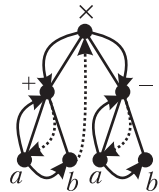


Рис. 8.26.
Обход дерева.

Сначала выбирается значение, хранящееся в корне дерева (оно загружается в стек). Затем происходит спуск по левой ветви до терминальной вершины. Все значения, лежащие на этом пути, записываются после корневого: $\times + a$. Дойдя до терминальной вершины, мы поднимаемся до первой снизу транзитивной вершины, и спускаемся по правому поддереву; получаем $\times + ab$. Последовательно повторяя этот процесс, мы дойдем опять до корня дерева, после чего спускаемся по правому поддереву по тому же алгоритму.

В результате получаем выражение: $\times + ab - ab$.

8.11. Планарные графы

↪ **Определение 8.30.** Граф называется *планарным*, если он может быть нарисован на плоскости так, что его ребра пересекаются только в вершинах графа. Граф называется *плоским*, если он уже уложен на плоскости так, что никакие его два ребра не пересекаются в точках, отличных от вершин графа.

На рис. 8.27, а показан планарный граф, изображенный так, что его ребра пересекаются, а на рис. 8.27, б – тот же граф без пересечений ребер, т. е. плоский граф.

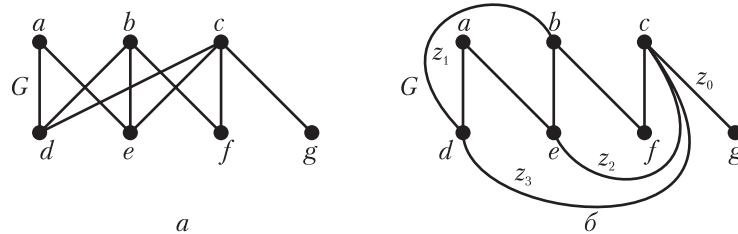


Рис. 8.27. Плоский граф.

Рассмотрим условия, при которых граф является плоским.

↪ **Определение 8.31.** Часть плоского графа, которая ограничена циклом и не включает в себя никакой другой цикл, называется *гранью*. Неограниченная бесконечная область, внешняя по отношению к конечным граням, также считается гранью.

Грани плоского графа образуют разбиение плоскости, на которой он изображен. На рис. 8.27, б в графе G z_0 – бесконечная грань, $z_1, z_2,$

z_3 – конечные. Если граф непланарен, то он не может быть изображен в виде плоского графа, и понятие грани для него теряет смысл.

Теорема 8.20 (Эйлера). Плоское представление связного планарного графа (мультиграфа) с n вершинами, m ребрами и r гранями удовлетворяет следующей формуле:

$$n - m + r = 2.$$

Доказательство. Докажем теорему индукцией по числу граней. Если единственной гранью графа G является внешняя грань, то граф не имеет циклов, следовательно, это дерево, так как G связен. Тогда $m = n - 1$ и $r = 1$, следовательно, $n - m + r = 2$.

Предположим, что G имеет по крайней мере две грани и (x, y) – ребро, лежащее на границе этих граней. При удалении ребра (без удаления вершин x, y) граф остается связным, но число его ребер теперь равно $m - 1$, а число граней $- r - 1$, так как две грани теперь сливаются в одну. Тогда $n - (m - 1) + (r - 1) = n - m + r = 2$. Продолжая этот процесс, по принципу математической индукции, получим, что формула остается справедливой для любого связного планарного графа. ∞

Теорема 8.21. В простом планарном графе с n вершинами, m ребрами и r гранями $3r \leq 2m$.

Доказательство основывается на том факте, что каждая грань имеет по крайней мере три ограничивающих ее ребра, и каждое ребро находится на границе по крайней мере двух граней. ∞

Следующая теорема устанавливает так называемое *неравенство Эйлера*.

Теорема 8.22. В простом планарном графе с n вершинами, m ребрами и r гранями

$$m \leq 3n - 6.$$

Доказательство. Из формулы $n - m + r = 2$ получаем: $r = 2 + m - n$. Подставляя значение r в неравенство $3r \leq 2m$, получим: $6 + 3m - 3n \leq 2m$, т. е. $m \leq 3n - 6$. ∞

Теорема 8.22 дает необходимое условие планарности графа.

На рис. 8.28 изображены два неплоских графа, которые имеют наименьшее число вершин и не являются планарными. Докажем это.

Граф K_5 – это простой полный граф, представляющий собой звезду, вписанную в пятиугольник. Он имеет 5 вершин и 10 ребер, т. е. $3n - 6 = 9$, поэтому неравенство Эйлера $10 \leq 3n - 6$ не выполнено. По теореме 8.22, граф K_5 непланарен.

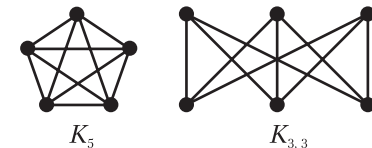


Рис. 8.28. Неплоские графы.

Очевидно, что любой граф, содержащий в качестве подграфа граф K_5 , обязательно будет непланским.

Другой граф, который не содержит графа K_5 и является непланарным, — это полный *двудольный* граф $K_{3,3}$. В *двудольных графах* множество вершин разбито на два непересекающихся подмножества, которые называют *долями*. Такие графы возникают в задачах о соединении n домов и m пунктов обслуживания с помощью коммуникаций (см. рис. 8.29). Например, исследование планарности графа $K_{3,3}$ необходимо в задаче «о трех домах и трех колодцах», в которой жители домов хотели бы ходить за водой к колодцам так, чтобы никогда не встречать никого из своих соседей. Очевидно, для того, чтобы их желание было выполнено, нужно, чтобы их пути никогда не пересекались. Для этого граф, соединяющий «дома» и «колодцы», должен быть плоским. Однако граф $K_{3,3}$ — непланарный, так что желание жителей невыполнимо (см. рис. 8.29).

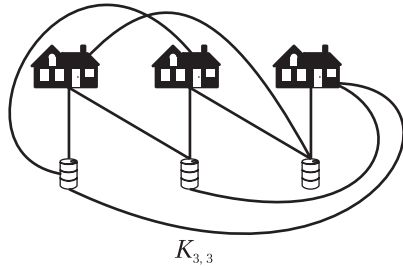


Рис. 8.29. Задача о домах и колодцах.

Для графа $K_{3,3}$ $m = 9$, $n = 6$, т. е. неравенство Эйлера выполняется. Тем не менее, он непланарен. Докажем это.

Предположим, что граф $K_{3,3}$ планарен. Тогда, по теореме Эйлера, число его граней $r = 9 - 6 + 2 = 5$. В силу двудольности $K_{3,3}$, в нем нет циклов длиной меньше 4, поэтому, суммируя длины границ всех граней и учитывая, что в этой сумме каждое ребро графа $K_{3,3}$ встретится дважды, получим: $2m \geq 4r$, т. е. $4r \leq 18$, и, следовательно, $r < 5$, что противоречит теореме Эйлера. Таким образом, $K_{3,3}$ непланарен. Это пример того, что условие $m \leq 3n - 6$ не является достаточным условием планарности.

Графы K_5 и $K_{3,3}$ позволяют определить наиболее общий критерий планарности, который мы приводим здесь без доказательства ввиду его сложности. Предварительно введем новые определения.

↪ **Определение 8.32.** Операция *подразбиения* ребра (u, v) в графе $G = \{V, E\}$ состоит в удалении из E ребра (u, v) , добавлении к V новой вершины w и добавлении к $E \setminus \{(u, v)\}$ двух ребер (u, w) и

(w, v) . Граф H называется *подразбиением графа G* , если H может быть получен из G путем последовательного применения операции подразбиения ребер.

Нетрудно убедиться в том, что операция подразбиения ребра не изменяет соотношения Эйлера. Действительно, в результате подразбиения как количество ребер, так и количество вершин, увеличится на единицу, а количество граней не изменится (см. рис. 8.30), так как при удалении ребра в плоском графе исчезнет одна грань, а при добавлении двух ребер появится новая. Таким образом, $(n + 1) - (m + 1) + (r - 1 + 1) = n - m + r$.

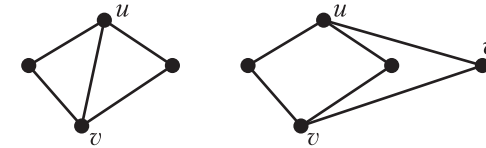


Рис. 8.30. Подразбиение ребра (u, v) .

↪ **Определение 8.33.** Графы G и H *гомеоморфны*, если существуют такие их подразделения, которые изоморфны.

Теорема 8.22 (Понтрягина — Куратовского). Граф планарен тогда и только тогда, когда он не содержит подграфов, гомеоморфных графам K_5 и $K_{3,3}$.

Глава 9.

БУЛЕВА АЛГЕБРА

Джордж Буль (1815—1864) родился в Англии, в Линкольне, в семье мелкого торговца. Его родители испытывали материальные затруднения, поэтому он не смог получить систематического образования, — кроме начальных классов школы для детей бедняков Джордж Буль не учился ни в одном учебном заведении. Однако с детских лет Буль стремился к знаниям, самостоятельно изучая многие предметы, в том числе латынь и греческий, которые изучались в те годы во всех аристократических школах. В 12 лет он уже печатал в местных изданиях свои переводы из Горация, но это не приносило денег, а семья сильно нуждалась. С ранних лет начался трудовой путь Буля, похожий на путь многих героев Диккенса: Буль долго искал работу, дающую какой-то заработок и, в то же время, оставляющую возможности для дальнейшего самообразования. Лишь после долгих мучительных поисков и многих неудачных попыток устроиться Булю удалось открыть маленькую элементарную школу, в которой он преподавал сам. Денег это давало мало, но оставляло некоторый досуг. В процессе занятий с учениками Буль впервые обратился к математике, и школьные учебники привели его в ужас своей нестрогостью и нелогичностью изложения. Стремясь понять, что же на самом деле представляет собой математика, Буль обратился к произведениям классиков и самостоятельно изучил обширные труды Лапласа и Лагранжа. В связи с этими занятиями у него появились первые самостоятельные идеи. К его счастью, Д. Грегори, основавший незадолго до того «Кембриджский математический журнал», сразу же оценил глубину мысли и оригинальность стиля провинциального учителя, приславшего ему свои статьи. Вторым человеком, активно поддержавшим Буля, был кембриджский математик, профессор университета Аугустус де Морган. Де Морган сам интересовался вопросами логического обоснования математики, которые вскоре стали краеугольным камнем всех размышлений Буля. Первые публикации Буля заинтересовали де Морганна, а краткая брошюра «Математический анализ логики, сопровождаемый наброском исчисления дедуктивных рассуждений» (1847), привела его в восторг. (Заметим, что в том же 1847 г., несколькими месяцами позже, вышло в свет сочинение самого де Морганна на ту же тему: «Формальная логика или исчисление выводов, необходимых и возможных», где, в частности, содержались те логические законы, которые сейчас называют «законами де Морганна»; это обстоятельство делало его оценку работы Буля особенно весомой). Усилиями де Морганна, Грегори и других друзей самоучка Буль стал в 1849 году профессором математики католического колледжа в г. Корк (Ирландия); здесь он провел последние 15 лет своей жизни, наконец-то получив возможность не только обеспечить старость родителей, но и спокойно заниматься наукой. Здесь же он женился на Мэри Эверест — дочери профессора греческого языка в том же колледже и родственнице бывшего генерал-

губернатора Индии, именем которого названа высочайшая вершина мира Эверест. Мэри Буль-Эверест много помогала Булю в работе, а после его смерти оставила интересные воспоминания о своем муже и о его научном творчестве. Она стала матерью четырех дочерей Буля, которые все оказались замечательными людьми (у нас наиболее известна Этель Лилиан Буль, в замужестве Войнич, автор романа «Овод»).

В 1854 г. вышло в свет основное произведение Буля «Исследование законов мысли, на которых основаны математические теории логики и вероятностей». В этой, ставшей классической, работе подробно исследуется алгебраическая система, которую сегодня называют «алгеброй высказываний». Глубокое понимание Булем природы математики и смысла абстрактных математических структур, которое проявилось в этой книге, отмечал Б. Рассел: «Чистую математику открыл Буль в сочинении, которое называлось «Законы мысли». Разумеется, фразу Рассела никак не следует понимать буквально: так, не говоря уже о гениальном Готфриде Вильгельме Лейбнице (1646—1716) или о древних греках, на европейском континенте не уступающую Булю глубину понимания абстрактной природы «чистой» математики демонстрировал в те же годы еще один самоучка (еще один школьный учитель, так же, как и Буль, по достоинству оцененный лишь после смерти), — немец Герман Грассман (1809—1877). Однако бесспорно, что данная Дж. Булем в «Законах мысли» характеристика (любого!) математического исчисления как «метода, базирующегося на употреблении символов, законы комбинации которых нам известны» или фраза «действенность анализа зависит не от истолкования символов, а исключительно от законов их комбинации» свидетельствуют об исключительной глубине проникновения в суть математики. Первая серьезная попытка формализованного изложения той логической системы, которая лежит в основе всех математических умозаключений, попытка строгого описания тех «правил игры», которым подчиняется математика, принадлежит именно Джорджу Булю.

9.1. Абстрактная булева алгебра

Определение булевой алгебры дано в главе 6 (см. определение 6.13). Поскольку любую решетку можно рассматривать как алгебру с двумя операциями, булеву решетку, в которой каждый элемент имеет единственное дополнение, можно рассматривать как булеву алгебру с тремя операциями. В данной главе мы рассмотрим в некотором смысле «минимальную» булеву алгебру, которая строится на решетке **2**, состоящей из двух элементов. Эти элементы обозначаются символами 0 и 1, хотя природа их может быть различна, например, «ложь» и «истина» в алгебре высказываний, положение выключателя «разомкнуто»/«замкнуто» — в теории релейно-контактных схем. В абстрактной булевой алгебре природа множества $\{0, 1\}$ не рассматривается. Решеточные операции объединения (\vee),

пересечения (\wedge) и дополнения (\neg) имеют другие наименования и рассматриваются как алгебраические операции. Все свойства булевых решеток, разумеется, выполнены в булевой алгебре и определяются в ней как аксиомы и теоремы. Рассмотрим определение булевой алгебры так, как это принято в общеизвестной литературе.

↪ **Определение 9.1.** Всякую переменную, которая может принимать одно из двух возможных значений, обозначаемых 0 и 1, назовем *булевой переменной*.

↪ **Определение 9.2.** Функция $f(x_1, \dots, x_n)$, принимающая значения на множестве $\{0, 1\}$ вместе со своими переменными, называется *булевой функцией*.

Совокупность значений переменных булевой функции будем называть *набором*. Например, для булевой функции $f(x, y, z)$ совокупность значений $x = 1, y = 0, z = 1$ записывается как набор 101. Булева функция может быть задана с помощью таблицы – перечислением ее значений на всех наборах. Множество наборов принято записывать в лексикографическом порядке, так что каждый набор представляет собой код двоичного числа. Соответствующее ему десятичное число будем называть *номером* набора. Например, номер набора 101 равен 5, номер набора 110 – 6.

Утверждение 9.1. Количество наборов булевой функции $f(x_1, \dots, x_n)$ от n переменных равно 2^n . Количество булевых функций от n переменных равно 2 в степени 2^n .

Доказательство этого утверждения непосредственно следует из основных соотношений кардинальной арифметики. Действительно, множество всех наборов булевой функции от n переменных образовано декартовым произведением $\{0, 1\}^n$, мощность которого равна 2^n . Множество всех булевых функций от n переменных есть множество отображений $\{0, 1\}^n \rightarrow \{0, 1\}$, мощность которого равна 2^{2^n} .

Существует 4 булевых функции от одной переменной и 16 булевых функций от двух переменных. В таблице 9.1 приведены булевы функции от одной переменной:

- f_1 – константа 0,
- f_2 – тождественная функция $f(x) = x$,
- f_3 – отрицание $f(x) = \neg x$,
- f_4 – константа 1.

Таблица 9.1.

x	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

В табл. 9.2 приведены основные функции от двух переменных.

Таблица 9.2.

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$x \equiv y$	$x \oplus y$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

Это функции:

$x \wedge y$ (или $x \& y$) – конъюнкция,

$x \vee y$ – дизъюнкция,

$x \rightarrow y$ (или $x \supset y$) – импликация,

$x \equiv y$ (или $x \sim y$) – эквивалентность (эквиваленция),

$x \oplus y$ – сложение по *mod 2* (операция Жегалкина).

Утверждение 9.2. Множество, состоящее из двух значений 0 и 1, на котором определены унарная операция отрицания \neg согласно табл. 9.1, и бинарные операции дизъюнкции \vee и конъюнкции \wedge согласно табл. 9.2, является булевой алгеброй.

Истинность утверждения 9.2. следует из теории решеток: операция отрицания булевой алгебры определяется как дополнение в решетке **2**, дизъюнкции \vee и конъюнкции \wedge – как объединение и пересечение соответственно.

Операция отрицания при рукописном написании обычно записывается как черта над символом переменной, например: \bar{x} , $\overline{(x \vee y)}$, однако, мы будем использовать символ \neg , например: $\neg x$, $\neg(x \vee y)$. Иногда отрицание обозначается символом \sim , например: $\sim x$. Операция конъюнкции в булевой алгебре обычно обозначается символом \wedge , в алгебре высказываний – символом $\&$. В выражениях булевой алгебры этот символ часто опускается, как символ умножения в арифметических выражениях, например, выражение $x \wedge y$ записывается как xy .

9.2. Основные аксиомы и теоремы булевой алгебры

Аксиомы и теоремы булевой алгебры непосредственно следуют из свойств булевых решеток. Приведем список аксиом и основных теорем булевой алгебры.

↪ **Аксиомы булевой алгебры:**

(9.1) *коммутативные законы:*

$$a \vee b = b \vee a;$$

$$a \wedge b = b \wedge a;$$

(9.2) *дистрибутивные законы:*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c);$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$

(9.3) *свойства 0 и 1:*

$$a \vee 0 = a, a \wedge 1 = a;$$

(9.4) *закон исключенного третьего:*

$$a \vee \neg a = 1;$$

закон противоречия:

$$a \wedge \neg a = 0.$$

↪ **Теоремы:**

(9.5) *ассоциативные законы:*

$$a \vee (b \vee c) = (a \vee b) \vee c;$$

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c;$$

(9.6) *если для всех a $a \vee b = a$, то $b = 0$;*

если для всех a $a \wedge b = a$, то $b = 1$;

(9.7) *если $a \vee b = 1$ и $a \wedge b = 0$, то $b = \neg a$;*

(9.8) $\neg \neg a = a$;

(9.9) $\neg 0 = 1, \neg 1 = 0$;

(9.10) *законы идемпотентности:*

$$a \vee a = a;$$

$$a \wedge a = a;$$

(9.11) $a \vee 1 = 1, a \wedge 0 = 0$;

(9.12) *законы поглощения:*

$$a \vee (a \wedge b) = a;$$

$$a \wedge (a \vee b) = a;$$

(9.13) *законы де Моргана:*

$$\neg(a \vee b) = \neg a \wedge \neg b;$$

$$\neg(a \wedge b) = \neg a \vee \neg b;$$

(9.14) *законы склеивания:*

$$(a \vee b) \wedge (a \vee \neg b) = a;$$

$$(a \wedge b) \vee (a \wedge \neg b) = a.$$

9.3. Булевы формулы

↪ **Определение 9.3.**

- Каждая переменная есть формула.
- Если x, y — формулы, то формулами являются $(\neg x)$, $(x \vee y)$, $(x \wedge y)$.
- Других формул нет.

В изображении формул приняты следующие допущения: внешние скобки опускают; устанавливают приоритеты выполнения операций в следующем порядке:

\neg — отрицание (наивысший приоритет),

\wedge — конъюнкция,

\vee — дизъюнкция,

\rightarrow, \equiv — импликация и эквивалентность (имеют одинаковый приоритет).

С учетом этих приоритетов избыточные скобки также опускаются.

Для каждой булевой формулы можно построить таблицу ее значений, пользуясь определением основных операций. Булевы формулы называются *эквивалентными*, или *равносильными*, если их таблицы совпадают. (Для обозначения равносильности формул мы используем символ \equiv). Такие формулы, которые на одних и тех же наборах принимают одинаковые значения, представляют одну и ту же булеву функцию. Таким образом, одна и та же булева функция может быть представлена различными формулами, а поскольку для каждой булевой формулы можно построить единственную таблицу значений, то каждой булевой формуле соответствует единственная булева функция.

Если две равносильные формулы соединить с помощью операции эквивалентности, то вновь полученная формула будет тождественно равна единице. Аксиомы и теоремы булевой алгебры задают равносильные формулы.

Рассмотрим некоторые равносильные формулы (см. табл. 9.3).

Таблица 9.3.

x	y	$x \rightarrow y$	$\neg x \vee y$	$y \rightarrow x$	$(x \rightarrow y)(y \rightarrow x)$	$x \equiv y$	$x \oplus y$	$\neg(x \oplus y)$
0	0	1	1	1	1	1	0	1
0	1	1	1	0	0	0	1	0
1	0	0	0	1	0	0	1	0
1	1	1	1	1	1	1	0	1

Мы видим, что таблицы значений формул $x \rightarrow y$ и $\neg x \vee y$ совпадают, следовательно, эти формулы эквивалентны:

$$(9.15) x \rightarrow y = \neg x \vee y.$$

Эквивалентны также формулы:

$$(9.16) x \equiv y = \neg(x \oplus y),$$

$$(9.17) x \equiv y = (x \rightarrow y)(y \rightarrow x).$$

В (9.17) мы можем заменить импликацию на равносильную ей формулу (9.15). В результате получим:

$$x \equiv y = (x \rightarrow y)(y \rightarrow x) = (\neg x \vee y)(\neg y \vee x).$$

Эти равносильности объясняют, почему при определении булевой формулы используются только операции \neg , \vee , \wedge , — операции импликации, эквивалентности и сложения по модулю 2 могут быть введены с помощью равносильных формул (9.15) – (9.17).

С помощью равносильных формул можно проводить эквивалентные преобразования булевых формул. Например, преобразуем булеву формулу $\neg x \oplus (z \rightarrow y)$.

$$\begin{aligned} \neg x \oplus (z \rightarrow y) &= z \rightarrow y = \neg z \vee y, \\ &= \neg x \oplus (\neg z \vee y) = x \oplus y = \neg(x \equiv y), \\ &= \neg(\neg x \equiv (\neg z \vee y)) = x \equiv y = (\neg x \vee y)(\neg y \vee x), \\ &= \neg((\neg \neg x \vee (\neg z \vee y))(\neg(\neg z \vee y) \vee \neg x)) = \neg \neg x = x \\ &= \neg((x \vee \neg z \vee y)(\neg(\neg z \vee y) \vee \neg x)) = \text{закон де Моргана} \\ &= \neg((x \vee \neg z \vee y)(z \neg y \vee \neg x)) = \text{закон де Моргана} \\ &= (\neg x z \neg y) \vee ((\neg z \vee y)x) = \text{дистрибутивный} \\ &= \neg x z \neg y \vee \neg z x \vee y x = \text{закон} \\ &= \neg x \neg y z \vee x \neg z \vee x y. \quad \text{ассоциативный закон} \end{aligned}$$

9.4. Дизъюнктивные и конъюнктивные нормальные формы

Поскольку одна и та же булева функция может быть представлена различными формулами, возникает вопрос о единственности представления булевых функций, т.е. нахождения такой универсальной формы, чтобы каждая булева функция могла быть представлена в ней. Такими формами в булевой алгебре являются совершенные дизъюнктивная и конъюнктивная нормальные формы.

↪ **Определение 9.4.** Всякая булева формула, построенная с помощью одной только операции дизъюнкции над булевыми переменными или их отрицаниями, называется *элементарной дизъюнкцией*, или *дизъюнктом*. Например, $x_1 \vee x_2 \vee \neg x_3 \vee x_4$ — элементарная дизъюнкция.

↪ **Определение 9.5.** Всякая булева формула, построенная с помощью одной только операции конъюнкции над переменными или их отрицаниями, называется *элементарной конъюнкцией*, или *конъюнктом*. Например, $x_1 x_2 \neg x_3 \neg x_4$ — элементарная конъюнкция.

Теорема 9.1. Для того чтобы элементарная дизъюнкция тождественно равнялась единице, необходимо и достаточно, чтобы в нее входила некоторая переменная вместе со своим отрицанием.

Теорема 9.2. Для того, чтобы элементарная конъюнкция тождественно равнялась нулю, необходимо и достаточно, чтобы в нее входила некоторая переменная вместе со своим отрицанием.

Справедливость теорем 9.1, 9.2 следует из аксиомы (9.4) и определения операций дизъюнкции и конъюнкции.

↪ **Определение 9.6.** Булева функция называется *конституентой единицы* (или минтермом), если она равна единице только на одном наборе своих аргументов.

↪ **Определение 9.7.** Булева функция называется *конституентой нуля* (или макстермом), если она равна нулю только на одном наборе своих аргументов.

✱ **Пример.** Среди булевых функций двух аргументов конъюнкция и стрелка Пирса ($x \uparrow y = \neg(x \vee y)$) являются конституентами единицы, а дизъюнкция, импликация, штрих Шеффера ($x \mid y = \neg(x \wedge y)$) являются конституентами нуля.

Теорема 9.3. Не тождественно ложная элементарная конъюнкция от n переменных является конституентой единицы от n переменных.

Доказательство. Введем обозначение: $x^0 = \neg x$, $x^1 = x$. Обозначим параметр 0 или 1 через α . Тогда $x^\alpha = 1$, если $x = \alpha$, и $x^\alpha = 0$, если $x \neq \alpha$. Кроме того, $1^\alpha = \alpha$, $0^\alpha = \neg \alpha$.

Рассмотрим элементарную конъюнкцию вида $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, о которой известно, что она не равна нулю тождественно. Из теоремы 9.2 следует, что все входящие в нее переменные различны и им можно придавать независимые значения. Придадим переменной x_1 значение α_1 , $x_2 = \alpha_2$ и т. д. до $x_n = \alpha_n$. Тогда элементарная конъюнкция $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ равна единице по самому выбору значений x_1, x_2, \dots, x_n . Выбор этих значений таков, что если переменная x_i входит в элементарную конъюнкцию с отрицанием, то $\alpha_i = 0$ и переменной x_i тоже придаем значение, равное нулю. Тогда, по определению, значение $x^{\alpha_i} = \neg x = \neg 0 = 1$. Если же переменная x_i входит в элементарную конъюнкцию без отрицания, то $\alpha_i = 1$ и $x^1 = x = 1$. Таким образом, будет найден набор, на котором данная конъюнкция будет равна единице. Единственность такого набора следует из определения операции конъюнкции. ▮

Из теоремы 9.3 следует, что всякую конституенту единицы можно представить в виде элементарной конъюнкции. Для этого необходимо образовать конъюнкцию всех ее аргументов и расставить отрицания над теми переменными, которые равны нулю на наборе, обращающем функцию в единицу.

Аналогичную теорему можно доказать для элементарной дизъюнкции.

Теорема 9.4. Не тождественно истинная элементарная дизъюнкция от n переменных является конституентой нуля от n переменных.

Доказательство предоставляется читателю.

Из этой теоремы следует, что любую конституенту нуля можно представить в виде элементарной дизъюнкции. Для этого необходимо образовать дизъюнкцию всех переменных и расставить отрицания над теми переменными, которые равны единице на наборе, обращающем функцию в нуль.

✱ **Пример.** Пусть функция $f(x, y, z, v)$ равна единице на единственном наборе 0110. Тогда она является конституентой единицы и ее можно записать в виде: $f(x, y, z, v) = \neg xyz\neg v$.

↪ **Определение 9.8.** Дизъюнкция элементарных конъюнкций, не содержащая двух одинаковых конъюнкций, называется *дизъюнктивной нормальной формой (ДНФ)*.

↪ **Определение 9.9.** Дизъюнктивная нормальная форма, все конъюнкции которой есть конституенты единицы, называется *совершенной дизъюнктивной нормальной формой (СДНФ)*.

↪ **Определение 9.10.** Конъюнкция элементарных дизъюнкций, не содержащая двух одинаковых дизъюнкций, называется *конъюнктивной нормальной формой (КНФ)*.

↪ **Определение 9.11.** Конъюнктивная нормальная форма, все дизъюнкции которой есть конституенты нуля, называется *совершенной конъюнктивной нормальной формой (СКНФ)*.

Теорема 9.5. Любую булеву функцию можно представить в виде СДНФ и СКНФ.

Доказательство. Рассмотрим произвольную булеву функцию $f(x_1, x_2, \dots, x_n)$, не являющуюся константой. Пусть $\alpha_1, \alpha_2, \dots, \alpha_k$ — наборы, на которых функция принимает значение, равное единице, а $\beta_1, \beta_2, \dots, \beta_l$ — наборы, на которых функция равна нулю ($l = 2^n - k$). Построим элементарные конъюнкции $K_{\alpha_1}(x_1, \dots, x_n), K_{\alpha_2}(x_1, \dots, x_n), \dots, K_{\alpha_k}(x_1, \dots, x_n)$, каждая из которых содержит все n переменных и не является тождественно ложной. Построим эти элементарные конъюнкции таким образом, чтобы K_{α_1} принимала значение, равное единице, на наборе α_1 , K_{α_2} — на наборе α_2 и т. д. Согласно теореме 9.3, каждая из этих конъюнкций является конституентой единицы и на остальных наборах принимает значение, равное нулю. По своему построению совокупность всех этих конституент единицы описывает все единицы данной функции. Поэтому их дизъюнкция равносильна данной функции: $f(x_1, \dots, x_n) = K_{\alpha_1}(x_1, \dots, x_n) \vee K_{\alpha_2}(x_1, \dots, x_n) \vee \dots \vee K_{\alpha_k}(x_1, \dots, x_n)$. По определению 9.9 полученная

формула является совершенной дизъюнктивной нормальной формой данной функции.

Аналогично можно показать, что формула $A = K_{\beta_1} \wedge K_{\beta_2} \wedge \dots \wedge K_{\beta_l}$ являющаяся конъюнкцией всех конституент нуля, соответствующих наборам, на которых функция равна нулю, равносильна данной функции, и является СКНФ функции. ∞

✱ **Пример.** Пусть булева функция $f(x, y, z)$ задана табл. 9.4. Построим СДНФ и СКНФ данной функции.

Таблица 9.4.

x	0	0	0	0	1	1	1	1
y	0	0	1	1	0	0	1	1
z	0	1	0	1	0	1	0	1
$f(x, y, z)$	1	0	0	1	1	1	0	0

Для построения СДНФ булевой функции необходимо рассмотреть все наборы, на которых функция равна единице, и образовать конституенты единицы, соответствующие этим наборам. Полученные конституенты объединить знаками дизъюнкции. Получим СДНФ: $f(x, y, z) = \neg x\neg y\neg z \vee \neg xyz \vee x\neg y\neg z \vee x\neg yz$. Двойственное правило существует для построения СКНФ. Рассмотрим все наборы, на которых булева функция равна нулю. Образует все конституенты нуля как элементарные дизъюнкции, в которых каждая переменная берется без отрицания, если она равна нулю, и с отрицанием, если она равна единице в данном наборе. Соединив все конституенты нуля символами конъюнкции, получим СКНФ: $f(x, y, z) = (x \vee y \vee \neg z)(x \vee \neg y \vee z)(\neg x \vee \neg y \vee z)(\neg x \vee \neg y \vee \neg z)$.

Другой способ заключается в том, что любую булеву формулу можно привести к виду ДНФ (КНФ) и СДНФ (СКНФ) с помощью эквивалентных преобразований, используя соотношения (9.1) – (9.17).

✱ **Пример.** Приведем к СДНФ формулу $(x \rightarrow y) \rightarrow xz$. В силу того, что $x \rightarrow y = \neg x \vee y$, получим: $(x \rightarrow y) \rightarrow xz = \neg(\neg x \vee y) \vee xz = x\neg y \vee xz$. Полученная формула представлена в ДНФ, и для того, чтобы получить ее представление в СДНФ, «домножим» $x\neg y$ на $z \vee \neg z$, и xz — на $y \vee \neg y$. Тогда $x\neg y(z \vee \neg z) \vee xz(y \vee \neg y) = x\neg yz \vee x\neg y\neg z \vee xyz \vee x\neg yz$. В силу идемпотентности, $x\neg yz \vee x\neg yz = x\neg yz$, поэтому СДНФ есть $x\neg yz \vee x\neg y\neg z \vee xyz$.

9.5. Алгебра Жегалкина

↪ **Определение 9.12.** Система элементов $\{0,1\}$, на которой определены операции \wedge (конъюнкция) и \oplus (сложение по $mod\ 2$), для которых выполняются соотношения

$$(9.18) \quad x \oplus y = y \oplus x,$$

$$(9.19) \quad x(y \oplus z) = xy \oplus xz,$$

$$(9.20) \quad x \oplus x = 0,$$

$$(9.21) \quad x \oplus 0 = x,$$

а также соотношения булевой алгебры (9.3, 9.4, 9.6, 9.7, 9.10, 9.11), относящиеся к конъюнкции и константам, называется *алгеброй Жегалкина*.

Из таблицы истинности операции сложения по $mod\ 2$ следует, что

$$(9.22) \quad \neg x = x \oplus 1.$$

Операцию дизъюнкции можно выразить через \oplus и \wedge так:

$$(9.23) \quad x \vee y = \neg(\neg x \neg y) = (x \oplus 1)(y \oplus 1) \oplus 1 = xy \oplus x \oplus y.$$

↪ **Определение 9.13.** Всякая формула алгебры Жегалкина, имеющая вид суммы (по $mod\ 2$) конъюнкций булевых переменных, называется *полиномом Жегалкина*.

Если в каждый член полинома Жегалкина каждая переменная входит один раз и полином не содержит одинаковых членов, то такой полином Жегалкина называется *каноническим*.

Теорема 9.6. Всякая булева функция единственным образом представима в виде канонического полинома Жегалкина.

Доказательство. Всякую булеву формулу можно представить в виде полинома Жегалкина, используя соотношения (9.22), (9.23). Из (9.23) следует, что если две функции f_1 и f_2 таковы, что $f_1 \wedge f_2 = 0$, то $f_1 \vee f_2 = f_1 \oplus f_2$. Отсюда следует правило для представления булевой функции в виде полинома Жегалкина: для булевой формулы, заданной в виде СДНФ, достаточно заменить знак \vee на знак \oplus , представить отрицания переменных как $\neg x = x \oplus 1$, раскрыть скобки по закону дистрибутивности (9.19) и привести подобные члены согласно (9.20, 9.21). ▀

✱ **Пример.** Приведем к каноническому полиному Жегалкина булеву функцию из предыдущего примера: $f(x, y, z) = x\neg yz \vee x\neg y\neg z \vee xyz$. Поскольку функция находится в СДНФ, заменим символы \vee на \oplus , получим: $f(x, y, z) = x\neg yz \oplus x\neg y\neg z \oplus xyz = x(y \oplus 1)z \oplus x(y \oplus 1)(z \oplus 1) \oplus xyz = xyz \oplus xz \oplus xy \oplus x \oplus xyz = xyz \oplus xy \oplus x$.

9.6. Свойства булевых функций

↪ **Определение 9.14.** Функция, которая выражима полиномом Жегалкина вида $\sum \alpha_i x_i \oplus \gamma$, где α_i, γ есть 0 или 1, называется *линейной*.

Все функции одной переменной линейны. Линейными функциями двух переменных являются $x \oplus y$ и $x \equiv y$: $x \equiv y = \neg x \neg y \vee xy = (x \oplus 1)(y \oplus 1) \oplus xy = xy \oplus x \oplus y \oplus 1 \oplus xy = x \oplus y \oplus 1$.

↪ **Определение 9.15.** Пусть дана некоторая булева формула A . Формула A^* называется *двойственной* формуле A , если она получается из A путем замены операций конъюнкции на дизъюнкцию, дизъюнкции на конъюнкцию, 1 на 0, 0 на 1 всюду, где они входят.

Например: $A = xy \vee \neg x \neg y$; $A^* = (x \vee y)(\neg x \vee \neg y)$.

Теорема 9.7. Если $A(x_1, \dots, x_n)$ и $A^*(x_1, \dots, x_n)$ - две взаимно двойственные формулы, то $\neg A(x_1, \dots, x_n) = A^*(\neg x_1, \dots, \neg x_n)$.

Доказательство следует из законов де Моргана.

↪ **Определение 9.16.** Функция называется *самодвойственной*, если она двойственна самой себе, т.е. $A(x_1, x_2, \dots, x_n) = \neg A(\neg x_1, \neg x_2, \dots, \neg x_n)$, или $\neg A(x_1, x_2, \dots, x_n) = A(\neg x_1, \neg x_2, \dots, \neg x_n)$.

Для самодвойственных функций отрицание ее аргументов приводит к отрицанию самой функции, следовательно, самодвойственная функция на противоположных наборах принимает противоположные значения. Например, функция $xy \vee xz \vee yz$ самодвойственна. Чтобы показать это, возьмем отрицания от каждой переменной и от всей функции:

$$\begin{aligned} \neg(\neg x \neg y \vee \neg x \neg z \vee \neg y \neg z) &= (x \vee y)(x \vee z)(y \vee z) = \\ &= (x \vee xy \vee xz \vee yz)(y \vee z) = \\ &= xy \vee xy \vee xyz \vee yz \vee xz \vee xyz \vee xz \vee yz = \\ &= xy \vee xz \vee yz. \end{aligned}$$

Множество наборов булевой функции от n переменных частично упорядочено и образует булеву решетку 2^n . Булеву функцию можно задать на этой решетке, как показано на рис. 9.1, причем среди булевых функций можно выделить такие, которые не убывают с возрастанием значений наборов на булевой решетке. Такие функции называются *монотонными*. Например, на рис. 9.1. показана монотонная функция.

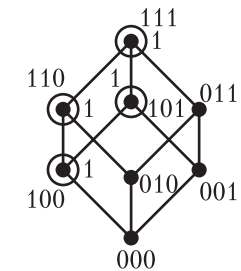


Рис. 9.1.
Монотонная функция.

Обычно отношение порядка на наборах булевых переменных определяется так. Рассмотрим два набора: $A = (\alpha_1, \dots, \alpha_r, \dots, \alpha_n)$ и $B = (\beta_1, \dots, \beta_r, \dots, \beta_n)$. Если для всех i ($i = 1, \dots, n$) $\alpha_i \leq \beta_i$ и существует хотя бы одно такое j , при котором $\alpha_j < \beta_j$, то набор A *предшествует* (меньше) набору B . Это обозначается: $A \leq B$. Если для некоторых i $\alpha_i \leq \beta_i$ и существует такое j , что $\alpha_j > \beta_j$, то наборы A и B *несравнимы*. Например: наборы (0101) и (0010) несравнимы, а набор (0101) предшествует набору (0111).

↪ **Определение 9.17.** Булева функция f называется *монотонной*, если для любых двух наборов A и B из ее области определения, таких, что $A \leq B$, $f(A) \leq f(B)$. Если хотя бы для одной пары наборов, таких, что $A \leq B$, $f(A) > f(B)$, то функция немонотонна.

Среди булевых функций одной и двух переменных конъюнкция, дизъюнкция, константы 0 и 1 монотонны, а функции отрицания, импликации, эквивалентности, штрих Шеффера, стрелка Пирса — немонотонны. Например, импликация на наборе (00) равна 1, а на наборе (10) — 0, а поскольку $(00) \leq (10)$, то получаем, что $f(0,0) > f(1,0)$, т.е. свойство монотонности не выполнено.

↪ **Определение 9.18.** Булева функция называется функцией, *сохраняющей ноль*, если на нулевом наборе она равна нулю, т.е. $f(0, \dots, 0) = 0$.

Нетрудно убедиться, что функции 0, x , $x \wedge y$, $x \vee y$, $x \oplus y$ сохраняют 0, а функции 1, $\neg x$, $x \equiv y$ не сохраняют 0.

↪ **Определение 9.19.** Булева функция называется функцией, *сохраняющей единицу*, если на единичном наборе она равна единице, т.е. $f(1, \dots, 1) = 1$.

Например, функции 1, x , $x \wedge y$, $x \vee y$ сохраняют 1, а 0, $\neg x$, $x \oplus y$ — нет.

9.7. Функционально замкнутые классы булевых функций

↪ **Определение 9.20.** Класс функций называется *функционально замкнутым*, если суперпозиция этих функций принадлежит данному классу.

Теорема 9.8. Суперпозиция линейных функций есть функция линейная.

Доказательство. Если в линейный полином Жегалкина на место какой-либо переменной подставить линейную функцию, то вновь полученный полином будет также линейным. Возьмем полином: $\alpha_1 x_1 \oplus \dots \oplus \alpha_r x_r \oplus \dots \oplus \alpha_n x_n \oplus \gamma$. Подставим вместо x_1 линейный полином $\sum \beta_i y_i \oplus \xi$. Получим линейный полином: $\alpha_1 \beta_1 y_1 \oplus \dots \oplus \alpha_1 \beta_r y_r \oplus$

$\oplus \dots \oplus \alpha_1 \beta_m y_m \oplus \alpha_1 \xi \oplus \dots \oplus \alpha_n x_n \oplus \gamma$. Следовательно, класс линейных функций функционально замкнут. \approx

Теорема 9.9. Суперпозиция монотонных функций есть функция монотонная. Следовательно, класс монотонных функций является функционально замкнутым.

Доказательство. Пусть функции $f(x_1, \dots, x_n)$, $g_1(y_1, \dots, y_k)$, \dots , $g_n(y_1, \dots, y_k)$ монотонны. Составим суперпозицию функций $\Phi = f(g_1, \dots, g_n)$. Пусть α и β — два набора значений переменных y_1, \dots, y_k , причем $\alpha \leq \beta$. В силу монотонности функций g_1, \dots, g_n

$$g_1(\alpha) \leq g_1(\beta), \dots, g_n(\alpha) \leq g_n(\beta),$$

поэтому наборы значений функций упорядочены:

$$(g_1(\alpha), \dots, g_n(\alpha)) \leq (g_1(\beta), \dots, g_n(\beta)),$$

а в силу монотонности функции f

$$f(g_1(\alpha), \dots, g_n(\alpha)) \leq f(g_1(\beta), \dots, g_n(\beta)).$$

Отсюда получаем $\Phi(\alpha) \leq \Phi(\beta)$. \approx

Теорема 9.10. Класс функций, сохраняющих ноль, является функционально замкнутым.

Доказательство. Пусть функции $f(x_1, \dots, x_n)$, $g_1(y_1, \dots, y_k)$, \dots , $g_n(y_1, \dots, y_k)$ сохраняют ноль. Составим суперпозицию функций $\Phi = f(g_1, \dots, g_n)$. Тогда

$$\Phi(0, \dots, 0) = f(g_1(0, \dots, 0), \dots, g_n(0, \dots, 0)) = f(0, \dots, 0) = 0. \approx$$

Теорема 9.11. Класс функций, сохраняющих единицу, является функционально замкнутым.

Доказывается двойственно теореме 9.10.

Теорема 9.12. Класс самодвойственных функций является функционально замкнутым.

Доказательство. Пусть функции $f(x_1, \dots, x_n)$, $g_1(y_1, \dots, y_k)$, \dots , $g_n(y_1, \dots, y_k)$ самодвойственны. Составим суперпозицию функций $\Phi = f(g_1, \dots, g_n)$. Тогда

$$\Phi^* = f^*(g_1^*, \dots, g_n^*) = f(g_1, \dots, g_n) = \Phi. \approx$$

9.8. Функциональная полнота систем булевых функций

↪ **Определение 9.21.** Система булевых функций называется *функционально полной*, если любая булева функция может быть представлена как суперпозиция функций из этой системы.

Обозначим: T_0 — класс функций, сохраняющих 0; T_1 — класс функций, сохраняющих 1; S — класс самодвойственных функций; M — класс монотонных функций; L — класс линейных функций.

Теорема 9.13 (Поста). Для того, чтобы система функций была полна, необходимо и достаточно, чтобы она содержала хотя бы одну немонотонную, хотя бы одну нелинейную, хотя бы одну несамодвойственную, хотя бы одну, не сохраняющую нуль, и хотя бы одну, не сохраняющую единицу, функцию.

Доказательство. Необходимость условий теоремы следует из функциональной замкнутости и неполноты классов монотонных, линейных, сохраняющих 0, сохраняющих 1 и самодвойственных функций. Доказано (теоремы 9.9 – 9.12), что функция, не принадлежащая данному функционально замкнутому классу, не может быть построена путем суперпозиции функций этого класса.

Для доказательства *достаточности* покажем, что с помощью функций, не принадлежащих некоторым из классов T_0, T_1, S, M, L , можно построить некоторую полную систему функций. Такой (полной) системой является, например, отрицание и конъюнкция. Действительно, любая булева функция представима в виде СДНФ, т.е. как суперпозиция \neg, \wedge, \vee . Следовательно, система $\{\neg, \wedge, \vee\}$ функционально полна. Можно исключить из нее \vee , так она представима как суперпозиция \neg и \wedge : $x \vee y = \neg(\neg x \wedge \neg y)$.

Сначала построим константы. Если функция $f(x_1, \dots, x_n)$ несамодвойственна, то подстановкой в нее x и $\neg x$ можно получить константу. Действительно, ввиду несамодвойственности $f(x_1, \dots, x_n)$ существует такой набор $(\alpha_1, \dots, \alpha_n)$, что $f(\alpha_1, \dots, \alpha_n) = f(\neg \alpha_1, \dots, \neg \alpha_n)$. Тогда функция $\varphi(x) = f(x^{\alpha_1}, \dots, x_n^{\alpha_n})$ является константой, так как $\varphi(0) = f(0^{\alpha_1}, \dots, 0^{\alpha_n}) = f(\neg \alpha_1, \dots, \neg \alpha_n) = f(\alpha_1, \dots, \alpha_n) = f(1^{\alpha_1}, \dots, 1^{\alpha_n}) = \varphi(1)$.

Константу 1 можно построить с помощью функции, не сохраняющей 0 и сохраняющей 1, т.е. несамодвойственной. Действительно, пусть f не сохраняет 0. Тогда $\varphi(0) = f(0, \dots, 0) = 1$, а если при этом f сохраняет 1, то $\varphi(1) = f(1, \dots, 1) = 1$, т.е. константа 1 построена.

Двойственно, пусть f_1 не сохраняет 1. Тогда $\psi(x) = f_1(\varphi(x), \dots, \varphi(x)) = f_1(1, \dots, 1) = 0$, т.е. $\psi(x)$ есть константа 0.

Если же $f(1, \dots, 1) = 0$, то $\varphi(x) = \neg x$, так как $\varphi(0) = 1$ по определению f , а $\varphi(1) = 0$. Тогда, если взять несамодвойственную функцию f_2 , то, подставляя в нее x и $\neg x$, также можно получить константу, а с помощью еще одного отрицания, получить другую константу. Таким образом, с помощью функций, не сохраняющих 0, не сохраняющих 1 и несамодвойственных, можно построить константы 0, 1.

С помощью немонотонной функции подстановкой в нее констант можно получить отрицание. Действительно, пусть f немонотонна. Тогда существуют наборы α и β , такие, что $\alpha \leq \beta$, $f(\alpha) = 1$, $f(\beta) = 0$. Поскольку $\alpha \leq \beta$, то в α есть несколько, например, k элементов, которые равны 0, в то время как в β эти же элементы равны 1. Возьмем набор α и заменим в нем первый такой нулевой

элемент на 1, получим набор $\alpha \leq \alpha^1$, который отличается от α только одним элементом (такие наборы называют соседними). Повторяя эту операцию k раз, получим последовательность наборов $\alpha \leq \alpha^1 \leq \dots \leq \alpha^{k-1} \leq \beta$, в которой любые два соседних набора отличаются друг от друга только одним элементом. В этой цепочке найдутся два таких набора α^i, α^{i+1} , что $f(\alpha^i) = 1, f(\alpha^{i+1}) = 0$. Пусть эти наборы отличаются i -м элементом (значением переменной x_i), остальные элементы одинаковы. Подставим в f эти значения. Тогда получим функцию $f(\alpha_1^i, \dots, x_i, \alpha_{i+1}^i, \dots, \alpha_n^i) = g(x_i)$, которая зависит только от x_i . Тогда $g(0) = g(\alpha_1^i) = f(\alpha^i) = 1, g(1) = g(\alpha^{i+1}) = f(\alpha^{i+1}) = 0$. Отсюда следует, что $g(x_i) = \neg x_i$.

С помощью подстановки в нелинейную функцию констант и использования отрицания можно построить конъюнкцию и дизъюнкцию. Действительно, если функция f нелинейная, то ее полином Жегалкина содержит конъюнкцию переменных, например, $K = x_1 x_2 \dots x_k$. Положим $x_3 = \dots = x_k = 1$, а для всех x_i , не содержащихся в K , $x_i = 0$. Тогда конъюнкция $\bar{K} = x_1 x_2$, остальные конъюнкции обратятся в 0, а полином Жегалкина примет вид $\varphi(x_1, x_2) = x_1 x_2 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \gamma$, где $\alpha_1, \alpha_2, \gamma$ – коэффициенты, равные 0 или 1. При подстановке различных констант вместо $\alpha_1, \alpha_2, \gamma$ будут получены разные функции. Рассмотрим функцию $\psi(x_1, x_2)$, получаемую из $\varphi(x_1, x_2)$ следующим образом:

$$\begin{aligned} \psi(x_1, x_2) &= \varphi(x_1 \oplus \alpha_2, x_2 \oplus \alpha_1) \oplus \alpha_1 \alpha_2 \oplus \gamma = \\ &= (x_1 \oplus \alpha_2)(x_2 \oplus \alpha_1) \oplus \alpha_1(x_1 \oplus \alpha_2) \oplus \alpha_2(x_2 \oplus \alpha_1) \oplus \gamma \oplus \alpha_1 \alpha_2 \oplus \gamma = x_1 x_2. \end{aligned}$$

Таким образом, конъюнкция получена.

Для получения дизъюнкции по законам де Моргана потребуется только отрицание. \bowtie

★ **Пример.** Системы функций $\{\vee, \wedge, \neg\}, \{\oplus, \wedge, 0, 1\}, \{\rightarrow, \neg\}$ являются функционально полными. Для примера проверим полноту системы функций $\{\neg, \rightarrow\}$. Для исследуемой системы составим таблицу Поста (см. табл. 9.5). Если функция входит в функционально замкнутый класс, то в таблице Поста в соответствующей ячейке ставится знак «+», иначе – знак «-».

Функция $\neg x$ не сохраняет 0 и 1, так как на нулевом наборе она принимает значение 1, а на единичном – 0. Очевидно, что данная функция немонотонна. Функция самодвойственна, так как на противоположных наборах она принимает противоположные значения. Функция линейна – ее полином Жегалкина: $\neg x = x \oplus 1$. Функция $x \rightarrow y$ не сохраняет 0 и сохраняет 1. Эта функция немонотонна, так как набор (0, 0) предшествует набору (1, 0), но $0 \rightarrow 0 = 1$, а $1 \rightarrow 0 = 0$. На противоположных наборах (0, 0) и (1, 1) функция принимает одинаковые значения 1, следовательно, она несамодвойственна.

Для проверки линейности $x \rightarrow y$ построим канонический полином Жегалкина:

$$x \rightarrow y = \neg x \neg y \vee \neg xy \vee xy = (x \oplus 1)(y \oplus 1) \oplus (x \oplus 1)y \oplus xy = xy \oplus x \oplus 1. \text{ Функция нелинейна, так как содержит элемент } xy.$$

Таблица 9.5

	T_0	T_1	S	M	L
\neg	—	—	+	—	+
\rightarrow	—	+	—	—	—

Система функций $\{\neg, \rightarrow\}$ полна, так как в каждом столбце таблицы Поста имеется хотя бы один знак «—».

9.9. Минимизация булевых функций

↪ **Определение 9.22.** Импликантой булевой функции $f(x_1, \dots, x_n)$ называется такая булева функция $g(x_1, \dots, x_n)$, которая равна единице на некоторых из тех наборов, на которых равна единице данная функция, и равна нулю на остальных наборах (Из определения следует, что функция g — импликанта f , если $g \rightarrow f \equiv 1$.) Говорят, что импликанта g покрывает своими единицами некоторые единицы данной функции f .

Если функция задана в виде ДНФ, т.е. в виде дизъюнкции элементарных конъюнкций, то каждый конъюнкт является импликантой данной функции. Длина некоторых элементарных конъюнкций может быть уменьшена с помощью эквивалентных преобразований. Для этого применяются следующие соотношения:

(9.24) закон неполного склеивания:

$$xy \vee \neg xy = y;$$

$$(x \vee y)(\neg x \vee y) = y;$$

(9.25) закон полного склеивания:

$$xy \vee \neg xz = xy \vee \neg xz \vee yz;$$

$$(x \vee y)(\neg x \vee z) = (x \vee y)(\neg x \vee z)(y \vee z);$$

(9.26) законы поглощения:

$$x \vee xy = x;$$

$$x(x \vee y) = x;$$

(9.27) $x \vee \neg xy = x \vee y;$

$$x(\neg x \vee y) = xy.$$

↪ **Определение 9.23.** Элементарная конъюнкция, которая является импликантой функции f , но никакая ее собственная часть импликантой этой функции не является, называется *простой импликантой* данной функции.

Длина простой импликанты уже не может быть уменьшена путем склеивания ее с другими импликантами данной функции.

↪ **Определение 9.24.** Дизъюнкция всех простых импликант булевой функции называется *сокращенной дизъюнктивной нормальной формой* булевой функции.

* **Пример.** Сократим формулу: $F(x, y, z) = xyz \vee x\neg yz \vee xy\neg z \vee \neg xy\neg z$. Склеим конститутенты: $xyz \vee x\neg yz = xz$, $xy\neg z \vee \neg xy\neg z = y\neg z$, $xyz \vee xy\neg z = xy$. Получим сокращенную форму: $F(x, y, z) = xz \vee y\neg z \vee xy$.

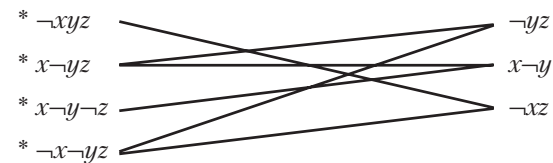
Множество всех простых импликант покрывает все единицы булевой функции. Однако представление булевой функции в виде сокращенной ДНФ еще не является самым экономичным. Среди множества простых импликант могут оказаться лишние, т.е. такие, которые покрывают единицы функции, уже покрытые другими импликантами. Удаляя ненужные импликанты, можно получить *тупиковую* дизъюнктивную нормальную форму. Тупиковая ДНФ, содержащая наименьшее количество импликант и переменных, называется *минимальной* ДНФ.

9.9.1. Метод Квайна получения сокращенной дизъюнктивной нормальной формы

Теорема 9.14 (Квайна). Если в совершенной дизъюнктивной нормальной форме булевой функции произвести все операции неполного склеивания (9.24), а затем все операции поглощения (9.25, 9.26), то в результате будет получена сокращенная ДНФ данной функции.

Для преобразования произвольной ДНФ к виду СДНФ необходимо применить к элементарным конъюнкциям, содержащим не все переменные, операцию развертывания, например: $xy(z \vee \neg z) = xyz \vee xy\neg z$, где z — недостающая переменная.

* **Пример.** Булева функция задана в виде: $f(x, y, z) = \neg xyz \vee x\neg y\neg z \vee \neg yz$. Приведем формулу к СДНФ: $f(x, y, z) = \neg xyz \vee x\neg y\neg z \vee \neg yz(x \vee \neg x) = \neg xyz \vee x\neg y\neg z \vee x\neg yz \vee \neg x\neg yz$. Выпишем все конститутенты единицы и произведем все операции неполного склеивания:



Отмечаем все склеивающиеся конъюнкции символом «*». Они поглощаются импликантами, полученными в результате склеивания. Неотмеченные конъюнкции ничем не поглощаются и являются простыми импликантами. Сокращенная ДНФ данной функции: $f(x, y, z) = \neg yz \vee x\neg y \vee \neg xz$. Для нахождения минимальной ДНФ составим импликантную матрицу (табл. 9.6), в которой по строкам записываем импликанты, по столбцам – конституенты единицы.

Таблица 9.6

	$\neg xyz$	$x\neg y$	$x\neg yz$	$\neg x\neg yz$
$\neg yz$			×	×
$x\neg y$ *		×	×	
$\neg xz$ *	×			×
	*	*	+	+

В клетках таблицы крестиками отмечаем импликанты, покрывающие единицы данной функции. Внизу таблицы символом «*» отмечаем те столбцы, в которых стоит только один крестик, соответствующие им импликанты также отмечаем символом «*» – они являются обязательными. Отмечаем также символом «+» те столбцы, которые покрываются обязательными импликантами. Если все столбцы отмечены, то полученный набор обязательных импликант составляет минимальную ДНФ. Если часть столбцов остается непокрытой, из оставшихся импликант выбирается наименьшее число наиболее коротких импликант так, чтобы все столбцы были покрыты. В нашем примере минимальная ДНФ: $f(x, y, z) = x\neg y \vee \neg xz$.

9.9.2. Минимизация булевых функций с помощью диаграмм Вейча

Булевы функции могут быть представлены графически с виде диаграмм Вейча или карт Карно (они различаются только обозначениями клеток таблицы). Рассмотрим диаграммы Вейча для функций от трех и четырех переменных (см. рис. 9.2).

Каждая клетка диаграммы соответствует одному набору переменных, номер клетки – это двоичный код набора. При задании булевой функции в соответствующую номеру набора клетку записывается единица, и, таким образом, каждая клетка диаграммы с 1 представляет собой одну конституенту единицы.

Пример. Пусть функция $f(x, y, z, t) = 1$ на наборах 0, 1, 2, 3, 6, 7, 8, 15. Диаграмма Вейча для заданной функции представлена на рис. 9.3. Единицы функции, стоящие в соседних клетках, отличаются значением только одной переменной, следовательно, они склеиваются по этой переменной и образуют импликанту. В этом случае говорят, что импликанта *покрывает* соответствующие единицы бу-

левой функции. Например, две единицы на наборах 7 и 15, покрываются импликантой yzt , четыре единицы на наборах 2, 3, 7, 6 – импликантой $\neg xz$. При этом соседними считаются также клетки, стоящие вдоль левого и правого края диаграммы (отличаются значением y) и вдоль верхнего и нижнего края (отличаются значением x).

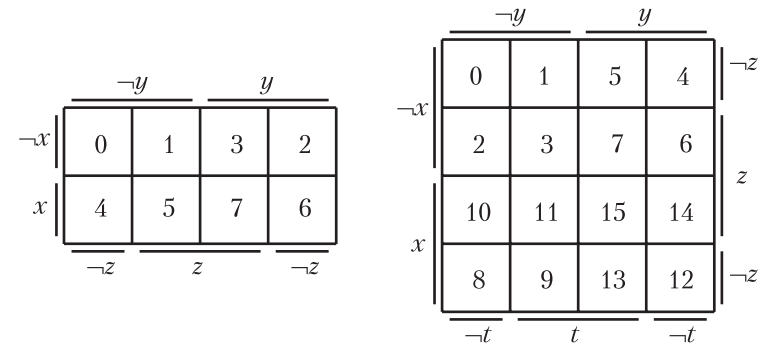


Рис. 9.2. Диаграммы Вейча

При минимизации булевой функции на диаграмме Вейча сначала находят покрытия, содержащие максимальное число единиц (8, 4, 2), а затем покрытия, накрывающие оставшиеся единицы таким образом, чтобы они также были максимальны по величине и при удалении этого покрытия хотя бы одна единица функции осталась непокрытой. При этом некоторые единицы могут быть покрыты неоднократно. Для функции, представленной на рис. 9.3, минимальная ДНФ: $\neg x\neg y \vee \neg xz \vee yzt \vee \neg y\neg z\neg t$.

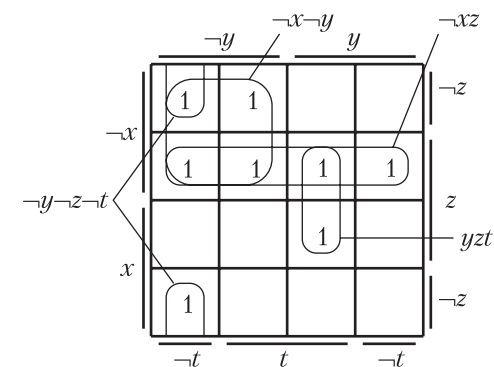


Рис. 9.3. Минимальная ДНФ

Минимальная КНФ строится двойственно по диаграмме Вейча, заполненной нулями в пустых клетках. Для данной функции минимальная КНФ: $(\neg y \vee z)(\neg x \vee \neg z \vee t)(\neg x \vee y \vee \neg t)$.

Глава 10. ЛОГИКА ВЫСКАЗЫВАНИЙ

10.1. Методологические принципы формальной логики

Логика – наука о правильных рассуждениях, о приемах и методах познания с помощью рассуждений. Слово «логика» происходит от древнегреческого «логос»: «понятие», «разум», «рассуждение». Логика как наука о правильных рассуждениях была заложена в древней Греции Аристотелем и на протяжении многих веков развивалась как часть философии. Только в конце 19-го – начале 20-го века с появлением булевой алгебры началось бурное развитие математической (формальной) логики. В настоящее время различают традиционную логику и формальную, математическую логику, соотношение которых показано на рис. 10.1.

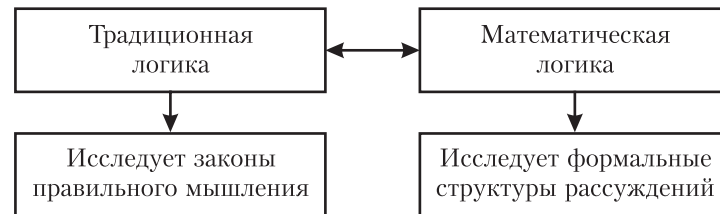


Рис.10. 1. Структура логики

Логика, изучая правильные рассуждения, оперирует понятиями истинности и ложности. Правильное рассуждение или высказывание полагается истинным, неправильное – ложным. Методологические основы формальной логики заключаются в выполнении нескольких принципов.

Принцип тождества. Истинность фактов, лежащих в основе высказываний и рассуждений, устанавливается на основании действительности, известных законов, наблюдений. Если истинность какого-либо факта установлена, то она не подвергается сомнению и не изменяется в процессе рассуждения. Это означает также, что один и тот же термин используется всегда в одном и том же смысле.

Принцип непротиворечивости означает, что, утверждая что-либо, нельзя отрицать то же самое. Один и тот же факт (высказывание) не может быть одновременно истинным и ложным.

Например, высказывание Сократа «Я знаю, что я ничего не знаю» противоречиво, так как одновременно утверждает и опровергает один и тот же факт: если Сократ знает, что он ничего не знает, то он не знает также и этого. Согласно принципу непротиворечивости, из рассмотрения исключаются такие высказывания, истинность или

ложность которых не может быть установлена, например, высказывание о браздобрее, который должен (или не должен) брить самого себя, высказывание критянина о том, что все критяне – лжецы, и другие семантические парадоксы.

Принцип исключенного третьего. Нельзя одновременно отвергать высказывание и его отрицание. Любое высказывание может быть либо истинным, либо ложным, – третьего не дано.

Принцип достаточного основания. Всякое высказывание должно быть обосновано, т.е. истинность утверждения нельзя принимать на веру. Если утверждение выводится из каких-либо суждений, данных, фактов – *оснований*, то их должно быть достаточно для установления истинности утверждения.

10.2. Основные понятия логики высказываний

Суждение, или высказывание – это мысль, в которой утверждается наличие или отсутствие каких-либо фактов или связей между фактами. Высказывания выражаются повествовательными предложениями.

➔ **Определение 10.1.** *Простое высказывание* – это простое повествовательное предложение, относительно которого можно однозначно сказать, истинно оно или ложно.

Вопросительные и восклицательные предложения высказываниями не являются.

Логические значения *Истинно (True)* и *Ложно (False)* будем обозначать соответственно *T* и *F*.

* Примеры.

«Киев – столица Украины» – истинное высказывание, оно имеет значение *True* («истинно»). « $5 > 10$ » – ложное высказывание, оно имеет значение *False* («ложно»). «Все люди смертны» – истинное высказывание. «Некоторые люди – юристы» – истинное высказывание.

Каждое простое высказывание обозначают символами латинского алфавита (с индексами или без индексов), которые называют *пропозициональными символами*: A, B, C, A_1, A_2, \dots

Сложные высказывания составляются из простых с помощью союзов «не», «и», «или», «если ..., то...», «тогда и только тогда». Этим союзам соответствуют логические операции: унарная операция отрицания \neg («не»), бинарные операции конъюнкции $\&$ («и»), дизъюнкции \vee («или»), импликации \rightarrow («если..., то...», эквивалентности \equiv («тогда и только тогда»). Символы операций называют *пропозициональными связками*. Истинность или ложность сложного высказывания зависит от истинности или ложности входящих в

него простых высказываний, а также тем способом, которыми они комбинируются, т.е. связкой, используемой для построения сложного высказывания. Каждая логическая связка определяется своей *таблицей истинности* (см. табл. 10.1, 10.2).

Таблица 10.1

A	$\neg A$
F	T
T	F

Таблица 10.2

A	B	$A \& B$	$A \vee B$	$A \rightarrow B$	$A \equiv B$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

С помощью связки **отрицания** \neg из утвердительных получаются отрицательные высказывания. Например, если высказывание A – «воробей – птица» истинно, то высказывание $\neg A$ – «воробей не птица» – ложно, а высказывание $\neg\neg A$ – «Неверно, что воробей не птица» эквивалентно высказыванию «воробей – птица».

Конъюнкция $A \& B$, соответствующая союзам «и», «а», истинна в том и только том случае, если истинны оба входящих в нее высказывания. Например, утверждение «самый большой город Англии, Лондон (A), является ее столицей (B)» можно записать как $A \& B$. Высказывание «на улице идет дождь (A) с сильным ветром (B)» также выражается формулой $A \& B$. Конъюнкция коммутативна, потому высказывание «на улице сильный ветер (B) и дождь (A)», выразимое формулой $B \& A$, эквивалентно предыдущему. Однако, в естественном языке подобные высказывания не всегда эквивалентны, например, высказывания «девушка вышла замуж (A) и родила ребенка (B)» и «девушка родила ребенка (B) и вышла замуж (A)», эквивалентные в силу коммутативности конъюнкции, описывают, по всей видимости, совершенно различные ситуации, в которых неявно подразумевается временная последовательность событий. Для описания таких ситуаций средств логики высказываний недостаточно.

Для конъюнкции выполнен **закон противоречия**: $A \& \neg A \equiv F$ – формальное выражение принципа непротиворечивости.

Дизъюнкция $A \vee B$, соответствующая союзу «или», истинна в любом случае, когда истинно хотя бы одно входящее в нее высказывание, и ложна только в том случае, если оба простых высказывания ложны. Например, высказывание «дважды два – четыре (A) или пять (B)» выражается формулой $A \vee B$ и является истинным. Высказывание «население Канады говорит на английском (A) или на французском языке (B)» также выражается формулой $A \vee B$. Для дизъюнкции выполнен **закон исключенного третьего**: $A \vee \neg A \equiv T$.

Импликация $A \rightarrow B$ выражает логическую (часто – причинно-следственную) связь между высказываниями A и B и формализует высказывание, в котором из *посылки (антецедента)* A следует *заключение (консеквент)* B . Формула $A \rightarrow B$ читается как «из A следует B » или « A влечет B ». Импликация истинна в том случае, если из истинной посылки следует истинное заключение: $T \rightarrow T = T$, и ложна, если из истинной посылки следует ложное заключение: $T \rightarrow F = F$. Если же посылка ложна, то из нее может следовать как ложное, так и истинное заключение, – высказывание остается истинным в обоих случаях: $F \rightarrow T = T$, $F \rightarrow F = T$, т.е. *из лжи следует все, что угодно*. Обычно импликация $A \rightarrow B$ описывает некоторое правило, которое выражает *достаточность* истинности посылки A для того, чтобы выполнялась истинность заключения B , например: «если воду нагреть до 100 градусов (A), то она закипит (B)»; «чтобы получить диплом (B), нужно закончить институт (A)»; «если кошка перебежит дорогу (A), то случится неприятность (B)»; «когда на небе тучи (A), может пойти дождь (B)».

Эквивалентность $A \equiv B$ утверждает равнозначность (равносильность, тождественность) двух высказываний A и B ; она истинна тогда, когда истинностные значения A и B совпадают. Например, высказывание «животное является птицей (A) тогда и только тогда, когда у него есть крылья (B)» выразимо формулой $A \equiv B$.

$A \equiv B = (A \rightarrow B) \& (B \rightarrow A)$, т.е. эквивалентность утверждает не только достаточность условия A для того, чтобы было истинно B , но и необходимость этого условия. Например, утверждение: «птицы летают над морем (A) – земля близка (B)», – выражает одновременно два утверждения: достаточность условия – «если птицы летают над морем, то близка земля», и необходимость: «если земля близка, то птицы летают над морем».

С помощью логических связок сложные высказывания можно записать в виде *формулы*, которую называют *пропозициональной формой*.

Определение 10.2.

- Каждая пропозициональная буква есть формула.
- Если A и B – формулы, то формулами являются: $(\neg A)$, $(A \& B)$, $(A \vee B)$.
- Других формул нет.

При записи формул приняты следующие соглашения: внешние скобки можно опускать; установлен приоритет операций: \neg , $\&$, \vee , \rightarrow , \equiv . Логические связки для импликации \rightarrow и эквивалентности \equiv вводятся для сокращения записи формул: $A \rightarrow B = \neg A \vee B = \neg(A \& \neg B)$, $A \equiv B = (A \rightarrow B) \& (B \rightarrow A)$.

Построив формулу логики высказываний, мы отвлекаемся от ее содержательного смысла и оперируем только с понятиями истинности и ложности.

Приписывание пропозициональным буквам их истинностных значений называется *интерпретацией* формулы. Множество всех интерпретаций формулы образует ее *таблицу истинности*. Если выполнить отображения $0 \Leftrightarrow F, 1 \Leftrightarrow T$, то каждой пропозициональной связке будет соответствовать булева операция, а каждой формуле логики высказываний – булева формула, следовательно, логика высказываний является интерпретацией булевой алгебры. В связи с этим в ней сохраняются все аксиомы и теоремы булевой алгебры, в том числе представимость формул логики высказываний в виде СДНФ и СКНФ.

↪ **Определение 10.3.** Тавтологией истинная формула называется *тавтологией*. Тавтологически ложная формула называется *противоречием*. Формула, которая принимает истинное значение хотя бы на одной своей интерпретации, называется *выполнимой*. Две формулы называются *эквивалентными*, если их таблицы истинности совпадают.

Запись $\models A$ означает: «формула A – тавтология». Очевидно, что если A – тавтология, то $\neg A$ – противоречие.

Тавтологии являются *выделенными* формулами логики высказываний; именно они представляют наибольший интерес, так как формализуют правильные схемы рассуждений. Простые тавтологии, такие как «снег белый, потому что он белый», «масло масляное», выразимы формулой: $A \rightarrow A$, тождественную истинность которой нетрудно проверить: если $|A| = F$, то $F \rightarrow F = T$, если $|A| = T$, то $T \rightarrow T = T$. Утверждение: «Больной либо умрет, либо выживет» – тоже тавтология, так как оно выразимо тождественно истинной формулой: $A \vee \neg A$. Законы де Моргана также являются тавтологиями; нетрудно придать им содержательный смысл:

$\models \neg(A \vee B) \equiv (\neg A \ \& \ \neg B)$ – «неверно, что это преступление совершили A или B » эквивалентно высказыванию: «ни A , ни B не совершали этого преступления»;

$\models \neg(A \ \& \ B) \equiv (\neg A \vee \neg B)$ – «неверно, что A и B вместе участвовали в ограблении» эквивалентно «либо A , либо B , либо оба они в ограблении не участвовали».

Проблема разрешимости в алгебре высказываний заключается в том, чтобы отыскать эффективную процедуру (алгоритм), с помощью которой для каждой формулы логики высказываний можно установить, является она тавтологией или нет.

Очевидно, что такая процедура для формул логики высказываний существует: это построение таблиц истинности.

* Примеры.

1. В качестве примера рассмотрим закон утверждения консеквента: $\models A \rightarrow (B \rightarrow A)$. (Содержательно эта тавтология утверждает *принцип монотонности достоверных рассуждений*: если истинность некоторого высказывания A уже установлена, то добавление новых фактов не изменяет его истинности). Поскольку каждая строка таблицы истинности (табл. 10.3) этой формулы содержит значения T , формула является тавтологией.

Таблица 10.3

A	B	$B \rightarrow A$	$A \rightarrow (B \rightarrow A)$
F	F	T	T
F	T	F	T
T	F	T	T
T	T	T	T

2. **Метод редукции (сведение к противоречию)** служит способом сокращения перебора при составлении таблицы истинности. В качестве примера докажем, что формула $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ – тавтология.

Предположим, что это не так, т.е. существует такая интерпретация, на которой формула принимает ложное значение:

$$\overbrace{(A \rightarrow (B \rightarrow C))}^T \rightarrow \overbrace{((A \rightarrow B) \rightarrow (A \rightarrow C))}^F = F$$

$\underbrace{\hspace{1.5cm}}_T$
 $\underbrace{\hspace{1.5cm}}_F$

Получаем систему уравнений:

- 1) $|A \rightarrow (B \rightarrow C)| = T$,
- 2) $|A \rightarrow B| = T$,
- 3) $|A \rightarrow C| = F$.

Из 3) следует: $|A| = T, |C| = F$. Подставим эти значения в 2): $|T \rightarrow B| = T$, откуда $|B| = T$. Подставим найденные значения $|A| = T, |C| = F, |B| = T$ в 1): $|T \rightarrow (T \rightarrow F)| = |T \rightarrow F| = F$. Полученное значение противоречит условию 1), следовательно, не существует такой интерпретации, на которой формула принимает ложное значение, т.е. она является тавтологией.

3. Проверим, является ли следующая формула тавтологией:

$$(A \rightarrow (B \rightarrow C)) \rightarrow (A \vee B \rightarrow C).$$

Предположим, что $(A \rightarrow (B \rightarrow C)) \rightarrow (A \vee B \rightarrow C) = F$. Тогда

- 1) $|A \rightarrow (B \rightarrow C)| = T$,
- 2) $|A \vee B| = T$,
- 3) $|C| = F$.

Из 2) следует:

- a) $|A| = T, |B| = T$;
- б) $|A| = T, |B| = F$;
- с) $|A| = F, |B| = T$.

Подставляя значения $|A| = T, |B| = T$ в 1), получаем противоречие: $|T \rightarrow (T \rightarrow F)| = F$. Однако, это еще не доказывает, что формула является тавтологией. Рассмотрим другие значения:

- б) $|A| = T, |B| = F$.

Подставляя эти значения в 1), получим: $|T \rightarrow (F \rightarrow F)| = T$. Таким образом, на интерпретации $|A| = T, |B| = F, |C| = F$ формула принимает ложное значение, следовательно, она не является тавтологией.

10.3. Логическое следование

↪ **Определение 10.4.** Если A и B – формулы, то говорят, что B логически следует из A , или A логически влечет B , если на всех интерпретациях, где A принимает истинное значение, B также принимает истинное значение. Это обозначается как $A \models B$ или $A \Rightarrow B$.

Говорят, что логическое следование *сохраняет истинность*.

Теорема 10.1. Логическое следование $A \models B$ выполнено тогда и только тогда, когда формула $A \rightarrow B$ – тавтология.

Доказательство. Пусть логическое следование $A \models B$ выполнено. Это означает, что на всех интерпретациях, на которых формула $|A| = T$, формула $|B| = T$, следовательно, $|A \rightarrow B| = T$. Если формула $|A| = F$, то $|A \rightarrow B| = T$ независимо от значения B , следовательно, формула $A \rightarrow B$ – тавтология. Предположим теперь, что формула $A \rightarrow B$ – тавтология. Тогда не существует такой интерпретации, на которой $|A \rightarrow B| = F$. Следовательно, если формула $|A| = T$, то и $|B| = T$, что соответствует определению логического следования, т.е. $A \models B$. ▮

↪ **Определение 10.5.** Формула B логически следует из формул A_1, \dots, A_n , если на всех тех интерпретациях, на которых A_1, \dots, A_n принимают истинные значения одновременно, формула B также принимает истинное значение. Это обозначается так: $A_1, \dots, A_n \models B$.

Теорема 10.2. $A_1, A_2, \dots, A_n \models B$ тогда и только тогда, когда $\neg A_1 \& A_2 \& \dots \& A_n \rightarrow B$.

Доказать самостоятельно.

↪ **Определение 10.6.** Если $A \models B$ и $B \models A$, то формула A логически эквивалентна формуле B . Это обозначается как $A \Leftrightarrow B$, или $A \equiv B$.

Если формула A логически эквивалентна B , то $A \equiv B$ – тавтология.

✱ **Пример.** Проверим логическое следование: $A \rightarrow B, A \rightarrow \neg B \models \neg A$ и тавтологию: $\models (A \rightarrow B) \& (A \rightarrow \neg B) \rightarrow \neg A$. Обозначим тавтологию через E . Построим таблицу истинности (табл. 10.4).

Таблица 10.4

A	B	$A \rightarrow B$	$A \rightarrow \neg B$	$(A \rightarrow B) \& (A \rightarrow \neg B)$	$\neg A$	E
F	F	T	T	T	T	T
F	T	T	T	T	T	T
T	F	F	T	F	F	T
T	T	T	F	F	F	T

Как видим, на тех наборах, на которых посылки $A \rightarrow B, A \rightarrow \neg B$ принимают истинное значение одновременно, формула $\neg A$ также принимает истинное значение. Следовательно, логическое следование выполнено. С другой стороны, формула $(A \rightarrow B) \& (A \rightarrow \neg B) \rightarrow \neg A$ является тавтологией, что также является доказательством выполнимости логического следования. Содержательно логическое следование $A \rightarrow B, A \rightarrow \neg B \models \neg A$ (*приведение к абсурду*) формализует следующую схему рассуждений. Если из одной и той же посылки A выведено два противоположных заключения B и $\neg B$, то посылка неверна (это примерно то, о чем говорил Козьма Прутков: «Если на клетке с тигром написано «лев», не верь глазам своим»).

10.4. Теоремы о тавтологиях

Следующие теоремы о тавтологиях позволяют получать новые тавтологии из доказанных ранее.

Теорема 10.3 (правило *modus ponens*). Если A – тавтология и $A \rightarrow B$ – тавтология, то B – тавтология, т.е. если $\models A$ и $\models A \rightarrow B$, то $\models B$.

Доказательство. Предположим, что на некоторой интерпретации $|B| = F$. Тогда $|A \rightarrow B| = |A \rightarrow F| = T$ на той же интерпретации (по условию теоремы). Следовательно, $|A| = F$, что невозможно, так как A – тавтология. ▮

Правило *modus ponens* (сокращенно *МР*) устанавливает логическое следование $A, A \rightarrow B \models B$ и называется еще правилом *отделения*.

Правило *МР* выражает элементарный акт дедукции. Импликацию $A \rightarrow B$, которая по определению имеет смысл «если A , то B »,

можно интерпретировать как правило, в котором A является «причиной», а B – «следствием». Тогда правило МР говорит о том, что следствие B наступает при выполнении условия A , т.е. при истинности посылки. Например, формула $A \rightarrow B$ может выражать такое правило: «если на светофоре горит зеленый свет, то можно переходить дорогу». Мы ждем зеленого света на светофоре, чтобы перейти дорогу, т.е. мы неявно пользуемся правилом МР: когда посылка становится истинной (зеленый свет), то истинно и заключение (можно переходить дорогу). Тем самым мы выполняем элементарный акт дедукции: из истинности посылки мы выводим истинное заключение. Разумеется, этот вывод справедлив только в том случае, если правило $A \rightarrow B$ истинно. Например, многие полагают, что если кошка перебежит дорогу, то случится неприятность. Принимая это правило за истинное, человек, увидев перебегающую ему дорогу кошку, весь день ждет неприятности (и обычно ее находит). Многие правила, однако, не вызывают сомнений в их истинности. Это, например, математические теоремы, физические, химические и другие установленные законы.

Теорема 10.4 (правило подстановки). Если A – тавтология, содержащая пропозициональные переменные a_1, a_2, \dots, a_n , то формула B , полученная из A подстановкой формул A_1, A_2, \dots, A_n вместо каждого вхождения a_1, a_2, \dots, a_n соответственно, также будет тавтологией.

Доказательство. Пусть задано истинностное распределение для пропозициональных букв, входящих в B . Формулы A_1, \dots, A_n для этого распределения примут некоторые значения $\delta_1, \delta_2, \dots, \delta_n$, где δ_i есть T или F . Если такое же распределение придать пропозициональным буквам a_1, a_2, \dots, a_n , то значение формулы A совпадет со значением формулы B . Так как A – тавтология, то значение B при этом распределении будет T . Таким образом B при любом истинностном распределении входящих в нее букв будет принимать значение T . Следовательно, B – тавтология. \square

✱ **Пример.** Формула $A \rightarrow (B \rightarrow A)$ – тавтология. Подставим $A \vee B$ вместо A , получим новую тавтологию: $|A \vee B \rightarrow (B \rightarrow A \vee B)|$. Таким образом, каждую тавтологию можно рассматривать как схему, из которой с помощью подстановки можно получить бесконечное множество тавтологий.

Теорема 10.5 (правило эквивалентной замены). Если B получается из A подстановкой формулы B_1 вместо одного или нескольких вхождений подформулы A_1 в A , то $((A_1 \equiv B_1) \rightarrow (A \equiv B))$ есть тавтология, и, следовательно, если A_1 и B_1 логически эквивалентны, то A и B также логически эквивалентны.

Иными словами, если есть тавтология A , и в ней есть подформула A_1 , и если заменить A_1 на эквивалентную ей формулу B_1 , то полученная формула B будет эквивалентна A .

Доказательство. Рассмотрим произвольное истинностное распределение переменных, входящих в A, B, A_1, B_1 . Если при этом распределении A_1 и B_1 имеют различные значения, то $|A_1 \equiv B_1| = F$ и, следовательно, $((A_1 \equiv B_1) \rightarrow (A \equiv B))$ примет значение T . Если же A_1 и B_1 принимают одинаковые значения, то одинаковые истинностные значения примут A и B , так как B отличается от A только тем, что некоторые вхождения подформулы A_1 заменены в ней на B_1 , которая имеет то же самое истинностное значение. Следовательно, в этом случае, если $|A_1 \equiv B_1| = T$, то и $|A \equiv B| = T$, и $((A_1 \equiv B_1) \rightarrow (A \equiv B))$ есть тавтология. \square

✱ **Пример.** В тавтологии $A \rightarrow (B \rightarrow A)$ заменим подформулу $B \rightarrow A$ на эквивалентную ей формулу $\neg B \vee A$, получим новую тавтологию $A \rightarrow \neg B \vee A$. Тавтологией также будет формула: $A \rightarrow \neg(B \& \neg A)$, так как $B \rightarrow A$ эквивалентно $\neg(B \& \neg A)$.

10.5. Формализация и решение логических задач

Язык логики высказываний используется для формализации предложений естественного языка и доказательства логических следований. Для этого каждое простое высказывание обозначается пропозициональной буквой; сложное высказывание записывается как формула, в которой связки естественного языка заменяются пропозициональными связками (как это указано в 10.2).

✱ **Пример 10.1.** Рассмотрим логическое следование. Если цены растут, уровень жизни падает. Если уровень жизни падает, то люди недовольны. Цены растут. Следовательно, люди недовольны.

Обозначим пропозициональными буквами простые высказывания: P – «цены растут»; S – «уровень жизни падает»; R – «люди недовольны». Необходимо доказать логическое следование: $P \rightarrow S, S \rightarrow R, P \models R$.

Доказательство.

1 способ. Проверить, что формула $(P \rightarrow S) \& (S \rightarrow R) \& P \rightarrow R$ – тавтология. Для этого достаточно построить таблицу истинности.

2 способ. Доказательство от противного (метод редукции).

Предположим, что существует такая интерпретация, на которой все посылки принимают истинное значение, а заключение – ложное, т.е. $|P \rightarrow S| = T, |S \rightarrow R| = T, |P| = T, |R| = F$. Тогда из $|S \rightarrow R| = |S \rightarrow F| = T$ следует, что $|S| = F$; из $|P \rightarrow S| = |P \rightarrow F| = T$ следует, что $|P| = F$, что противоречит третьей посылке $|P| = T$. Это противоречие доказывает логическое следование.

3 способ. Построение логического вывода.

Логическое следование – это некоторое правильное с логической точки зрения рассуждение. Некоторые логические следования формализуют простейшие схемы рассуждений и используются как *правила вывода* истинных заключений из истинных посылок. Последовательное применение правил вывода к заданной системе посылок позволяет строить логический вывод. Логический вывод, в котором из истинных посылок могут быть получены только истинные заключения, называется *достоверным (дедуктивным) выводом (рассуждением)*.

Построим логический вывод, используя известные правила вывода. Логический вывод записывается обычно как нумерованная последовательность формул, справа от каждой формулы записывается комментарий, указывающий, на каком основании формула включена в эту последовательность. Посылки вывода обычно обозначаются буквой Г (гипотеза).

- | | |
|----------------------|-----------------|
| 1. $P \rightarrow S$ | Г1 |
| 2. $S \rightarrow R$ | Г2 |
| 3. P | Г3 |
| 4. S | правило МР(3,1) |
| 5. R | правило МР(4,2) |

Последняя формула в этом выводе является логическим следствием посылок Г1, Г2, Г3.

В силу того, что правило МР сохраняет истинность, каждая формула, участвующая в выводе, истинна при истинности посылок Г1, Г2, Г3. Поэтому, если соединить символом \rightarrow формулы, так чтобы посылка импликации предшествовала заключению в этом выводе, то полученная формула также будет истинной, и, следовательно, она является логическим следованием исходных посылок. Поэтому из данного вывода мы можем получить логическое следование: $P \rightarrow S, S \rightarrow R \models P \rightarrow R$. Это логическое следование соответствует правилу вывода, которое называют *правилом силлогизма*:

$$A \rightarrow B, B \rightarrow C \models A \rightarrow C.$$

★ **Пример 10.2.** Из-за плохой погоды (А) рейс может быть отложен (В): $A \rightarrow B$. Рейс не отложен ($\neg B$). Следовательно, погода не плохая ($\neg A$). Докажем $A \rightarrow B, \neg B \models \neg A$.

Предположим, что $|A \rightarrow B| = T, |\neg B| = T$ и $|\neg A| = F$, тогда $|A \rightarrow B| = |T \rightarrow F| = F$. Полученное противоречие доказывает логическое следование.

Это логическое следование соответствует правилу вывода *modus tollens (MT)*:

$$A \rightarrow B, \neg B \models \neg A.$$

★ **Пример 10.3.** Дело может быть пересмотрено (В) в том случае, если результаты расследования вызывают сомнения (А): $A \rightarrow B$. Следовательно, если дело не пересматривается ($\neg B$), то результаты расследования не вызывают сомнения ($\neg A$): $\neg B \rightarrow \neg A$.

Предположим, что $|A \rightarrow B| = T, |\neg B \rightarrow \neg A| = F$, тогда $|\neg B| = T, |\neg A| = F$ и $|A \rightarrow B| = |T \rightarrow F| = F$. Полученное противоречие доказывает логическое следование.

Это логическое следование соответствует *правилу контрапозиции*:

$$A \rightarrow B \models \neg B \rightarrow \neg A.$$

★ **Пример 10.4.** Получить возможные логические следования из данного множества посылок. *Малые дети неразумны. Тот, кто может укрощать крокодилов, заслуживает уважения. Неразумные люди не заслуживают уважения.*

Пусть А – «человек – малый ребенок», В – «человек разумен», С – «человек заслуживает уважения», D – «человек может укрощать крокодилов». Построим логический вывод, используя доказанные ранее правила вывода.

- | | |
|--|----------------------------|
| 1. $A \rightarrow \neg B$ | Г1 |
| 2. $D \rightarrow C$ | Г2 |
| 3. $\neg B \rightarrow \neg C$ | Г3 |
| 4. $A \rightarrow \neg C$ | правило силлогизма (1, 3). |
| (Малые дети не заслуживают уважения). | |
| 5. $C \rightarrow B$ | правило контрапозиции (3). |
| (Только разумные люди заслуживают уважения). | |
| 6. $D \rightarrow B$ | правило силлогизма (2, 5). |
| (Разумно укрощать крокодилов). | |
| 7. $\neg B \rightarrow \neg D$ | правило контрапозиции (6). |
| (Неразумные люди не укрощают крокодилов). | |
| 8. $A \rightarrow \neg D$ | правило силлогизма (1, 7). |
| (Малые дети не укрощают крокодилов). | |

Таким образом, из данного набора посылок мы вывели все возможные заключения. Такие логические задачи называются *соритами*.

Понятие о дедуктивном методе мы получаем прежде всего из детективной литературы, в частности, от Шерлока Холмса. Как известно, Шерлок Холмс пользовался при раскрытии преступлений именно дедуктивным методом. Вот как он объясняет сущность дедуктивного метода: «Мой принцип расследования состоит в том, чтобы исключить все явно невозможные предположения. Тогда то, что остается, является истиной, какой бы неправдоподобной она ни казалась». Это рассуждение можно выразить такой схемой: $A \vee B, \neg A \models B$, что эквивалентно $\neg A \rightarrow B, \neg A \models B$, т.е. применению

правила МР. В одном из рассказов о Шерлоке Холмсе сложилась такая ситуация: «Нам известно, что преступник не мог попасть в комнату ни через дверь (A), ни через дымовой ход (B). Мы знаем также, что он не мог спрятаться в комнате (C), поскольку в ней прятаться негде. Как же тогда он проник сюда? – Через крышу(D)! – Без сомнения. Он мог проникнуть в эту комнату только через крышу.» Это рассуждение можно формализовать так: $A \vee B \vee C \vee D$, $\neg A, \neg B, \neg C \models D$, что равносильно: $\neg A \rightarrow (\neg B \rightarrow (\neg C \rightarrow D))$, $\neg A, \neg B, \neg C \models D$. Трехкратное применение правила МР доказывает это логическое следование.

Не следует забывать, что логическое следование выполнено только тогда, когда из истинных посылок следует истинное заключение. Поэтому должна существовать хотя бы одна интерпретация (т.е. истинностное распределение букв, входящих в каждую посылку), на которой все посылки истинны одновременно. Если такой интерпретации не существует, то система посылок противоречива и из нее выводимо любое заключение, т.е. вместе с некоторой формулой A выводимо и ее отрицание $\neg A$. С другой стороны, логическое следование может оказаться не выполненным, если посылка недостаточно для вывода нужных заключений. В таких случаях, в зависимости от содержания задачи, множество посылок может быть пополнено.

★ **Пример 10.5.** Проверить непротиворечивость множества посылок:
 $A \rightarrow \neg B \ \& \ C, D \vee E \rightarrow G, G \rightarrow \neg(H \vee K), \neg C \ \& \ E \ \& \ H$.

Предположим, что существует интерпретация, на которой все посылки принимают истинное значение:

1. $|A \rightarrow \neg B \ \& \ C| = T$,
2. $|D \vee E \rightarrow G| = T$,
3. $|G \rightarrow \neg(H \vee K)| = T$,
4. $|\neg C \ \& \ E \ \& \ H| = T$.

Из 4 следует: $|\neg C| = T, |C| = F, |E| = T, |H| = T$. Подставляя $|C| = F$ в 1, находим: $|A \rightarrow \neg B \ \& \ F| = T$, откуда $|A| = F$. Подставляя $|E| = T$ в 2, получим: $|D \vee T \rightarrow G| = T$, откуда $|G| = T$. Подставим это значение в 3, получим $|T \rightarrow \neg(H \vee K)| = T$, откуда $|\neg(H \vee K)| = T$, т.е. $|H \vee K| = F$, следовательно, $|H| = F, |K| = F$. Получили противоречие: $|H| = T, |H| = F$, откуда следует, что данная система посылок противоречива.

Глава 11.

ФОРМАЛЬНЫЕ ТЕОРИИ. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

11.1. Определение формальной теории

Теория называется *содержательной*, если существует какая-либо интерпретация объектов, операций, символов теории. Логика высказываний является содержательной теорией, так как каждый символ в ней интерпретируется как простое высказывание, истинное или ложное, формулы также могут быть истинными или ложными, и, несмотря на то, что мы отвлекаемся от содержательного смысла высказываний, все рассуждения ведутся в терминах истинности и ложности. В отличие от содержательных теорий, формальная теория (исчисление) представляет собой множество символов и отношений между ними, которым не приписывается никакого содержательного смысла. Вспоминая о задачах логики, можно сказать, что выражения и формулы формальной теории представляют «чистые» схемы рассуждений, которым можно придавать самый разнообразный смысл, т.е. строить различные модели теории.

Формальные теории строятся по следующим правилам.

Задается счетное множество символов, которое называется *алфавитом* теории. Из этого множества символов строятся конечные последовательности, которые называются *словами* или *выражениями* данной теории. Из множества выражений выделяют *правильно построенные выражения* — *формулы*. Из множества формул выделяют подмножество *аксиом*. Между формулами теории определяют отношения — *правила вывода* теории. Правила вывода позволяют из множества аксиом выводить *теоремы*. Таким образом, формальная теория является аксиоматической теорией.

↪ **Определение 11.1.** Доказательством теоремы называют последовательность формул A_1, \dots, A_n , каждая из которых либо является аксиомой, либо получена из предыдущих по правилам вывода данной теории. Каждая формула в списке является *теоремой* данной теории. Иными словами, *теорема* — это формула, выводимая из множества аксиом по правилам вывода, определенным в данной теории. Запись $\vdash_J A_n$ означает, что формула A_n выводима в теории J , т.е. является теоремой теории J .

↪ **Определение 11.2.** Выводом формулы A_n из множества гипотез Γ называется последовательность формул A_1, \dots, A_n , каждая из которых является либо аксиомой, либо гипотезой из множества Γ , либо получена из предыдущих по *правилам вывода*. Формула A_n называется выводимой из множества гипотез Γ . Обозначение

$\Gamma \vdash_n A_n$ означает, что формула A_n выводима из множества гипотез Γ в теории J .

Доказательство отличается от вывода тем, что в нем не используются гипотезы, поэтому теорему можно определить как формулу, выводимую из пустого множества гипотез.

Свойства выводимости.

1. Если $\Gamma \vdash B$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash B$ (Δ — множество формул).

Это свойство называется свойством *монотонности* вывода. Оно означает, что формула B будет по-прежнему выводима, если к множеству гипотез Γ , из которых выводима формула B , добавить другие гипотезы, т.е. расширить множество гипотез Γ до Δ .

2. $\Gamma \vdash B$ тогда и только тогда, когда существует $\Delta \subseteq \Gamma$, такое что $\Delta \vdash B$. Это свойство *полноты* множества гипотез: для того, чтобы формула B была выводима из множества гипотез Γ , необходимо и достаточно, чтобы в Γ существовало подмножество $\Delta \subseteq \Gamma$, из которого выводима формула B . Иными словами, не все гипотезы из заданного множества гипотез Γ обязательно должны использоваться в процессе вывода, — некоторые могут оказаться лишними, однако, заданных гипотез должно быть достаточно для вывода B .

3. Если $\Delta \vdash A$, и для каждого $B_i \in \Delta$, $\Gamma \vdash B_i$ то $\Gamma \vdash A$. Это свойство *транзитивности* отношения выводимости. Оно позволяет использовать ранее доказанные теоремы (выводы), не повторяя всего списка формул, составляющих доказательство (вывод). Поэтому ранее доказанные теоремы и выводы могут использоваться в других доказательствах как схемы, в которых каждое вхождение переменной может замещаться произвольной формулой.

11.2. Исчисление высказываний.

Формальная теория L

Определение 11.3.

1. *Символами алфавита* теории L являются пропозициональные буквы A, B, C, \dots с индексами или без индексов, пропозициональные связки \neg, \rightarrow , и вспомогательные символы — скобки: (и).

2. *Определение формулы.*

- Всякая пропозициональная буква есть формула.
- Если A и B есть формулы, то формулами являются $(\neg A)$, $(A \rightarrow B)$.
- Других формул нет.

3. В формальной теории L определено бесконечное множество аксиом, которые задаются тремя *схемами аксиом*:

A1: $A \rightarrow (B \rightarrow A)$;

A2: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$;

A3: $(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$.

Конкретные аксиомы получаются подстановкой формулы вместо каждого вхождения одной и той же пропозициональной буквы.

4. В теории L определено единственное *правило вывода* МР:

$A, A \rightarrow B \vdash B$.

Для сокращения записи формул вводятся *метаопределения*:

МО1: $\neg(A \rightarrow \neg B) = A \ \& \ B$.

МО2: $\neg A \rightarrow B = A \vee B$.

МО3: $(A \rightarrow B) \ \& \ (B \rightarrow A) = A \equiv B$.

11.3. Доказательство и вывод в формальной теории L

Рассмотрим доказательство и вывод в теории L . Докажем теорему $A \rightarrow A$. Поскольку единственным правилом вывода является МР, нам нужно взять такую аксиому, чтобы выводимая формула $A \rightarrow A$ оказалась в конце формулы. Возьмем схему аксиомы A2, сделав замену B на $A \rightarrow A$ и C на A . Получим

$(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$.

В схеме аксиомы A1 также заменим B на $A \rightarrow A$, получим

$A \rightarrow ((A \rightarrow A) \rightarrow A)$.

Теперь к этим двум формулам применим правило МР, в результате чего получим

$(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$.

В схеме аксиомы A1 заменим B на A , получим

$A \rightarrow (A \rightarrow A)$.

Применяя к двум последним формулам правило МР, получим $A \rightarrow A$.

Доказательство и вывод принято записывать в столбик, нумеруя каждую формулу и указывая справа в качестве комментария, на каком основании формула включена в эту последовательность. Ниже приводятся доказательства теорем 1, 2.

Теорема 1. $\vdash A \rightarrow A$

1. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow$	
$\rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$	A2
2. $A \rightarrow ((A \rightarrow A) \rightarrow A)$	A1
3. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$	МР(1, 2)
4. $A \rightarrow (A \rightarrow A)$	A1
5. $A \rightarrow A$	МР(3, 4)

Теорема 2. $\vdash (\neg A \rightarrow A) \rightarrow A$

1. $(\neg A \rightarrow \neg A) \rightarrow ((\neg A \rightarrow A) \rightarrow A)$ A3

2. $\neg A \rightarrow \neg A$ T1

3. $(\neg A \rightarrow A) \rightarrow A$ MP(1, 2)

При доказательстве теоремы 2 в пункте 2 мы ссылались на доказанную ранее теорему 1, что фактически соответствует включению в доказательство всех пунктов доказательства теоремы 1.

Построим выводы.

B1. Правило силлогизма.

$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$

1. $A \rightarrow B$ Г1

2. $B \rightarrow C$ Г2

3. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ A2

4. $(B \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))$ A1

5. $A \rightarrow (B \rightarrow C)$ MP(2, 4)

6. $(A \rightarrow B) \rightarrow (A \rightarrow C)$ MP(3, 5)

7. $A \rightarrow C$ MP(1, 6)

B2. Правило удаления средней посылки.

$A \rightarrow (B \rightarrow C), B \vdash A \rightarrow C$

1. $A \rightarrow (B \rightarrow C)$ Г1

2. B Г2

3. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ A2

4. $(A \rightarrow B) \rightarrow (A \rightarrow C)$ MP(1, 3)

5. $B \rightarrow (A \rightarrow B)$ A1

6. $A \rightarrow B$ MP(2, 5)

7. $A \rightarrow C$ MP(4, 6)

Такие правила вывода, доказанные средствами формальной теории, называются *производными* правилами вывода.

11.4. Метатеорема о дедукции

В формальных теориях используется символический язык для описания некоторой содержательной теории. Этот язык имеет точно определенный синтаксис и формальные средства логического вывода (правила вывода). С помощью этих средств из выбранных аксиом можно выводить теоремы формальной теории. Однако, обсуждение свойств формальной теории и получаемых результатов обычно производится в некоторой другой теории, которую называют *метатеорией*. Язык этой метатеории называют *метаязыком*. Саму же формальную теорию называют тогда *предметной*, или *объектной* теорией, а ее язык — *предметным* языком, или *языком-*

объектом. Изучение свойств формальной теории, производимое содержательными математическими методами средствами метаязыка, называют *теорией доказательств*, или *метаматематикой*.

Рассмотрим некоторые особенности формального доказательства и вывода в теории L . В качестве метаязыка мы будем пользоваться обычным русским языком. Теоремы о свойствах формальной теории, доказанные с помощью содержательного метаязыка, будем называть *метатеоремами*.

Метатеорема о дедукции (МТД).

Если из множества формул Γ и формулы A выводима формула B , то из множества Γ выводима формула $A \rightarrow B$, т.е. если $\Gamma, A \vdash B$, то $\Gamma \vdash A \rightarrow B$.

Доказательство этой метатеоремы может быть проведено по методу математической индукции. Пусть вывод формулы B — это последовательность $B_1, B_2, \dots, B_n = B$. Докажем следующую металемму.

Металемма. Из $\Gamma, A \vdash B_i$ следует, что $\Gamma \vdash A \rightarrow B_i$ ($i = 1, \dots, n$).

Доказательство металеммы.

Базис индукции. Пусть $i = 1$. Рассмотрим три случая.

а) B_1 — аксиома.

$\vdash B_1$

$\vdash B_1 \rightarrow (A \rightarrow B_1)$ A1

$\vdash A \rightarrow B_1$ по правилу MP

$\Gamma \vdash A \rightarrow B_1$ по свойству выводимости 1.

б) $B_1 = A$, т.е. B_1 есть сама формула A .

$\vdash A \rightarrow A$ T1

Поскольку теорема выводима из пустого множества посылок, она выводима из любого множества посылок, согласно свойству выводимости 1. Поэтому $\Gamma \vdash A \rightarrow A$, что равносильно $\Gamma \vdash A \rightarrow B_1$.

в) $B_1 \in \Gamma$, т.е. B_1 — гипотеза из Γ .

Доказательство проводится так же, как и в случае а).

Шаг индукции. Пусть металемма выполнена для всех $k < i$. Докажем, что она выполняется при $k = i$. Возможны четыре случая:

а) B_i — аксиома; { доказательство проводится

б) $B_i = A$; { так же, как и для базиса

в) $B_i \in \Gamma$; { индукции.

г) B_i выводится по MP из предыдущих формул, т.е. в последовательности B_1, \dots, B_n есть формулы: B_m и $B_l = B_m \rightarrow B_i$ ($m < l < i$). Тогда по предположению индукции справедливы выводы:

$\Gamma \vdash A \rightarrow B_m$,

$\Gamma \vdash A \rightarrow B_l$ т.е. $\Gamma \vdash A \rightarrow (B_m \rightarrow B_i)$.

По схеме аксиомы A2

$$\vdash (A \rightarrow (B_m \rightarrow B_i)) \rightarrow ((A \rightarrow B_m) \rightarrow (A \rightarrow B_i)).$$

Применяя дважды к последним трем выражениям правило МР, получим $\Gamma \vdash A \rightarrow B_i$.

При $i = n$ получим формулировку метатеоремы о дедукции. \approx
Справедлива метатеорема, обратная метатеореме о дедукции.

Обратная метатеорема о дедукции.

Если существует вывод $\Gamma \vdash A \rightarrow B$, то формула B выводима из Γ и A , т.е. если $\Gamma \vdash A \rightarrow B$, то $\Gamma, A \vdash B$

Доказательство. Пусть вывод формулы $A \rightarrow B$ имеет вид: $B_1, \dots, B_{n-1}, A \rightarrow B$, где B_1, \dots, B_{n-1} — формулы из множества Γ . Тогда вывод формулы B из Γ и A будет иметь вид: $B_1, \dots, B_{n-1}, A \rightarrow B, A, B$, так как B следует из $A \rightarrow B$ и A по правилу МР. \approx

Из метатеоремы о дедукции выводимы следствия:

Следствие 1 (B1). Правило силлогизма: $A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$.

Следствие 2 (B2). Правило удаления средней посылки:
 $A \rightarrow \rightarrow (B \rightarrow C), B \vdash A \rightarrow C$.

Следствие 3 (B3) Правило удаления крайней посылки:
 $(A \rightarrow B) \rightarrow \rightarrow C \vdash B \rightarrow C$.

Правила силлогизма и удаления средней посылки были доказаны ранее, без использования метатеоремы о дедукции. Для сравнения приведем доказательство правила B2 с ее использованием. Пользуясь обратной метатеоремой о дедукции, будем строить вывод:

$$A \rightarrow (B \rightarrow C), B, A \vdash C.$$

- | | |
|--------------------------------------|------------|
| 1. $A \rightarrow (B \rightarrow C)$ | $\Gamma 1$ |
| 2. B | $\Gamma 2$ |
| 3. A | $\Gamma 3$ |
| 4. $B \rightarrow C$ | МР(1,3) |
| 5. C | МР(2,4) |

Теперь, по метатеореме о дедукции, получаем вывод:
 $A \rightarrow (B \rightarrow C), B \vdash A \rightarrow C$.

(B3) Правило удаления крайней посылки: $(A \rightarrow B) \rightarrow C \vdash B \rightarrow C$.

Применяя обратную метатеорему о дедукции, получим:
 $(A \rightarrow B) \rightarrow \rightarrow C, B \vdash C$.

- | | |
|--------------------------------------|------------|
| 1. $(A \rightarrow B) \rightarrow C$ | $\Gamma 1$ |
| 2. B | $\Gamma 2$ |
| 3. $B \rightarrow (A \rightarrow B)$ | A1 |
| 4. $A \rightarrow B$ | МР(2, 3) |
| 5. C | МР(1, 4) |

По метатеореме о дедукции, получаем вывод: $(A \rightarrow B) \rightarrow C \vdash B \rightarrow C$.

Применение метатеоремы о дедукции (МТД) позволяет из любого правила вывода получить теорему. Например, применяя два раза МТД к правилу силлогизма, получим теорему силлогизма:

$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$	правило силлогизма
$A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$	МТД
$\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	МТД

Обратная метатеорема о дедукции (ОМТД) позволяет получать правила вывода из теорем. Например, применяя два раза ОМТД к аксиоме A3, получим правило вывода:

$\vdash (\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$	A3
$\neg B \rightarrow \neg A \vdash ((\neg B \rightarrow A) \rightarrow B)$	ОМТД
$\neg B \rightarrow \neg A, \neg B \rightarrow A \vdash B$	ОМТД

Применение метатеоремы о дедукции и следствий из нее позволяет упрощать построение выводов и доказательств. Рассмотрим примеры такого применения. (Необходимо отметить, что приводимые ниже доказательства не являются единственными, могут быть найдены и другие доказательства соответствующих теорем.)

Теорема 3 (снятия двойного отрицания). $\vdash \neg \neg A \rightarrow A$

- | | |
|---|---------|
| 1. $(\neg A \rightarrow \neg \neg A) \rightarrow ((\neg A \rightarrow \neg A) \rightarrow A)$ | A3 |
| 2. $\neg A \rightarrow \neg A$ | T1 |
| 3. $(\neg A \rightarrow \neg \neg A) \rightarrow A$ | B2(1,2) |
| 4. $\neg \neg A \rightarrow A$ | B3(3) |

Теорема 4 (введения двойного отрицания). $\vdash A \rightarrow \neg \neg A$

- | | |
|---|---------|
| 1. $(\neg \neg \neg A \rightarrow \neg A) \rightarrow ((\neg \neg \neg A \rightarrow A) \rightarrow \neg \neg A)$ | A3 |
| 2. $\neg \neg \neg A \rightarrow \neg A$ | T3 |
| 3. $(\neg \neg \neg A \rightarrow A) \rightarrow \neg \neg A$ | МР(1,2) |
| 4. $A \rightarrow \neg \neg A$ | B3(3) |

Теорема 5 (противоречия). $\vdash \neg A \rightarrow (A \rightarrow B)$

Построим вывод: $\neg A, A \vdash B$.

- | | |
|---|------------|
| 1. $\neg A$ | $\Gamma 1$ |
| 2. A | $\Gamma 2$ |
| 3. $(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$ | A3 |
| 4. $\neg A \rightarrow (\neg B \rightarrow \neg A)$ | A1 |
| 5. $A \rightarrow (\neg B \rightarrow A)$ | A1 |
| 6. $\neg B \rightarrow \neg A$ | МР(1,4) |
| 7. $\neg B \rightarrow A$ | МР(2,5) |
| 8. $(\neg B \rightarrow A) \rightarrow B$ | МР(3,6) |
| 9. B | МР(7,8) |

Теорема 6 (контрапозиции). $\vdash (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

Построим вывод: $\neg A \rightarrow \neg B \vdash B \rightarrow A$

1. $\neg A \rightarrow \neg B$ Г1
2. $(\neg A \rightarrow \neg B) \rightarrow ((\neg A \rightarrow B) \rightarrow A)$ А3
3. $(\neg A \rightarrow B) \rightarrow A$ МР(1,2)
4. $B \rightarrow A$ В3(3)

Теорема 7 (контрапозиции). $\vdash (B \rightarrow A) \rightarrow (\neg A \rightarrow \neg B)$

Построим вывод: $B \rightarrow A \vdash \neg A \rightarrow \neg B$

1. $B \rightarrow A$ Г1
2. $\neg \neg B \rightarrow B$ Т3
3. $A \rightarrow \neg \neg A$ Т4
4. $\neg \neg B \rightarrow A$ В1(2,1)
5. $\neg \neg B \rightarrow \neg \neg A$ В1(3,4)
6. $(\neg \neg B \rightarrow \neg \neg A) \rightarrow (\neg A \rightarrow \neg B)$ Т6
7. $\neg A \rightarrow \neg B$ МР(5,6)

Теорема 8. $\vdash A \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$

Построим вывод: $A \vdash \neg B \rightarrow \neg(A \rightarrow B)$

1. $((A \rightarrow B) \rightarrow B) \rightarrow (\neg B \rightarrow \neg(A \rightarrow B))$ Т7
2. A Г1
3. $A, A \rightarrow B \vdash B$ МР
4. $A \vdash (A \rightarrow B) \rightarrow B$ МТД(3)
5. $(A \rightarrow B) \rightarrow B$ из (2,4)
6. $\neg B \rightarrow \neg(A \rightarrow B)$ МР(1,5)

В доказательстве этой теоремы фактически использовались средства метаязыка — из правила МР применением МТД было получено новое правило вывода: $A \vdash (A \rightarrow B) \rightarrow B$.

Теорема 9. $\vdash (A \rightarrow B) \rightarrow ((\neg A \rightarrow B) \rightarrow B)$

Построим вывод: $A \rightarrow B, \neg A \rightarrow B \vdash B$

1. $A \rightarrow B$ Г1
2. $\neg A \rightarrow B$ Г2
3. $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ Т7
4. $(\neg A \rightarrow B) \rightarrow (\neg B \rightarrow \neg \neg A)$ Т7
5. $\neg B \rightarrow \neg A$ МР(1,3)
6. $\neg B \rightarrow \neg \neg A$ МР(2,4)
7. $(\neg B \rightarrow \neg \neg A) \rightarrow ((\neg B \rightarrow \neg A) \rightarrow B)$ А3
8. $(\neg B \rightarrow \neg A) \rightarrow B$ МР(6,7)
9. B МР(5,8)

11.5. Правила введения и удаления связок

При доказательстве теорем и построении выводов можно использовать производные правила вывода, доказанные ранее, в том числе правила введения и удаления связок (см. табл. 11.1).

Таблица 11.1.

Связка	Введение	Удаление
\rightarrow	$\Gamma, A \vdash B \Rightarrow \Rightarrow \Gamma \vdash A \rightarrow B$ (МТД)	$A, A \rightarrow B \vdash B$ (МР) $\Gamma_1 \vdash A, \Gamma_2 \vdash A \rightarrow B \Rightarrow \Rightarrow \Gamma_1, \Gamma_2 \vdash B$
\neg	$\Gamma, A \vdash B;$ $\Gamma, A \vdash \neg B \Rightarrow \Gamma \vdash \neg A$ (доказательство от противного)	$A, \neg A \vdash B$ (слабое удаление отрицания) $\neg \neg A \vdash A$ (удаление двойного отрицания)
$\&$	$\Gamma_1 \vdash A, \Gamma_2 \vdash B \Rightarrow \Rightarrow \Gamma_1, \Gamma_2 \vdash A \& B$	$\Gamma \vdash A \& B \Rightarrow \Gamma \vdash A$ $\Gamma \vdash A \& B \Rightarrow \Gamma \vdash B$
\vee	$\Gamma \vdash A \Rightarrow \Gamma \vdash A \vee B$ $\Gamma \vdash B \Rightarrow \Gamma \vdash A \vee B$	$\Gamma_1 \vdash A \vee B; \Gamma_2, A \vdash C;$ $\Gamma_3, B \vdash C \Rightarrow \Gamma_1, \Gamma_2, \Gamma_3 \vdash C$
\equiv	$A \rightarrow B, B \rightarrow A \vdash A \equiv B$	$A \equiv B \vdash A \rightarrow B;$ $A \equiv B \vdash B \rightarrow A$

Докажем некоторые из этих правил.

В4. \neg — введение. $A \rightarrow B, A \rightarrow \neg B \vdash \neg A$

1. $A \rightarrow B$ Г1
2. $A \rightarrow \neg B$ Г2
3. $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$ Т7
4. $(A \rightarrow \neg B) \rightarrow (\neg \neg B \rightarrow \neg A)$ Т7
5. $\neg B \rightarrow \neg A$ МР(1,3)
6. $\neg \neg B \rightarrow \neg A$ МР(2,4)
7. $(\neg B \rightarrow \neg A) \rightarrow ((\neg \neg B \rightarrow \neg A) \rightarrow \neg A)$ Т9
8. $(\neg \neg B \rightarrow \neg A) \rightarrow \neg A$ МР(5,7)
9. $\neg A$ МР(6,8)

В5. $\&$ — удаление 1. $A \& B \vdash A$.

Пользуясь метаопределением МО1, получим $\neg(A \rightarrow \neg B) \vdash A$, и применим МТД:

- $$\vdash \neg(A \rightarrow \neg B) \rightarrow A$$
1. $\neg A \rightarrow (A \rightarrow \neg B)$ Т5
 2. $(A \rightarrow \neg B) \rightarrow \neg \neg(A \rightarrow \neg B)$ Т4
 3. $\neg A \rightarrow \neg \neg(A \rightarrow \neg B)$ В1(1,2)

4. $(\neg A \rightarrow \neg\neg(A \rightarrow \neg B)) \rightarrow (\neg(A \rightarrow \neg B) \rightarrow A)$	T6
5. $\neg(A \rightarrow \neg B) \rightarrow A$	MP(3,4)
B6. & – удаление 2. $A \& B \vdash B$	
$\neg(A \rightarrow \neg B) \vdash B$	МО1
$\vdash \neg(A \rightarrow \neg B) \rightarrow B$	МТД
Доказать самостоятельно.	
B7. & – введение. $A, B \vdash A \& B$	
$A, B \vdash \neg(A \rightarrow \neg B)$	МО1
1. A	Г1
2. B	Г2
3. $A \rightarrow (\neg\neg B \rightarrow \neg(A \rightarrow \neg B))$	T8
4. $\neg\neg B \rightarrow \neg(A \rightarrow \neg B)$	MP(1,3)
5. $B \rightarrow \neg\neg B$	T4
6. $\neg\neg B$	MP(2,5)
7. $\neg(A \rightarrow \neg B)$	MP(4,6)

11.6. Другие формализации логики высказываний

Помимо \neg и \rightarrow , можно использовать другие функционально полные наборы связок, например, \vee и \neg или $\&$ и \neg , тогда будут получены другие формализации логики высказываний. Рассмотрим такие теории.

Теория L_1 (Гильберта, Аккермана). Основные связки: \vee, \neg .

Метаопределение: $A \rightarrow B = \neg A \vee B$.

Схемы аксиом:

A1: $A \vee A \rightarrow A$.

A2: $A \rightarrow A \vee B$.

A3: $A \vee B \rightarrow B \vee A$.

A4: $(B \rightarrow C) \rightarrow (A \vee B \rightarrow A \vee C)$.

Правило вывода: MP.

Теория L_2 (Россера). Основные связки: $\&, \neg$.

Метаопределение: $A \rightarrow B = \neg(A \& \neg B)$.

Схемы аксиом:

A1: $A \rightarrow (A \& A)$.

A2: $(A \& B) \rightarrow A$.

A3: $(A \rightarrow B) \rightarrow (\neg(B \& C) \rightarrow \neg(C \& A))$.

Правило вывода: MP.

Формальная теория, предложенная Клини, использует четыре логические связки: $\neg, \rightarrow, \&, \vee$.

Теория L_4 (Клини). Схемы аксиом:

A1: $A \rightarrow (B \rightarrow A)$.

A2: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.

A3: $(A \& B) \rightarrow A$.

A4: $(A \& B) \rightarrow B$.

A5: $A \rightarrow (B \rightarrow (A \& B))$.

A6: $A \rightarrow A \vee B$.

A7: $B \rightarrow A \vee B$.

A8: $(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow (A \vee B \rightarrow C))$.

A9: $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$.

A10: $\neg\neg A \rightarrow A$.

Правило вывода: MP.

11.7. Свойства формальной теории L

Для исследования свойств формальной теории обычно строится ее модель. Приписывание значений первичным терминам формальной теории называется ее *интерпретацией*. Если множество объектов, выбранных в качестве значений первичных терминов теории, удовлетворяет аксиомам формальной теории, то такая интерпретация называется *моделью* формальной теории.

Основными свойствами формальных теорий являются их непротиворечивость и полнота. Теория называется *противоречивой*, если она содержит такую формулу A , что как A , так и $\neg A$ являются теоремами теории. Теория не являющаяся противоречивой, называется *непротиворечивой*. Иными словами, в непротиворечивой теории не существует такой формулы A , что A и $\neg A$ являются теоремами. Противоречивые теории считаются не имеющими никакой ценности, так как любая формула такой теории есть теорема, и, следовательно, в ней можно вывести что угодно. Вопрос о непротиворечивости теории можно установить с помощью модели. Если теория противоречива, то каждая ее модель будет содержать противоречие, так как любая пара противоречивых формул A и $\neg A$, являющихся теоремами теории, будут переводиться в противоречивые высказывания модели. Теория непротиворечива, если для нее удастся найти свободную от противоречий модель. Если непротиворечивость теории доказана (или хотя бы принята на веру), то рассматривается вопрос о ее полноте. *Полнота* теории означает, что она содержит достаточное для каких-либо целей количество теорем. Например, если из теории L исключить схему аксиом A3, то в ней станут невыводимыми многие теоремы, содержащие отрицания (так как A1, A2 не содержат отрицаний). Очевидно, такая теория будет неполной, но пополнимой. Различают определе-

ния полноты в узком и в широком смысле. Теорию считают *полной в широком смысле*, если любой формуле A теории соответствует такое предложение модели, которое либо истинно, либо ложно. Тогда либо A , либо $\neg A$ оказывается истинным и должно быть выводимо в формальной теории, т.е. любая формула A теории, либо ее отрицание $\neg A$ является теоремами формальной теории.

Теория, которая одновременно непротиворечива и полна, является максимальной в том смысле, что добавление к ней в качестве аксиомы какой-либо формулы, не являющейся ее теоремой, приводит к противоречивой теории. Это свойство формальных теорий называют *полнотой в узком смысле*. Добавление к системе аксиом каких-либо теорем теории не изменяет ее свойств, но тогда система аксиом станет избыточной, так как некоторые аксиомы можно будет вывести из других аксиом. Например, система аксиом Клини (теория L_c) содержит избыточные аксиомы, выводимые из других аксиом. Система аксиом, содержащая такие аксиомы, что ни одна из них не выводима из других, называется *независимой*. Свойство независимости системы аксиом не является обязательным для формальных теорий, — это вопрос лаконичности и компактности средств формальной теории.

Рассмотрим свойства теории L . В качестве интерпретации формальной теории L выберем алгебру высказываний. Поставим в соответствие каждой букве теории L пропозициональную букву, каждой формуле L — формулу логики высказываний, каждой теореме — тавтологию логики высказываний. Нетрудно убедиться, что схемы аксиом теории L являются тавтологиями алгебры высказываний. Следовательно, логика высказываний является моделью теории L .

☞ **Определение 11.4.** Формальная теория *полна относительно модели*, если каждой теореме теории соответствует тождественная истинная формула модели, а каждой тождественно истинной формуле модели соответствует теорема формальной теории.

Покажем, что формула теории L тогда и только тогда является теоремой, когда она является тавтологией логики высказываний.

Метатеорема 11.1. Каждая теорема теории L является тавтологией логики высказываний.

Доказательство. Схемам аксиом $A1, A2, A3$ соответствуют тавтологии логики высказываний. Для проверки этого положения достаточно построить их таблицы истинности. Правило MP сохраняет свойство тавтологичности согласно теореме 10.3 о тавтологиях. Поскольку любая теорема выводима из аксиом с помощью правила MP , ей также будет соответствовать тавтология логики высказываний. ☞

Метатеорема 11.2 (теорема о полноте). Каждая тавтология логики высказываний является теоремой формальной теории L .

Доказательство основывается на следующей металемме.

Металемма. Пусть формула A логики высказываний зависит от пропозициональных букв B_1, B_2, \dots, B_k . Тогда каждой строке таблицы истинности этой формулы соответствует вывод формальной теории L вида $B_1', \dots, B_k' \vdash A'$, где $B' = B$, если $|B| = T$, и $B' = \neg B$, если $|B| = F$, $A' = A$ или $\neg A$, если $|A| = T$ или F соответственно.

Смысл леммы заключается в следующем. Если дана формула, например, $E = A \rightarrow ((A \rightarrow B) \rightarrow A)$, то, построив ее таблицу истинности (табл. 11.2), можно определить, из каких посылок она выводима.

Таблица 11.2.

A	B	$(A \rightarrow B) \rightarrow A$	$B \rightarrow ((A \rightarrow B) \rightarrow A)$
F	F	F	T
F	T	F	F
T	F	T	T
T	T	T	T

Согласно металемме, для данной формулы можно построить четыре вывода: $\neg A, \neg B \vdash E$; $\neg A, B \vdash \neg E$; $A, \neg B \vdash E$; $A, B \vdash E$.

Доказательство металеммы.

Доказательство проводится индукцией по числу связей n в формуле A .

1. *Базис индукции.* Пусть $n = 0$, тогда $A = B$, т.е. A представляет собой просто пропозициональную букву B . Тогда формула A может принимать одно из двух значений, T или F , каждому из которых соответствует вывод: $B \vdash B$ и $\neg B \vdash \neg B$.

2. *Шаг индукции.* Допустим, число связей в формуле A равно m и при этом выполняется металемма. Докажем, что металемма выполняется, если $n = m + 1$.

1 случай. Формула A образована с помощью связки отрицания: $A = \neg B$, где B содержит m связей. Возможны следующие случаи.

а) $|B| = T$, тогда $|\neg B| = F$, т.е. $|A| = F$. Необходимо доказать, что существует вывод:

$$B_1', \dots, B_n' \vdash \neg A.$$

Согласно предположению индукции, существует вывод: $B_1', \dots, B_n' \vdash B$. Согласно теореме 4, $B \vdash \neg \neg B$, тогда по правилу силлогизма $B_1', \dots, B_n' \vdash \neg \neg B$. Но $\neg \neg B = \neg A$, поскольку $A = \neg B$, следовательно, $B_1', \dots, B_n' \vdash \neg A$.

б) $|B| = F, |\neg B| = T, |A| = T$. Необходимо доказать, что существует вывод $B'_1, \dots, B'_n \vdash A$, или, что то же самое, $B'_1, \dots, B'_n \vdash \neg B$.

Так как $|B| = F$, то $\neg B = B'$. Вывод $B'_1, \dots, B'_n \vdash B'$ существует по предположению индукции, значит, существует и $B'_1, \dots, B'_n \vdash \neg B$.

2 случай. Формула A образована с помощью логической связки импликации: $A = B \rightarrow C$, где B и C содержат не более m связок. По предположению индукции существуют выводы:

$$B'_1, \dots, B'_n \vdash B',$$

$$B'_1, \dots, B'_n \vdash C'.$$

Рассмотрим истинностные распределения.

$$а) |C| = T, |A| = T.$$

Нужно доказать, что существует вывод $B'_1, \dots, B'_n \vdash A$, т.е. $B'_1, \dots, B'_n \vdash B \rightarrow C$.

По индуктивному предположению существует вывод $B'_1, \dots, B'_n \vdash C$. Тогда из этого вывода и аксиомы А1: $C \rightarrow (B \rightarrow C)$ по МР получаем: $B'_1, \dots, B'_n \vdash B \rightarrow C$.

$$б) |B| = F, |A| = T.$$

Вывод $B'_1, \dots, B'_n \vdash \neg B$ существует по индуктивному предположению. Тогда из этого вывода и теоремы Т5: $\vdash \neg B \rightarrow (B \rightarrow C)$ по правилу МР получаем: $B'_1, \dots, B'_n \vdash B \rightarrow C$.

в) $|C| = F, |B| = T, |A| = F$. Доказать, что существует вывод $B'_1, \dots, B'_n \vdash \neg A$, т.е. $B'_1, \dots, B'_n \vdash \neg(B \rightarrow C)$. Построим этот вывод.

$$1. B'_1, \dots, B'_n \vdash \neg C \quad (\text{по индуктивному предположению})$$

$$2. B'_1, \dots, B'_n \vdash B \quad (\text{по индуктивному предположению})$$

$$3. \vdash B \rightarrow (\neg C \rightarrow \neg(B \rightarrow C)) \quad \text{T8}$$

$$4. B'_1, \dots, B'_n \vdash \neg C \rightarrow \neg(B \rightarrow C) \quad \text{MP(2,3)}$$

$$5. B'_1, A = \neg B, \dots, B'_n \vdash \neg(B \rightarrow C) \quad \text{MP(1,4)}$$

Металемма доказана. \simeq

Доказательство метатеоремы о полноте.

Пусть A — тавтология, зависящая от пропозициональных букв B_1, \dots, B_n . Согласно металемме, для каждого истинностного распределения пропозициональных букв существуют выводы: $B'_1, \dots, B'_n \vdash A$ (A' совпадает с A , так как A истинно в каждой строке таблицы истинности). В таблице истинности имеются две строки, которые различаются только значением истинности B_n . Для этих строк существуют выводы:

$$B'_1, \dots, B'_n \vdash A, \text{ где } |B_n| = T \text{ и}$$

$$B'_1, \dots, \neg B_n \vdash A, \text{ где } |B_n| = F.$$

Применим к ним метатеорему о дедукции. Получим:

$$B'_1, \dots, B'_{n-1} \vdash B_n \rightarrow A,$$

$$B'_1, \dots, B'_{n-1} \vdash \neg B_n \rightarrow A.$$

Возьмем теорему Т9: $\vdash (B_n \rightarrow A) \rightarrow ((\neg B_n \rightarrow A) \rightarrow A)$.

Применяя дважды правило МР, получим, вывод $B'_1, \dots, B'_{n-1} \vdash A$.

Аналогичным образом мы можем исключить все переменные, и за n шагов получим $\vdash A$. \simeq

➤ **Определение 11.5.** Формальная теория непротиворечива, если не существуют такой формулы A , чтобы A и $\neg A$ одновременно являлись теоремами теории.

Метатеорема 11.3. Теория L непротиворечива.

Доказательство. Каждая теорема теории L является тавтологией логики высказываний. Отрицание формулы, являющейся тавтологией, тавтологией не является. Следовательно, ни для какой формулы A невозможно, чтобы A и $\neg A$ были теоремами теории L . \simeq

Из непротиворечивости L следует существование формулы, которая не является теоремой теории L . С другой стороны, непротиворечивость теории L можно вывести из факта существования формулы теории, не являющейся теоремой. Действительно, если теория L противоречива, т.е. в ней существуют теоремы $\vdash \neg A$ и $\vdash A$, то двукратным применением правила МР из теоремы $\vdash \neg A \rightarrow (A \rightarrow B)$ получаем $\vdash B$, т.е. тогда в L выводима любая формула. (Теорию, в которой не все формулы являются теоремами, часто называют абсолютно непротиворечивой).

Полнота теории понимается в узком и широком смысле.

➤ **Определение 11.6.** Теория называется *полной (в узком смысле)*, если добавление к ней в качестве аксиомы любой недоказуемой в этой теории формулы делает ее противоречивой. *Полнота в широком смысле* означает, что каждую формулу можно доказать либо опровергнуть, т.е. либо $\vdash A$, либо $\vdash \neg A$.

Метатеорема 11.4. Теория L неполна в широком смысле.

Доказательство. Действительно, не любая формула или ее отрицание являются теоремами теории L . Если взять нейтральную формулу логики высказываний, то ее отрицание также является нейтральной формулой, т.е. ни сама формула, ни ее отрицание не являются тавтологиями алгебры высказываний. Поэтому эти формулы не являются теоремами исчисления L . \simeq

Метатеорема 11.5. Теория L полна в узком смысле.

Для доказательства теоремы нужно показать, что теория L становится противоречивой при добавлении к ее системе аксиом любой недоказуемой в этой теории формулы.

Доказательство. Теория L имеет три схемы аксиом А1, А2, А3 и правило вывода МР. Построим новую теорию L' , добавив к системе

аксиом L формулу A , которая не является тавтологией алгебры высказываний. Тогда формула A принимает хотя бы одно ложное значение на некоторой интерпретации. Значит, если A представлена конъюнктивной нормальной формой, то эта форма должна содержать хотя бы одну элементарную дизъюнкцию δ , не содержащую ни одну переменную вместе с ее отрицанием: $\delta = B'_1 \vee B'_2 \vee \dots \vee B'_n$, где $B'_i = \neg B_i$, если $|B_i| = T$, и $B'_i = B_i$, если $|B_i| = F$. В элементарной дизъюнкции δ заменим каждое вхождение пропозициональной буквы B'_i на B , если $|B_i| = F$, и на $\neg B$, если $|B_i| = T$. Получим: $\delta' = B \vee \neg B \vee \dots \vee B \vee \neg B = B$. Произведем другую замену: заменим B'_i на $\neg B$, если $|B_i| = F$, и на B , если $|B_i| = T$. Получим: $\delta'' = \neg B \vee \neg B \vee \dots \vee \neg B = \neg B$. В новой теории L' формула A — аксиома, т.е. $\vdash A$. Поскольку A представима в виде СКНФ, то по правилу удаления $\&$ любая дизъюнкция δ конъюнктивной нормальной формы также доказуема, а поскольку дизъюнкция δ представима как в виде δ' , так и в виде δ'' , то в L' имеет место $\vdash \delta'$ и $\vdash \delta''$, а это означает, что $\vdash_{L'} \neg B$ и $\vdash_{L'} B$, т.е. теория L' противоречива. \sphericalangle

Определение 11.7. Формальная теория называется *разрешимой*, если существует эффективная процедура, позволяющая за конечное число шагов определить, является произвольная формула теоремой или нет.

Теория L разрешима, так как каждой теореме теории соответствует тавтология, а для любой тавтологии можно построить таблицу истинности.

Определение 11.8. Система аксиом является *независимой*, если ни одна из аксиом не может быть выведена из других.

Метатеорема 11.6. Схемы аксиом $A1$, $A2$, $A3$ в теории L независимы.

Доказательство. Докажем независимость $A1$. Для этого необходимо построить такую непротиворечивую модель, в которой выполняются все аксиомы, кроме первой. Построим модель в трехзначной логике, где истинностные значения операций \neg и \rightarrow определены в табл. 11.3, 11.4.

Формулу A будем считать выделенной, если она всегда принимает значение 0. Нетрудно показать, что правило МР сохраняет свойство выделенности. Можно показать (построением таблиц истинности), что схемы аксиом $A2$, $A3$ являются выделенными в данной модели. Следовательно, выделенной является и всякая формула, выводимая из $A2$, $A3$ с помощью правила МР. Однако формула $A1$ не выделенная, — для доказательства этого достаточно найти один набор, на котором значение $A1$ отлично от 0, например: $1 \rightarrow (2 \rightarrow 1) = 1 \rightarrow 0 = 2$.

Таблица.11.3.

A	$\neg A$
0	1
1	1
2	0

Таблица.11.4.

A	B	$A \rightarrow B$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

Аналогично можно доказать независимость $A2$, построив другую трехзначную модель, где выделенными будут аксиомы $A1$ и $A3$ ¹. Чтобы показать независимость $A3$, достаточно переопределить отрицание так, чтобы $\neg x = x$ (тождественная операция). Тогда $A1$ и $A2$ по-прежнему будут тавтологиями, а $A3$ уже не будет тавтологией.

¹ Подробное доказательство можно найти в [Мендельсон, 1976].

Глава 12.

ТЕОРИЯ ПРЕДИКАТОВ
ПЕРВОГО ПОРЯДКА

12.1. Понятие предиката

Существуют такие логические схемы рассуждений, которые не могут быть обоснованы в логике высказываний. Рассмотрим умозаключение: «Все люди смертны (A). Сократ — человек (B). Следовательно, Сократ смертен (C)». Очевидно, что C следует из A и B , однако, логическое следование $A, B \models C$ недоказуемо в логике высказываний. Причина заключается во внутренней структуре высказываний.

Внутреннюю структуру высказывания можно разделить на субъект и предикат, где субъект есть подлежащее, а предикат определяет свойство субъекта (рис. 12.1).

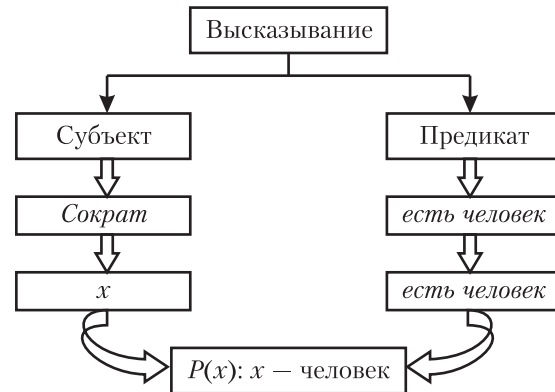


Рис.12.1. Структура высказывания.

Например, *Сократ* — это субъект, который обладает свойством быть человеком. Это свойство представляет собой одноместный предикат, определенный на множестве людей: «__ есть человек». Обозначим его $P(x)$, где x — переменная, обозначающая так называемое «свободное место предиката». Подставляя на место переменной x объекты из области определения предиката, получаем высказывания. Таким образом, одноместный предикат, определенный на некотором множестве объектов, задает свойство, которым эти объекты могут обладать или не обладать. При подстановке на свободное место предиката какого-либо объекта из его области определения предикат обращается в высказывание, истинное или ложное. Таким образом, предикат разбивает это множество на две области: области истинности и ложности.

↪ **Определение 12.1.** Одноместным предикатом $P(x)$, определенным на множестве M , называется выражение, которое после подстановки в него вместо x предмета из области определения M обращается в высказывание. Область определения предиката называется *предметной областью*. Элементы из области определения называются *предметными постоянными (предметами)*. Переменная, от которой зависит предикат, называется *предметной переменной*.

Одноместные предикаты традиционно служат для формализации понятий. *Понятие* представляет собой единицу мышления. Абстрактное мышление основывается на понятиях, отображающих действительность, поэтому абстрактное мышление называют понятийным. Понятия возникают как результат обобщения множества предметов по системе признаков, общей только для этих выделенных предметов. *Признак* — это наличие или отсутствие свойства у предмета, а также наличие или отсутствие отношения между предметами. Понятие характеризуется своим содержанием и объемом. *Содержание понятия* — это система признаков, на основе которой множество предметов обобщается в понятие. *Объем понятия* — это множество предметов, обобщаемых и выделяемых в понятие, т.е. множество предметов, которые характеризуются системой признаков, составляющих содержание понятия. Например, понятие «рыба» можно охарактеризовать как множество всех живых существ (объем понятия), которые обладают признаками: живут в воде, плавают, имеют жабры, плавники и хвост (содержание понятия). Каждое из перечисленных свойств можно задать одноместным предикатом, определенным на множестве *всех живых существ*: $V(x)$ — x живет в воде, $P(x)$ — x плавает, $G(x)$ — x имеет жабры, $L(x)$ — x имеет плавники, $R(x)$ — x имеет хвост. Таким образом, понятие рыба может быть описано выражением: $V(x) \& P(x) \& G(x) \& L(x) \& R(x)$. Область истинности этого выражения составляет *объем* понятия — это все существующие рыбы. Между объемом и содержанием понятия существует обратная зависимость: чем больше объем, тем меньше содержание. Например, понятие «обитатели водных глубин» можно определить как «множество всех существ, живущих в воде». Содержание этого понятия описывается предикатом $V(x)$ — x живет в воде. Добавив свойство $P(x)$ — x плавает, мы увеличим содержание понятия, но уменьшим объем: будут исключены моллюски, ракообразные и прочие обитатели водных глубин, которые не плавают. Добавив новые свойства, мы еще более уменьшим объем понятия.

Двуместный предикат задает отношение между двумя объектами. Объекты могут принадлежать одной и той же, либо разным областям определения. Например, предикат $P(x, y): x > y$, где

$x, y \in \mathbf{R}$, задает отношение «больше» на множестве действительных чисел; подставив в него значения, получим высказывания, например: $5 > 2 = T$, $6,8 > 10 = F$. Если в предикат $P(x, y): x > y$ подставить значение $y = 0$, получим одноместный предикат: $x > 0$, который задает *свойство* действительных чисел быть (или не быть) больше нуля и определяет понятие «*положительные действительные числа*». На место переменной в предикат можно подставить функцию, определенную на предметной области предиката и принимающую значения в этой области. Например, если в предикат $P(x, y)$ подставить на место x функцию $f(u, v) = u + v$, получим новый предикат: $R(f(u, v), y): u + v > y$, определяющий отношение между суммой двух чисел и третьим числом.

Другой пример двуместного предиката: $S(x, y)$: «*x родился в y году*», где $x \in \{\text{люди}\}$, $y \in \mathbf{N}$. Предикат $S(x, y)$ задает отношение на множестве людей и множестве целых чисел. При замене y на объект из области определения, например, $y = 1814$, получим одноместный предикат $S(x, 1814)$, определяющий свойство: «*человек x родился в 1814 году*». При замене обеих переменных получим высказывание, например, «*Лермонтов родился в 1814 году*».

Таким образом, двуместный предикат задает некоторое бинарное отношение на заданных множествах, причем при замене одной переменной местность предиката понижается (двуместный предикат становится одноместным), а при замене обеих переменных на предметные постоянные он обращается в высказывание.

В общем случае n -местный предикат определяет n -местное отношение.

↪ **Определение 12.2.** N -местным предикатом, определенным на множествах M_1, M_2, \dots, M_n , называется выражение, которое обращается в высказывание при замене каждой предметной переменной на элемент из ее области определения. Если все предметные переменные определены на одном и том же множестве, то предикат называется *однородным*.

✱ Примеры.

$R(x, y, z, t)$: «*x родился в y году в городе z, имеет образование t*», $x \in \{\text{люди}\}$, $y \in \mathbf{N}$, $z \in \{\text{города}\}$, $t \in \{\text{начальное, среднее, высшее}\}$. $R(x, y, z, t)$ — неоднородный четырехместный предикат. Однородный предикат: $Q(x, y, z)$: «*параллелепипед имеет высоту x, ширину y, длину z*», где $x, y, z \in \mathbf{R}$.

12.2. Формулы логики предикатов

12.2.1. Операции над предикатами

Предикат можно рассматривать как функцию, определенную на некотором множестве объектов и принимающую два значения, T и F . Поэтому над предикатами определены все булевы операции: \neg (отрицание), $\&$ (конъюнкция), \vee (дизъюнкция), \rightarrow (импликация), \equiv (эквивалентность), а также две новые операции — операции наложения кванторов: \forall — всеобщности и \exists — существования.

Если $P(x)$ определяет некоторое свойство на множестве M , то формула $\forall x P(x)$ обозначает высказывание: «для всякого предмета $x \in M$ свойство $P(x)$ выполнено», или «все x обладают свойством $P(x)$ ». Значение формулы $|\forall x P(x)| = T$ (истинно), если свойство P выполнено для всех объектов из M , и $|\forall x P(x)| = F$ (ложно), если существует хотя бы один элемент $x = a$, $a \in M$, для которого свойство P не выполнено, т.е. $|P(a)| = F$. Например: если $P(x)$: x смертен, $x \in \{\text{люди}\}$, то $\forall x P(x)$ — «все люди смертны» (значение формулы $|\forall x P(x)| = T$); если $P(x)$: $x > 0$, $x \in \mathbf{R}$, то $\forall x P(x)$ — «все действительные числа положительные» ($|\forall x P(x)| = F$).

Формула $\exists x P(x)$ означает: «существует по крайней мере один предмет x , обладающий свойством $P(x)$ », или: «некоторые x обладают свойством $P(x)$ ». Значение формулы $|\exists x P(x)| = T$ (истинно), если существует хотя бы один элемент $x = a$, $a \in M$, для которого свойство P выполнено: $|P(a)| = T$; значение $|\exists x P(x)| = F$ (ложно), если свойство P не выполнено для всех объектов из M . Например: если $P(x)$: $x > 0$, $x \in \mathbf{R}$, то $\exists x P(x)$ — это высказывание: «некоторые действительные числа положительны», тогда $|\exists x P(x)| = T$; если $P(x)$: x смертен, $x \in \{\text{люди}\}$, то $\exists x \neg P(x)$ — «существуют бессмертные люди» (ложное высказывание).

Если $M = \{a_1, a_2, \dots, a_n\}$ — конечная область определения предиката $P(x)$, то формулы с кванторами могут быть выражены через конъюнкцию и дизъюнкцию:

$$\forall x P(x) = P(a_1) \& P(a_2) \& \dots \& P(a_n), \exists x P(x) = P(a_1) \vee P(a_2) \vee \dots \vee P(a_n).$$

Таким образом, квантор всеобщности является обобщением конъюнкции, а квантор существования — обобщением дизъюнкции на бесконечную область определения.

Кванторы \forall и \exists связаны друг с другом по принципу двойственности (по законам де Моргана):

$$\neg \forall x P(x) \equiv \exists x \neg P(x), \neg \exists x P(x) \equiv \forall x \neg P(x).$$

Например, если $P(x)$: «*x смертен*», $x \in \{\text{люди}\}$, то формула $\neg \forall x P(x)$ обозначает высказывание: «не все люди смертны», которое эквивалентно высказыванию «существуют бессмертные люди», т.е.

$\exists x \neg P(x)$, а формула $\neg \exists x P(x)$ — «не существует смертных людей» эквивалентна высказыванию «все люди бессмертны», т.е. $\forall x \neg P(x)$.

12.2.2. Определение формулы

Основными символами языка логики предикатов являются:

- пропозициональные символы \neg и \rightarrow ,
- кванторы всеобщности \forall и существования \exists ,
- вспомогательные символы: запятая , и скобки (,),
- предметные переменные $x_1, x_2, \dots, x_n, \dots$,
- предметные постоянные $a_1, a_2, \dots, a_n, \dots$,
- функциональные символы $f_1^1, f_1^2, \dots, f_k^j, \dots$,
- предикатные символы $P_1^1, P_1^2, \dots, P_k^j, \dots$.

Нижний индекс предикатного или функционального символа — это номер, который служит для различения одноименных символов с одинаковым числом аргументов, верхний индекс указывает число аргументов.

Определим понятия *терма* и *формулы*.

Определение терма.

- ↪ 1. Каждая предметная переменная есть *терм*.
 2. Каждая предметная постоянная есть *терм*.
 3. Если f_k^j — функциональный символ и t_1, \dots, t_n — термы, то $f_k^j(t_1, \dots, t_n)$ есть терм.
 4. Других термов нет.

Определение формулы.

- ↪ 1. $P_i^n(t_1, \dots, t_n)$, где P_i^n — предикатный символ, t_1, \dots, t_n — термы, есть *атомарная (элементарная) формула*.
 2. Если A и B — формулы и x — предметная переменная, то формулами являются $(\neg A)$, $(A \rightarrow B)$, $(\forall x A)$, $(\exists x A)$.
 3. Других формул нет.

Выражения $A \& B$, $A \vee B$, $A \equiv B$ определяются так же, как в исчислении L .

Определение 12.3. Формула, на которую распространяется действие квантора, называется *областью действия квантора*. Переменная, по которой навешивается квантор и попадающая в его область действия, называется *связанной переменной*. Переменная, лежащая вне области действия квантора, называется *свободной переменной*.

- ↪ Формула, не содержащая свободных переменных, называется *замкнутой*. Замкнутые формулы являются высказываниями.

Область действия квантора ограничивается скобками, если она содержит более одного предиката.

* Примеры.

1. На рис. 12.2 приведены примеры формул логики предикатов и указаны свободные и связанные переменные.

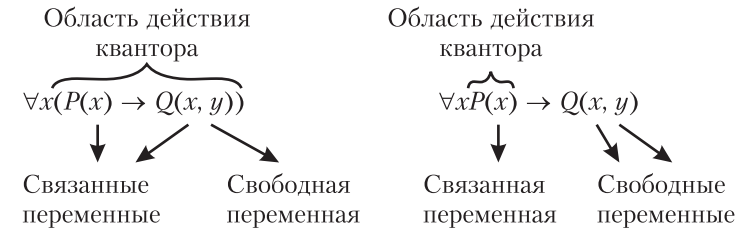


Рис. 12.2. Свободные и связанные переменные.

2. Пусть $Q(x, y)$: « x родился в y году», $x \in \{\text{люди}\}$, $y \in \{\text{годы}\}$, тогда формула $\forall x \exists y Q(x, y)$ обозначает высказывание: «Каждый человек родился в каком-нибудь году», а формула $\exists y \forall x Q(x, y)$ — высказывание: «Существует такой год, в котором родились все люди». Из этого примера видно, что разноименные кванторы в общем случае не перестановочны.

В формулах логики предикатов можно делать замену переменных (в общем случае — термов) при выполнении определенных условий, которые сводятся к тому, чтобы никакое свободное вхождение переменной не стало связанным в результате замены.

↪ **Определение 12.4.** Говорят, что терм y *свободен для переменной x в формуле $A(x)$* , если никакое свободное вхождение x в $A(x)$ не лежит в области действия никакого квантора по z , где z — переменная, входящая в терм y .

Всякий терм, не содержащий переменных, свободен для любой переменной в любой формуле. Всякий терм свободен для x в формуле $A(x)$, если $A(x)$ не содержит свободных вхождений x . Терм y свободен для любой переменной в формуле A , если никакая переменная терма y не является связанной переменной в формуле A .

* Примеры.

$\exists x(x = 2y)$, $x, y \in \mathbf{R}$. В этой формуле z свободно для y : $\exists x(x = 2z)$. Терм $f(x, z)$ свободен для x в формуле $\forall y A(x, y) \rightarrow B(x)$, но не свободен для x в формуле $\exists z \forall y A(x, y) \rightarrow B(x)$.

12.3. Интерпретация формул логики предикатов

Формулы имеют смысл только тогда, когда имеется какая-либо интерпретация входящих в нее символов.

↪ **Определение 12.5.** Под *интерпретацией* будем понимать систему, состоящую из непустого множества D , называемого *областью интерпретации*, а также соответствия, ставящего каждой предикатной букве P_i^n некоторое отношение на области D , каждой предметной постоянной a_i — некоторый элемент из области D , каждой функциональной букве f_i^n — некоторую n -местную операцию на области D (т.е. функцию $D^n \rightarrow D$).

При заданной интерпретации все предметные переменные пробегает все значения из области D , а логические связки имеют обычный логический смысл.

Для заданной интерпретации всякая замкнутая формула представляет собой высказывание, которое истинно или ложно, а формула со свободными переменными выражает отношение на области D , которое может быть истинно (выполнено) при одних значениях переменных и ложно (не выполнено) при других.

* Примеры.

1. В таблице 12.1. приведены три интерпретации одной и той же формулы.

Таблица 12.1.

Область интерпретации D	Интерпретация	Высказывание $\forall x(P(x) \rightarrow Q(x))$
Множество живых существ	$P(x)$: x — рыба, $Q(x)$: x живет в воде.	Все рыбы живут в воде.
Множество живых существ	$P(x)$: x — человек, $Q(x)$: x смертен.	Все люди смертны.
Множество целых чисел	$P(x)$: x делится на 6, $Q(x)$: x делится на 3.	Все числа, которые делятся на 6, делятся на 3.

2. Пусть дана формула $\exists x \exists y P(f(x, y), t)$. Предикат $P(v, u)$ — двуместный, переменные x, y — связанные, t — свободная переменная. Зададим следующую интерпретацию: область интерпретации D — множество действительных чисел \mathbf{R} , $t = 1$, $f(x, y) = x^2 + y^2$, предикат $P(u, t)$: $u = t$. Тогда формула имеет вид: $\exists x \exists y (x^2 + y^2 = 1)$. Она истинна, так как существуют такие x и y , которые удовлетворяют уравнению окружности $x^2 + y^2 = 1$.

Если положить $f(x, y) = x^2 + y^2$, $t = r^2$, то формула $\exists x \exists y (x^2 + y^2 = r^2)$ — одноместный предикат, область истинности которого — множество действительных чисел, удовлетворяющих уравнению окружности $x^2 + y^2 = r^2$ с радиусом r .

↪ **Определение 12.6.** Интерпретация называется *моделью* для данного множества формул Γ , если каждая формула из Γ истинна в данной интерпретации.

↪ **Определение 12.7.** Формула называется *выполнимой*, если существует хотя бы одна интерпретация, на которой формула истинна.

↪ **Определение 12.8.** Формула называется *логически общезначимой* (ЛОЗ), если она истинна на любой интерпретации для любых значений переменных.

Так же, как тавтологии, логически общезначимые формулы обозначаются: $\models A(x)$.

↪ **Определение 12.9.** Формула, которая ложна на любой интерпретации при любых значениях переменных, называется *противоречием*.

Логически общезначимые формулы являются выделенными формулами логики предикатов.

Так как область определения предиката может быть бесконечной, то, очевидно, что построение таблицы истинности не может служить алгоритмом для определения логической общезначимости формул. Однако существуют другие способы, которые в частных случаях позволяют определить логическую общезначимость, выполнимость или эквивалентность формул. Можно строить таблицы истинности формул логики предикатов для частичных интерпретаций на ограниченных конечных областях. Например, возьмем область интерпретации, состоящую из двух произвольных элементов: $D = \{a, b\}$. Построим таблицу истинности формул: $E_1 = \exists x P(x)$ и $E_2 = \forall x P(x)$. Одноместный предикат на области определения из двух элементов может принимать одно из четырех значений, которые определяются таблицами истинности (табл. 12.2).

Таблица 12.2

x	$P_1(\cdot)$	$P_2(\cdot)$	$P_3(\cdot)$	$P_4(\cdot)$
a	F	F	T	T
b	F	T	F	T

Формулы E_1 и E_2 будут принимать на этих интерпретациях следующие значения (табл. 12.3).

Таблица.12.3

$P(\cdot)$	$\exists xP(x)$	$\forall xP(x)$
P_1	F	F
P_2	T	F
P_3	T	F
P_4	T	T

Построим таблицы истинности на области интерпретации из двух элементов $D = \{a, b\}$ для следующих формул:

$E_1 = \forall yP(y) \rightarrow \exists xQ(x)$, $E_2 = \forall y(P(y) \rightarrow \exists xQ(x))$, $E_3 = \forall y \exists x(P(y) \rightarrow Q(x))$. Для этих формул существует 16 интерпретаций, так как каждый из одноместных предикатов P и Q принимает по 4 значения в соответствии с таблицей 12.2. Рассмотрим вычисление значений формул на интерпретации P_2 , Q_1 .

$$E_1 = \forall yP_2(y) \rightarrow \exists xQ_1(x) = F \rightarrow F = T;$$

$$E_2 = \forall y(P_2(y) \rightarrow \exists xQ_1(x)) = \forall y \left(\frac{P_2(1) \rightarrow \exists xQ_1(x)}{P_2(2) \rightarrow \exists xQ_1(x)} \right) =$$

$$= \forall y \left(\frac{F \rightarrow F = T}{T \rightarrow F = F} \right) = F;$$

$$E_3 = \forall y \exists x(P_2(y) \rightarrow Q_1(x)) = \forall y \left(\frac{\exists x(P_2(1) \rightarrow Q_1(x))}{\exists x(P_2(2) \rightarrow Q_1(x))} \right) =$$

$$= \forall y \left(\frac{\exists x \left(\frac{P_2(1) \rightarrow Q_1(1)}{P_2(1) \rightarrow Q_1(2)} \right)}{\exists x \left(\frac{P_2(2) \rightarrow Q_1(1)}{P_2(2) \rightarrow Q_1(2)} \right)} \right) = \forall y \left(\frac{\exists x \left(\frac{F \rightarrow F = T}{F \rightarrow F = T} \right) = T}{\exists x \left(\frac{T \rightarrow F = F}{T \rightarrow F = F} \right) = F} \right) = F.$$

Истинностные значения E_1 , E_2 , E_3 для восьми интерпретаций приведены в табл. 12.4.

Таблица. 12.4.

$P(\cdot)$	$Q(\cdot)$	E_1	E_2	E_3
P_1	Q_1	T	T	T
P_1	Q_2	T	T	T
P_1	Q_3	T	T	T
P_1	Q_4	T	T	T
P_2	Q_1	T	F	F
P_2	Q_2	T	T	T
P_2	Q_3	T	T	T
P_2	Q_4	T	T	T

Из таблицы видно, что формула E_1 не эквивалентна формулам E_2 и E_3 , а формулы E_2 и E_3 , возможно, эквивалентны, — для окончательного решения нужно рассмотреть оставшиеся интерпретации.

12.4. Логически общезначимые формулы логики предикатов

12.4.1. Основные логически общезначимые формулы логики предикатов

Основные логически общезначимые формулы логики предикатов приведены в таблице 12.5.

Каждая логически общезначимая формула выражает некоторое истинное высказывание относительно свойств объектов. Например, логически общезначимая формула $\exists x(P(x) \& Q(x)) \rightarrow \exists xP(x) \& \exists xQ(x)$ выражает тот факт, что если некоторые объекты обладают сразу двумя свойствами P и Q , то существуют объекты, обладающие свойством P , и объекты, обладающие свойством Q . Так, если существуют юристы-жулики, то существуют люди, которые являются юристами, и существуют жулики. Очевидно, что обратная импликация $\exists xP(x) \& \exists xQ(x) \rightarrow \exists x(P(x) \& Q(x))$ будет истинна далеко не всегда: из того, что существуют юристы и существуют жулики, еще не следует, что существуют юристы-жулики, — эти два множества могут не пересекаться.

Ниже приводятся интерпретации некоторых логически общезначимых формул.

$$\forall xP(x) \rightarrow P(y)$$

Если все люди смертны, то смертен любой человек.

$$P(a) \rightarrow \exists x(P(x))$$

Если кошка a — серая, то существуют серые кошки.

$$\neg \forall xP(x) \equiv \exists x \neg P(x)$$

Не все кошки серые \equiv

$$\neg \exists xP(x) \equiv \forall x \neg P(x)$$

Существуют не серые кошки.

Не существует серых кошек \equiv

Все кошки не серые.

$$\forall x(P(x) \& Q(x)) \equiv \forall xP(x) \& \forall xQ(x)$$

Все кошки с усами и с хвостами \equiv
Каждая кошка имеет усы
и каждая кошка имеет хвост.

$$\exists x(P(x) \vee Q(x)) \equiv \exists xP(x) \vee \exists xQ(x)$$

Некоторые кошки белые или черные \equiv Существует хотя бы одна белая кошка или существует хотя бы одна черная кошка.

Таблица 12.5.

№ п/п	Общезначимые формулы и комментарий
1	2
1	$\forall xP(x) \rightarrow P(y)$ правило универсальной конкретизации;
2	$P(a) \rightarrow \exists x(P(x))$ правило экзистенциального обобщения;
3	$\neg\forall xP(x) \equiv \exists x\neg P(x)$ правило де Моргана
4	$\neg\exists xP(x) \equiv \forall x\neg P(x)$ правило де Моргана
5	$\forall x(P(x) \& Q(x)) \equiv \forall xP(x) \& \forall xQ(x)$ закон пронесения \forall через $\&$
6	$\exists x(P(x) \vee Q(x)) \equiv \exists xP(x) \vee \exists xQ(x)$ закон пронесения \exists через \vee
7	$\forall xP(x) \vee \forall xQ(x) \rightarrow \forall x(P(x) \vee Q(x))$ закон пронесения \forall через \vee
8	$\exists x(P(x) \& Q(x)) \rightarrow \exists xP(x) \& \exists xQ(x)$ закон пронесения \exists через $\&$
9	$(\forall x(P(x) \rightarrow Q(x))) \rightarrow (\forall xP(x) \rightarrow \forall xQ(x))$ закон пронесения \forall через \rightarrow
10	$(\exists xP(x) \rightarrow \exists xQ(x)) \rightarrow \exists x(P(x) \rightarrow Q(x))$ закон пронесения \exists через \rightarrow
11	$\forall x(P(x) \equiv Q(x)) \rightarrow (\forall xP(x) \equiv \forall xQ(x))$ закон пронесения \forall через \equiv
12	$\forall x(P(x) \& B) \equiv \forall xP(x) \& B$ B не содержит вхождений x

Продолжение табл. 12.5.

1	2
13	$\forall x(P(x) \vee B) \equiv \forall xP(x) \vee B$ B не содержит вхождений x
14	$\exists x(P(x) \& B) \equiv \exists xP(x) \& B$ B не содержит вхождений x
15	$\exists x(P(x) \vee B) \equiv \exists xP(x) \vee B$ B не содержит вхождений x
16	$\forall x(P(x) \rightarrow B) \equiv (\exists xP(x) \rightarrow B)$ B не содержит вхождений x
17	$\exists x(P(x) \rightarrow B) \equiv (\forall xP(x) \rightarrow B)$ B не содержит вхождений x
18	$\forall x\forall yP(x, y) \equiv \forall y\forall xP(x, y)$ закон перестановки кванторов \forall
19	$\forall x\forall yP(x, y) \rightarrow \forall xP(x, x)$
20	$\exists x\exists yP(x, y) \equiv \exists y\exists xP(x, y)$ закон перестановки кванторов \exists
21	$\exists xP(x, x) \rightarrow \exists x\exists yP(x, y)$
22	$\exists y\forall xP(x, y) \rightarrow \forall x\exists yP(x, y)$ закон перестановки кванторов \exists и \forall
23	$\forall xP(x) \rightarrow \exists xP(x)$
24	$(\forall xP(x) \rightarrow \exists xQ(x)) \equiv \exists x(P(x) \rightarrow Q(x))$
25	$(\exists xP(x) \rightarrow \forall xQ(x)) \rightarrow \forall x(P(x) \rightarrow Q(x))$
26	$\forall xP(x) \equiv \forall yP(y)$ если y свободно для x в $P(x)$
27	$\exists xP(x) \equiv \exists yP(y)$ если y свободно для x в $P(x)$

$\forall x(P(x) \rightarrow Q(x)) \rightarrow$
 $\rightarrow (\forall xP(x) \rightarrow \forall xQ(x))$

Если все сторожевые собаки злы, то если все собаки – сторожевые, то все они злы. Обратное не всегда верно.

$(\exists xP(x) \rightarrow \exists xQ(x)) \rightarrow$
 $\rightarrow \exists x(P(x) \rightarrow Q(x))$

Если из того, что существуют собаки, следует, что существуют лающие существа, то существуют такие собаки, которые лают. Обратное не всегда верно.

12.4.2. Проверка общезначимости формул логики предикатов

Проверка логической общезначимости формул может быть осуществлена сведением к противоречию, т.е. методом редукции. Предполагаем, что существует такая интерпретация формулы E , на которой она принимает ложное значение, т.е. $|E| = F$, и пробуем найти такую интерпретацию. Если в результате получаем противоречие, это означает, что таких интерпретаций не существует, и, следовательно, формула логически общезначима.

* Примеры.

1. Рассмотрим формулу $\forall x(A(x) \vee B) \equiv \forall xA(x) \vee B$, где B не зависит от x . Предположим, что существует такая интерпретация, на которой формула ложна импликация: $|\forall x(A^*(x) \vee B^*) \rightarrow \forall xA^*(x) \vee B^*| = F$. Это возможно, если $|\forall x(A^*(x) \vee B^*)| = T$, а $|\forall xA^*(x) \vee B^*| = F$. Из последнего равенства следует, что $|B^*| = F$ и $|\forall x(A^*(x))| = F$. Если $|\forall x(A^*(x))| = F$, то существует хотя бы одно значение $x = a$, такое, что $|A^*(a)| = F$. Формула $|\forall x(A^*(x) \vee B^*)| = T$. Но в области интерпретации данной формулы существует значение $x = a$, для которого $|A^*(a)| = F$ и $|B^*| = F$. Возможно, что существует другое значение $x = b$, для которого $|A^*(b)| = T$. Тогда $|\forall x(A^*(x) \vee B^*)| =$

$\forall \left\{ \begin{array}{l} A^*(a) \vee B^* = F \vee F = F \\ A^*(b) \vee B^* = T \vee F = T \end{array} \right\} = F$, что противоречит предположению $|(A^*(x) \vee B^*)| = T$.

Проверим выполнение другой импликации. Предположим, что $|\forall xA^*(x) \vee B^* \rightarrow \forall x(A^*(x) \vee B^*)| = F$. Тогда $|\forall xA^*(x) \vee B^*| = F$, и $|\forall x(A^*(x) \vee B^*)| = T$. Из $|\forall x(A^*(x) \vee B^*)| = F$ следует, что существует такое $x = a$, что $|A^*(a) \vee B^*| = F$. Отсюда следует, что $|A^*(a)| = F$, $|B^*| = F$. Следовательно, в области определения предиката $A(x)$ существует значение $x = a$, при котором предикат $|A^*(a)| = F$, значит, $|\forall xA^*(x)| = F$. Тогда формула $|\forall xA^*(x) \vee B^*| = F$, что противоречит предположению. Следовательно, формула $\forall x(A(x) \vee B) \equiv \forall xA(x) \vee B$ логически общезначима.

2. Докажем, что формула $(\forall xP(x) \rightarrow \forall xQ(x)) \rightarrow \forall x(P(x) \rightarrow Q(x))$ не является логически общезначимой. Предположим, что на некоторой интерпретации $|(\forall xP^*(x) \rightarrow \forall xQ^*(x)) \rightarrow \forall x(P^*(x) \rightarrow Q^*(x))| = F$. Тогда $|(\forall xP^*(x) \rightarrow \forall xQ^*(x))| = T$ и $|\forall x(P^*(x) \rightarrow Q^*(x))| = F$. Из последнего следует, что существует такое $x = a$, что $|P^*(a) \rightarrow Q^*(a)| = F$, откуда $|P^*(a)| = T$, $|Q^*(a)| = F$. Тогда $|\forall xQ^*(x)| = F$, и, возможно, существует такое b , что $|P^*(b)| = F$, тогда $|\forall xP^*(x)| = F$ и $|(\forall xP^*(x) \rightarrow \forall xQ^*(x))| = T$. Следовательно, существует такая интерпретация, на которой формула принимает ложное значение.

12.5. Логическое следование в логике предикатов

12.5.1. Определение логического следования

↪ **Определение 12.10.** Говорят, что формула B логически следует из формулы A , если в любой интерпретации, в которой A принимает истинное значение, B также принимает истинное значение. Обозначение: $A \models B$.

В общем случае формула B является логическим следствием множества формул Γ , если она истинна на всех тех интерпретациях, на которых выполнены (истинны одновременно) все формулы из Γ .

↪ **Определение 12.11.** Говорят, что формула A равносильна, или логически эквивалентна, формуле B , если каждая из них логически влечет другую, т.е. если $A \models B$ и $B \models A$. Обозначение: $A \Leftrightarrow B$.

Из определений следуют утверждения:

1. $A \models B$ тогда и только тогда, когда $\models A \rightarrow B$.
2. $A_1, \dots, A_n \models B$, тогда и только тогда, когда $\models A_1 \& \dots \& A_n \rightarrow B$.
3. $A \Leftrightarrow B$ тогда и только тогда, когда $\models A \equiv B$.
4. Если $A \models B$ и $|A| = T$, то $|B| = T$ в некоторой интерпретации.
5. Если $\Gamma \models B$ и $\forall i(|\Gamma_i| = T)$, то $|B| = T$.

12.5.2. Основные правила вывода логики предикатов

Рассмотрим некоторые логические следования, которые выполнены в логике предикатов. Каждое такое логическое следование задает правило вывода в логике предикатов; некоторые из них будут использованы в формальной теории предикатов.

1. Правило универсальной конкретизации (УК):

$\forall xA(x) \models A(y)$, если y свободно для x в $A(x)$.

Доказательство. Нужно доказать, что если $|\forall xA^*(x)| = T$ в некоторой интерпретации D , то $|A^*(y)| = T$ в той же интерпретации. Допустим $|A^*(y)| = F$. Тогда существует такое $b \in D$, что $|A^*(b)| = F$.

Но по условию формула $|\forall x A^*(x)| = T$ на D , а так как $b \in D$, то $|\forall x A^*(x)| = F$ на D . Это противоречие доказывает теорему. \simeq

2. Правило экзистенциальной конкретизации (ЭК):

$\exists x A(x) \models A(b)$, где $b \in D$.

Доказательство. Допустим, $|\exists x A^*(x)| = T$ в некоторой интерпретации D . Тогда существует такое $b \in D$, что $|A^*(b)| = T$. \simeq

3. Правило экзистенциального обобщения:

$A(y) \models \exists x A(x)$, где x свободно для y в $A(y)$.

Доказательство. Если $|A^*(y)| = T$ в некоторой интерпретации D , то существует $y = b$, $b \in D$, такое что $|A^*(b)| = T$. Следовательно, $|\exists x A^*(x)| = T$ в интерпретации D .

4. Правило всеобщности:

$C \rightarrow A(x) \models C \rightarrow \forall x A(x)$,

если C не содержит свободных вхождений x .

Доказательство. По условию $|C \rightarrow A^*(x)| = T$ в интерпретации D . Это возможно, если

а) $|C| = F$, тогда $|C \rightarrow A^*(x)| = T$ и $|C \rightarrow \forall x A^*(x)| = T$;

б) $|C| = T$, $|C \rightarrow A^*(x)| = T$, следовательно, $|A^*(x)| = T$ в интерпретации D для любого x , значит $|C \rightarrow \forall x A^*(x)| = T$. \simeq

5. Правило существования: $A(x) \rightarrow C \models \exists x A(x) \rightarrow C$,

если C не содержит свободных вхождений x .

Доказательство. $|A^*(x) \rightarrow C| = T$ в некоторой интерпретации D . Допустим $|\exists x A^*(x) \rightarrow C| = F$ в интерпретации D . Тогда $|C| = F$, (C не зависит от x) и $|\exists x A^*(x)| = T$, следовательно, существует $x = b$, такое что $|A^*(b)| = T$ и $|A^*(b) \rightarrow C| = F$, в то время как по условию $|A^*(x) \rightarrow C| = T$. Полученное противоречие доказывает теорему. \simeq

6. Правило обобщения *Gen* (от английского слова Generalization):

если $\Gamma \models A(x)$, то $\Gamma \models \forall x A(x)$, если x не входит свободно ни в одну из формул Γ .

Доказательство. Предположим, выбрана область интерпретации D и произведена замена в A всех свободных переменных на элементы из D , например, $x = b \in D$. Тогда $|A^*(b)| = T$, так как $|\Gamma| = T$ для всякого i . Так как x не входит свободно ни в одну из формул Γ , то в множестве Γ замены x на b не было и, следовательно, для любого $x \in D$, такого что $|A^*(x)| = T$, $\Gamma \models A^*(x)$, следовательно, $\Gamma \models \forall x A^*(x)$. \simeq

12.6. Исчисление предикатов первого порядка

12.6.1. Формальная теория K

Поскольку построение таблиц истинности для любой формулы не представляется возможным для проверки общезначимости

формул теории предикатов, аксиоматический метод необходим для исследования формул, содержащих кванторы. Рассмотрим формальную теорию первого порядка¹ K .

Символами теории K служат те же символы логики предикатов: пропозициональные связки $\rightarrow, \neg, \forall, \exists$, вспомогательные символы $(,)$, множества предметных переменных: x_1, x_2, \dots , предметных постоянных: a_1, a_2, \dots , функциональные символы: $f_i^n, i = 1, \dots, k, n = 0, \dots, m$, предикатные символы: $P_i^n, i = 1, \dots, k, n = 0, \dots, m$. Определения терма, формулы и пропозициональных связок $\&, \vee, \equiv$ остаются в силе для теории первого порядка.

Аксиомы теории K разбиваются на *логические* аксиомы и *собственные*.

Логические аксиомы. Каковы бы ни были формулы A, B, C теории K , следующие формулы являются логическими аксиомами теории K .

A1 $A \rightarrow (B \rightarrow A)$.

A2 $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$.

A3 $(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$.

A4 $\forall x A(x) \rightarrow A(y)$, если y свободно для x в формуле $A(x)$.

A5 $\forall x (A \rightarrow B(x)) \rightarrow (A \rightarrow \forall x B(x))$, если A не содержит свободных вхождений x .

Собственные аксиомы формулируются отдельно для каждой конкретной содержательной предметной области.

Правилами вывода во всякой теории первого порядка являются:

1) *modus ponens* (MP): из A и $A \rightarrow B$ следует B ,

2) правило *обобщения Gen*: из $\Gamma \models A(x)$, следует $\Gamma \models \forall x A(x)$, если x не входит свободно ни в одну из формул Γ .

Теория K , не содержащая собственных аксиом, называется *исчислением предикатов первого порядка*.

Моделью теории первого порядка K называется всякая интерпретация, в которой истинны все аксиомы теории K . Если правила вывода MP и *Gen* применяются к истинным в данной интерпретации формулам, то результатом являются формулы, также истинные в той же интерпретации. Следовательно, всякая теория K истинна во всякой ее модели.

¹ В теориях первого порядка не допускается навешивание кванторов по предикатам или по функциям и не используются предикаты, имеющие в качестве значений своих аргументов другие предикаты. Такие конструкции рассматриваются в теориях предикатов более высоких порядков.

Множество формул, выводимых по правилам вывода из аксиом теории K , является теоремами теории K . Аксиомы $A1, A2, A3$ теории K и правило MP определены в теории L , следовательно, все теоремы теории L включены в множество теорем теории K .

Метатеорема о дедукции в теории K может быть сформулирована в ослабленном виде.

Метатеорема о дедукции. Если существует вывод формулы B из множества гипотез Γ и формулы A : $\Gamma, A \vdash B$, и в этом выводе ни при каком применении правила Gen к формулам, зависящим от A , не связывается квантором никакая свободная переменная формулы A , то $\Gamma \vdash A \rightarrow B$.

Следствие 1. Если существует вывод $\Gamma, A \vdash B$, и в этом выводе ни разу не применялось правило Gen к формулам, зависящим от A , то $\Gamma \vdash A \rightarrow B$.

Следствие 2. Если существует вывод $\Gamma, A \vdash B$, где A — замкнутая формула, то $\Gamma \vdash A \rightarrow B$.

12.6.2. Теория первого порядка с равенством

Рассмотрим теорию первого порядка K , в числе предикатных символов которой содержится предикат равенства $A_1^2(t, s)$, который для сокращения будем обозначать $t = s$, а вместо $\neg A_1^2(t, s)$ соответственно будем писать $t \neq s$.

↪ **Определение 12.12.** Теория K называется теорией первого порядка с равенством, если следующие формулы являются теоремами теории K :

- $A6. \forall x_1 (x_1 = x_1)$ (рефлексивность равенства);
 $A7. (x = y) \rightarrow (A(x, x) \rightarrow A(x, y))$ (подстановочность равенства),

где x, y — предметные переменные, $A(x, x)$ — произвольная формула, $A(x, y)$ получается заменой каких-нибудь (не обязательно всех) свободных вхождений x на y , если y свободно для тех вхождений x , которые заменяются.

Докажем основные теоремы теории первого порядка с равенством.

Теорема 12.1. $\vdash t = t$ для любого терма t .

Доказательство. Из $A6: \vdash \forall x_1 (x_1 = x_1)$ по правилу универсальной конкретизации получаем $\vdash t = t$. ☞

Теорема 12.2. $\vdash x = y \rightarrow y = x$.

Доказательство. Пусть $A(x, x)$ есть $x = x$, $A(x, y)$ есть $y = x$. Тогда:

$\vdash (x = y) \rightarrow (x = x \rightarrow y = x)$ согласно $A7$;

$\vdash x = x$ согласно теореме 12.1;
 $\vdash x = y \rightarrow y = x$ по правилу удаления средней посылки. ☞

Теорема 12.3. $\vdash x = y \rightarrow (y = z \rightarrow x = z)$.

Доказательство. Пусть $A(y, y)$ есть $y = z$, $A(y, x) \rightarrow x = z$. Тогда, заменив x на y и y на x , получим:

$\vdash (y = x) \rightarrow (y = z \rightarrow x = z)$ согласно $A7$;
 $\vdash x = y \rightarrow y = x$ согласно теореме 12.2;
 $\vdash x = y \rightarrow (y = z \rightarrow x = z)$ по правилу силлогизма. ☞

12.7. Доказательство логических следствий в логике предикатов

12.7.1. Формализация предложений естественного языка

Язык логики предикатов традиционно служит для формализации высказываний естественного языка.

✱ **Пример.** Рассмотрим область определения $M = \{\text{люди}\}$ с заданными на ней предикатами: $J(x)$: x — судья; $L(x)$: x — юрист; $S(x)$: x — жулик; $A(x, y)$: x любит y .

Понятие «юрист» можно определить как множество всех людей, имеющих юридическое образование. Понятие «судья» можно определить как множество людей, имеющих юридическое образование, работающих в суде и выполняющих вполне определенные обязанности. Таким образом, множество *судей* является подмножеством множества *юристов*, т.е. свойство *быть судьей* влечет свойство *быть юристом*, и область истинности предиката J включена в область истинности предиката L (см. рис.12.3), т.е. справедливо высказывание: *каждый судья является юристом*, что можно выразить в виде формулы: $\forall x (J(x) \rightarrow L(x))$.



Рис. 12.3. Области определения предикатов.

Рассмотрим высказывание: «Некоторые юристы — жулики». Это высказывание истинно, если существуют такие объекты, которые являются одновременно и юристами, и жуликами: $\exists x (L(x) \& S(x))$, т.е. области истинности предикатов $L(x)$ и $S(x)$ пересекаются: $L \cap S$. Следует ли из этого, что *существуют судьи-жулики*? Нет, не следует.

Области истинности предикатов $J(x)$ и $S(x)$ могут пересекаться (рис. 12.3, б), а могут и не пересекаться (рис. 12.3, а). Мы могли бы сказать: «Возможно, существуют судьи-жулики», – однако категорию *возможности* нельзя выразить в теории предикатов 1-го порядка.

Формализуем некоторые другие высказывания:

$\exists x(S(x) \ \& \ \forall y(L(y) \rightarrow A(x, y)))$	некоторые жулики любят всех юристов;
$\exists x(S(x) \ \& \ \forall y(A(x, y) \rightarrow L(y)))$	некоторые жулики любят только юристов;
$\exists x(S(x) \ \& \ \exists y(L(y) \ \& \ A(x, y)))$	некоторые жулики любят некоторых юристов;
$\forall x(S(x) \rightarrow \forall y(J(y) \rightarrow \neg A(x, y)))$	все жулики не любят судей.

12.7.2. Основные схемы суждений

В традиционной логике обычно выделяют четыре основных схемы суждений.

1). Общеутвердительное суждение: A : Все S суть P : $\forall x(S(x) \rightarrow P(x))$.

✱ **Пример.** В последующих примерах пусть $x \in \{\text{люди}\}$, $y \in \{\text{произведения}\}$. На этих областях заданы предикаты: $P(x)$: x – писатель, $V(x)$: x – поэт, $W(x, y)$: x пишет y , $N(y)$: y – роман, $K(y)$: y – конспект, $C(y)$: y – стихи, $U(y)$: y – учебник. Рассмотрим два понятия: «учебники» и «конспекты». Понятие «учебники» обладает тем свойством, что это книги, по которым учатся. Предикат $U(x)$ среди всех книг выделяет те, которые являются учебниками. По конспектам также учатся, однако, конспекты обладают еще и тем свойством, что они написаны от руки. Поэтому конспекты можно считать подмножеством учебников (см. рис. 12.4). Отсюда следует, что «каждый конспект является учебником», или «все конспекты – учебники», что выражается формулой: $\forall x(K(x) \rightarrow U(x))$.

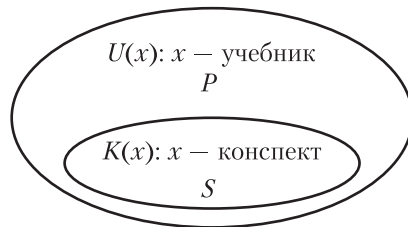


Рис. 12.4. $\forall x(K(x) \rightarrow U(x))$ – Все конспекты – учебники.

2). Общеотрицательное суждение: E : Ни одно S не суть P : $\forall x(S(x) \rightarrow \neg P(x))$.

✱ **Пример.** Рассмотрим два понятия: «конспекты» и «романы». Очевидно, что области истинности этих предикатов не пересекаются (см. рис. 12.5), т.е. «ни один конспект не является романом», что выражается формулой: $\forall x(K(x) \rightarrow \neg N(x))$.



Рис. 12.5. $\forall x(K(x) \rightarrow \neg N(x))$ – Ни один конспект не является романом.

3). Частноутвердительное суждение: I : Некоторые S суть P – $\exists x(S(x) \ \& \ P(x))$.

✱ **Пример.** Понятия «романы» и «стихи» имеют пересекающиеся объемы (рис. 12.6), – как известно, существуют романы в стихах, например, «Евгений Онегин». Утверждение «некоторые романы написаны в стихах» выражается формулой: $\exists x(N(x) \ \& \ C(x))$.

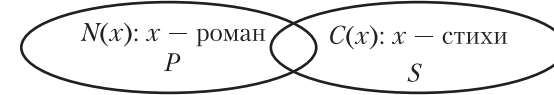


Рис. 12.6. $\exists x(N(x) \ \& \ C(x))$ – Некоторые романы – стихи.

4). Частноотрицательное суждение: O : Некоторые S не суть P : $\exists x(S(x) \ \& \ \neg P(x))$.

✱ **Пример.** Рассмотрим утверждения: «некоторые романы – не стихи»: $\exists x(N(x) \ \& \ \neg C(x))$, «некоторые конспекты – не романы»: $\exists x(K(x) \ \& \ \neg N(x))$. Области истинности соответствующих предикатов могут пересекаться, а могут и не пересекаться (см. рис. 12.7).

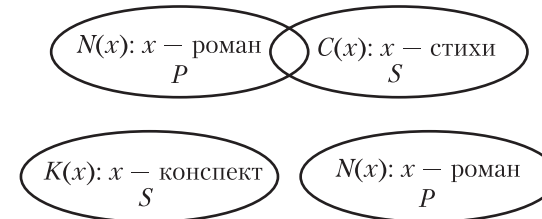
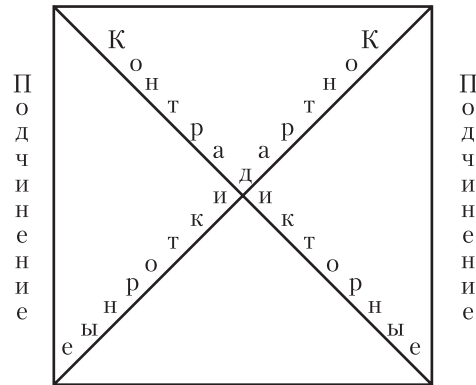


Рис. 12.7. $\exists x(N(x) \ \& \ \neg C(x))$ – Некоторые романы – не стихи;
 $\exists x(K(x) \ \& \ \neg N(x))$ – Некоторые конспекты – не романы.

Эти четыре типа суждений образуют так называемый *логический квадрат*, который показывает связь между схемами суждений (рис. 12.8).

A — Все S суть P E — Ни одно S не суть P
Контрарные



Субконтрарные
 I — Некоторые S суть P O — Некоторые S не суть P
Рис. 12.8. Логический квадрат.

Суждения, соединенные диагоналями, называются *контрадикторными*. *Контрадикторные* утверждения несовместимы по истинности и несовместимы по ложности, т.е. не могут быть одновременно истинными, и не могут быть одновременно ложными. Одно является отрицанием другого:

1) $\neg A = O$, т.е. «не все S суть P » \equiv «некоторые S не суть P ». Действительно: $\neg \forall x(S(x) \rightarrow P(x)) \equiv \exists x \neg (S(x) \rightarrow P(x)) \equiv \exists x(S(x) \wedge \neg P(x))$. Например, $\forall x(N(x) \rightarrow C(x))$ («все романы написаны в стихах») и $\exists x(N(x) \wedge \neg C(x))$ («некоторые романы — не стихи») — контрадикторные утверждения, одно является отрицанием другого.

2) $\neg E = I$, т.е. «неверно, что ни одно S не суть P » \equiv «некоторые S суть P ».

$\neg \forall x(S(x) \rightarrow \neg P(x)) \equiv \exists x \neg (S(x) \rightarrow \neg P(x)) \equiv \exists x(S(x) \wedge P(x))$.

Горизонтальные стороны квадрата показывают отношения контрарности и субконтрарности. Утверждения A : Все S суть P : $\forall x(S(x) \rightarrow P(x))$ и E : Ни одно S не суть P : $\forall x(S(x) \rightarrow \neg P(x))$ называются *контрарными*. Они совместимы по ложности, но несовместимы по истинности, т.е. могут быть одновременно ложными, но не могут быть одновременно истинными. Например, «все романы написаны в стихах»: $\forall x(N(x) \rightarrow C(x))$ и «ни один роман не написан в стихах»: $\forall x(N(x) \rightarrow \neg C(x))$, — контрарные утверждения; оба они ложны. Утверждения: «все люди смертны» и «все люди бессмертны», — также контрарны, первое — истинно, второе ложно.

Утверждения I : Некоторые S суть P : $\exists x(S(x) \wedge P(x))$ и O : Некоторые S не суть P : $\exists x(S(x) \wedge \neg P(x))$ называются *субконтрарными*. Субконтрарные утверждения совместимы по истинности, но несовместимы по ложности, т.е. могут быть одновременно истинными, но не могут быть одновременно ложными. Например, «некоторые романы — стихи»: $\exists x(N(x) \wedge C(x))$ и «некоторые романы не стихи»: $\exists x(N(x) \wedge \neg C(x))$, — субконтрарны; оба они истинны.

Вертикальные стороны квадрата показывают отношение логического следования (в логическом квадрате — отношение подчинения): утверждения, находящиеся снизу, логически следуют из тех, что находятся сверху. Действительно, если «все S суть P », то и «некоторые S суть P », т.е. выполнено логическое следование: $\forall x(S(x) \rightarrow P(x)) \models \exists x(S(x) \wedge P(x))$, откуда следует, что $|A \rightarrow I| \equiv T$. Например, если «все конспекты — учебники», то и «некоторые конспекты — учебники». Другое логическое следование также очевидно: если «ни одно S не суть P », то и «некоторые S не суть P »: $\forall x(S(x) \rightarrow \neg P(x)) \models \exists x(S(x) \wedge \neg P(x))$, откуда следует, что $|E \rightarrow O| \equiv T$. Например, если «ни один учебник не написан в стихах», то и «некоторые учебники не написаны в стихах».

Другие примеры формализации высказываний приведены в таблице 12.6.

Таблица 12.6.

Все конспекты — учебники.	$\forall y(K(y) \rightarrow U(y))$
Конспект по математике (М) — учебник.	$K(M) \rightarrow U(M)$
Ни один учебник не написан в стихах.	$\forall y(U(y) \rightarrow \neg C(y))$
Некоторые романы написаны в стихах.	$\exists y(N(y) \wedge C(y))$
«Евгений Онегин» — это роман в стихах.	$N(E.Онегин.) \wedge C(E.Онегин.)$
Все поэты пишут стихи.	$\forall x(V(x) \rightarrow \forall y(C(y) \rightarrow W(x,y)))$
Некоторые писатели пишут только романы.	$\exists x(P(x) \wedge \forall y(W(x,y) \rightarrow N(y)))$
Писатель Лев Толстой писал только романы.	$P(\text{Толстой}) \wedge \forall y(W(\text{Толстой}, y) \rightarrow N(y))$
Каждый что-нибудь пишет.	$\forall x \exists y W(x,y)$
Каждый, кто пишет что-нибудь, пишет поздравление с Новым годом (NY).	$\forall x(\exists y W(x,y) \rightarrow W(x, NY))$
Некоторые люди ничего не пишут.	$\exists x \forall y \neg W(x,y)$

12.7.3. Доказательство логических следований

В данном разделе мы рассмотрим два способа доказательства логических следований: неформальный способ, основанный на доказательстве от противного, и формальный вывод в исчислении предикатов. В следующей главе будет рассмотрен более эффективный метод, позволяющий автоматизировать процесс доказательства логического следования (логической общезначимости).

★ **Пример 12.1.** На области определения «люди» заданы высказывания:

1. Некоторые студенты любят своих преподавателей.
2. Никто не любит невежественных людей.

Следовательно, ни один преподаватель не является невежественным.

Пусть $P(x)$: x — студент, $D(x)$: x — преподаватель, $Q(x)$: x — невежественный, $L(x, y)$: x любит y . Формализуем посылки:

$$F1: \exists x(P(x) \ \& \ \forall y(D(y) \rightarrow L(x, y))),$$

$$F2: \forall x(P(x) \rightarrow \forall y(Q(y) \rightarrow \neg L(x, y))).$$

$$\text{Закключение } G: \forall y(D(y) \rightarrow \neg Q(y)).$$

По определению, $|F1| = T$, $|F2| = T$. Предположим, что $|G| = F$.

Из предположения $|\forall y(D(y) \rightarrow \neg Q(y))| = F$ следует, что существует по крайней мере одно значение $y = a$, такое что $|D(a) \rightarrow \neg Q(a)| = F$, откуда получаем, что $|D(a)| = T$, $|\neg Q(a)| = F$, т.е. $|Q(a)| = T$.

Из посылки $F1$: $|\exists x(P(x) \ \& \ \forall y(D(y) \rightarrow L(x, y)))| = T$ следует, что существует по крайней мере одно значение $x = b$, такое, что $|P(b) \ \& \ \forall y(D(y) \rightarrow L(b, y))| = T$, откуда получаем: $|P(b)| = T$ и $|\forall y(D(y) \rightarrow L(b, y))| = T$. Поскольку последнее истинно для всякого y , в том числе, для $y = a$, получаем $|D(a) \rightarrow L(b, a)| = T$, т.е. $|(T \rightarrow L(b, a))| = T$, откуда $|L(b, a)| = T$.

Поскольку посылка $F2$: $|\forall x(P(x) \rightarrow \forall y(Q(y) \rightarrow \neg L(x, y)))| = T$ для всех значений x и y , то она истинна и для $x = b$, $y = a$: $|P(b) \rightarrow (Q(a) \rightarrow \neg L(b, a))| = T$. А поскольку $|P(b)| = T$, то $|Q(a) \rightarrow \neg L(b, a)| = T$. Так как $|Q(a)| = T$, то $|\neg L(b, a)| = T$. Получаем, что истинны оба утверждения: $|L(b, a)| = T$ и $|\neg L(b, a)| = T$. Полученное противоречие доказывает логическое следование.

В формальном выводе применяются правила: универсальной конкретизации (УК), экзистенциальной конкретизации (ЭК), удаления & (уд. &), введения & (вв. &), правило МР.

Формальный вывод.

- | | |
|---|----------|
| 1. $\exists x(P(x) \ \& \ \forall y(D(y) \rightarrow L(x, y)))$ | Г1 |
| 2. $\forall x(P(x) \rightarrow \forall y(Q(y) \rightarrow \neg L(x, y)))$ | Г2 |
| 3. $P(b) \ \& \ \forall y(D(y) \rightarrow L(b, y))$ | ЭК(1) |
| 4. $P(b)$ | уд. &(3) |

- | | |
|--|----------------------------|
| 5. $\forall y(D(y) \rightarrow L(b, y))$ | уд. &(3) |
| 6. $P(b) \rightarrow \forall y(Q(y) \rightarrow \neg L(b, y))$ | УК(2) |
| 7. $\forall y(Q(y) \rightarrow \neg L(b, y))$ | МР(4, 6) |
| 8. $Q(z) \rightarrow \neg L(b, z)$ | УК(7) |
| 9. $D(z) \rightarrow L(b, z)$ | УК(5) |
| 10. $L(b, z) \rightarrow \neg Q(z)$ | правило контрапозиции (8) |
| 11. $D(z) \rightarrow \neg Q(z)$ | правило силлогизма (9, 10) |
| 12. $\forall y(D(y) \rightarrow \neg Q(y))$ | Gen (11) |

★ **Пример 12.2.** На области определения «люди» заданы высказывания:

1. Все старые члены конгресса — юристы.
2. Все женщины-юристы восхищаются каким-нибудь судьей.
3. Только судьи восхищаются судьями.
4. Все судьи восхищаются всеми судьями.

Что думает судья Джонс по поводу своей старой тещи, которая является членом конгресса? Ответ: Джонс восхищается своей тещей. Проверить, что это заключение логически следует из заданных посылок.

Пусть x — предметная переменная, которая принимает значения из области определения «люди». Введем предикаты: $J(x)$: x — судья; $L(x)$: x — юрист; $C(x)$: x — член конгресса; $W(x)$: x — женщина; $A(x, y)$: x восхищается y , D — Джонс, T — теща. Формализуем посылки.

1. $\forall x(O(x) \ \& \ C(x) \rightarrow L(x))$
Все старые члены конгресса — юристы.
2. $\forall x(W(x) \ \& \ L(x) \rightarrow \exists y(J(y) \ \& \ A(x, y)))$
Все женщины-юристы восхищаются каким-нибудь судьей.
3. $\forall x \forall y(J(y) \ \& \ A(x, y) \rightarrow J(x))$
Только судьи восхищаются судьями.
4. $\forall x(J(x) \rightarrow \forall y(J(y) \rightarrow A(x, y)))$
Все судьи восхищаются всеми судьями.
5. $J(D)$

Джонс — судья,

6. $W(T) \ \& \ O(T) \ \& \ C(T)$

старая теща, член конгресса.

Доказать: $A(D, T)$ — судья Джонс восхищается тещей.

Формальный вывод.

- | | |
|---|----|
| 1. $\forall x(O(x) \ \& \ C(x) \rightarrow L(x))$ | Г1 |
| 2. $\forall x(W(x) \ \& \ L(x) \rightarrow \forall y(J(y) \ \& \ A(x, y)))$ | Г2 |
| 3. $\forall x \forall y(J(y) \ \& \ A(x, y) \rightarrow J(x))$ | Г3 |

4. $\forall x(J(x) \rightarrow \forall y(J(y) \rightarrow A(x, y)))$	Г4
5. $W(T) \& O(T) \& C(T)$	Г5
6. $J(D)$	Г6
7. $J(D) \rightarrow \forall y(J(y) \rightarrow A(D, y))$	УК (4)
8. $\forall y(J(y) \rightarrow A(D, y))$	МР (6,7)
9. $J(T) \rightarrow A(D, T)$	УК (8)
10. $O(T) \& C(T) \rightarrow L(T)$	УК (1)
11. $O(T) \& C(T)$	уд. & (5)
12. $L(T)$	МР (11,10)
13. $L(T) \rightarrow \exists y(J(y) \& A(T, y))$	УК (2)
14. $W(T)$	уд. & (5)
15. $W(T) \& L(T)$	вв. & (12,14)
16. $\exists y(J(y) \& A(T, y))$	МР(13,15)
17. $J(a) \& A(T, a)$	ЭК (16)
18. $J(a) \& A(T, a) \rightarrow J(T)$	УК (3)
19. $J(T)$	МР(18, 17)
20. $A(D, T)$	МР(9, 19)

Глава 13.

АВТОМАТИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМ

13.1. Введение

Поиск общей разрешающей процедуры для проверки общезначимости формул был начат давно. Первым пытался найти такую процедуру Лейбниц (1646—1716), в дальнейшем над этим работала школа Гильберта. Эти попытки продолжались до тех пор, пока Чёрч и Тьюринг независимо друг от друга не доказали, что не существует никакой общей разрешающей процедуры, никакого алгоритма, проверяющего общезначимость формул в логике предикатов первого порядка. Тем не менее, существуют алгоритмы *поиска* доказательства, которые могут подтвердить, что формула общезначима. Для необщезначимых формул эти алгоритмы, вообще говоря, не заканчивают свою работу. Принимая во внимание результат Чёрча и Тьюринга, это лучшее, что можно ожидать от алгоритма поиска доказательства.

В 1930 г. важный подход к автоматическому доказательству теорем был дан Эрбраном. По определению общезначимая формула есть формула, которая истинна при всех интерпретациях. Эрбран разработал алгоритм нахождения интерпретации, которая опровергает данную формулу. Однако, если данная формула на самом деле общезначима, то такой интерпретации не существует и алгоритм оканчивает работу за конечное число шагов. Метод Эрбрана служит основой для большинства современных методов автоматического поиска доказательства. Главный результат был получен Робинсоном, который ввел так называемый *метод резолюций*.

В основе метода резолюций лежит процедура поиска опровержения, т. е. вместо доказательства общезначимости формулы доказывается, что отрицание формулы противоречиво. Метод опровержения для доказательства логического следования заключается в следующем. Пусть выполняется логическое следование: $F1, F2 \models G$. Тогда $\models F1 \& F2 \rightarrow G$ логически общезначима, и, следовательно, $\models (F1 \& F2 \rightarrow G) \equiv F1 \& F2 \& \neg G \equiv F$. Поскольку по определению посылки $F1, F2$ истинны, формула $F1 \& F2 \& \neg G$ может обратиться в ложь только, если $\models \neg G = F$, т.е. если $\models G = T$. Тогда логическое следствие выполнено. В принципе процедура опровержения формализует метод редукции. Проблема поиска автоматического доказательства при использовании процедуры опровержения значительно облегчается благодаря использованию так называемых «стандартных» форм формул. Любую формулу логики предикатов можно привести к эквивалентной ей предваренной нормальной форме,

когда все кванторы вынесены вперед, а в области действия кванторов формула находится в конъюнктивной нормальной форме. Если такая формула имеет только кванторы всеобщности, то она будет ложна, если найдется хотя бы одна интерпретация, которая обращает ее в ложь. Тогда эквивалентная ей исходная формула также будет ложна, а ее отрицание, соответственно, истинно. Если же среди кванторов имеются кванторы существования, то проблема усложняется. Однако, кванторы существования можно снять (на основании правила экзистенциальной конкретизации), в результате будет получена так называемая «скулемовская стандартная форма». Тогда поиск опровергающей интерпретации применяется к этой форме.

13.2. Предваренные нормальные формы

↪ **Определение 13.1.** Формула A находится в *предваренной нормальной форме* (ПНФ), если она имеет вид: $(Q_1x_1)...(Q_nx_n)M$, где каждое Q_ix_i есть $\exists x_i$ или $\forall x_i$, а M — формула в конъюнктивной нормальной форме, не содержащая кванторов. $(Q_1x_1)...(Q_nx_n)$ называется *префиксом*, а M — *матрицей* формулы A .

Теорема 13.1. Существует эффективная процедура приведения любой формулы логики предикатов к эквивалентной ей предваренной нормальной форме.

Доказательство теоремы конструктивно, т.е. дает алгоритм преобразования любой формулы к предваренной нормальной форме. Теорема доказывается индукцией по числу связок m .

1. Пусть $m = 0$. Тогда формула A не содержит связок и находится в ПНФ.

2. Предположим, что существует ПНФ для формулы B с числом связок n . Докажем, что существует ПНФ для формулы A с числом связок $m = n + 1$.

1 *случай.* Пусть существует ПНФ для $B = (Q_1x_1)...(Q_nx_n)M$. Формула A образована из B с помощью операции отрицания: $A = \neg(Q_1x_1)...(Q_nx_n)M$. По законам де Моргана связка \neg проносится через кванторы: $\neg\forall xM \equiv \exists x\neg M$, $\neg\exists xM \equiv \forall x\neg M$. Полученная формула будет находиться в ПНФ.

2 *случай.* Формула A образована из двух формул B_1 и B_2 с числом связок $n < m$ с помощью связок конъюнкции $\&$ или дизъюнкции \vee : $(Q_1x_1) \dots (Q_nx_n) M_1 \& (Q_1y_1) \dots (Q_ny_n) M_2$ или $(Q_1x_1) \dots (Q_nx_n) M_1 \vee (Q_1y_1) \dots (Q_ny_n) M_2$. Тогда, если формулы B_1 и B_2 имеют кванторы по одной и той же переменной, используем законы замены связанных переменных:

$$\forall xP(x) \equiv \forall yP(y), \exists xP(x) \equiv \exists yP(y),$$

так, чтобы ни одна свободная переменная не стала связанной в результате этой замены. После этого воспользуемся законами коммутативности для $\&$ и \vee и законами пронесения кванторов:

$$\forall x(P(x) \& B) \equiv \forall xP(x) \& B, \forall x(P(x) \vee B) \equiv \forall xP(x) \vee B,$$

$$\exists x(P(x) \& B) \equiv \exists xP(x) \& B, \exists x(P(x) \vee B) \equiv \exists xP(x) \vee B,$$

(B не содержит вхождений x).

3 *случай.* Формула A образована из B навешиванием квантора \forall или \exists . Тогда, поскольку B находится в ПНФ, вновь полученная формула будет в ПНФ.

✱ **Примеры.**

1. Приведем к ПНФ следующую формулу:

$$\begin{aligned} \exists xP(x) \rightarrow \forall x(\exists yD(y) \& L(x, y)) &= \neg\exists xP(x) \vee \forall x(\exists yD(y) \& L(x, y)) = \\ &= \forall x\neg P(x) \vee \forall x(\exists yD(y) \& L(x, y)) = \forall x\neg P(x) \vee \forall z(\exists yD(y) \& L(z, y)) = \\ &= \forall x(\neg P(x) \vee \forall z(\exists yD(y) \& L(z, y))) = \\ &= \forall x(\forall z(\exists yD(y) \& L(z, y)) \vee \neg P(x)) = \\ &= \forall x\forall z(\exists vD(v) \& L(z, y)) \vee \neg P(x) = \\ &= \forall x\forall z\exists v((D(v) \& L(z, y)) \vee \neg P(x)) = \\ &= \forall x\forall z\exists v((D(v) \vee \neg P(x)) \& (L(z, y) \vee \neg P(x))). \end{aligned}$$

2. Рассмотрим посылки примера 12.1.

$$\begin{aligned} \exists x(P(x) \& \forall y(D(y) \rightarrow L(x, y))) &= \exists x(P(x) \& \forall y(\neg D(y) \vee L(x, y))) = \\ &= \exists x(\forall y(\neg D(y) \vee L(x, y)) \& P(x)) = \\ &= \exists x\forall y((\neg D(y) \vee L(x, y)) \& P(x)). \\ \forall x(P(x) \rightarrow \forall y(Q(y) \rightarrow \neg L(x, y))) &= \forall x(\neg P(x) \vee \forall y(\neg Q(y) \vee \neg L(x, y))) = \\ &= \forall x(\forall y(\neg Q(y) \vee \neg L(x, y)) \vee \neg P(x)) = \\ &= \forall x\forall y(\neg Q(y) \vee \neg L(x, y) \vee \neg P(x)). \end{aligned}$$

13.3. Скулемовские стандартные формы

↪ **Определение 13.2.** Предваренная нормальная форма, содержащая только кванторы всеобщности, называется *скулемовской стандартной формой* (ССФ).

Процедура приведения ПНФ к скулемовской форме заключается в элиминации (удалении) кванторов существования.

Пусть формула A находится в предваренной нормальной форме $(Q_1x_1)...(Q_nx_n)M$, где M есть *конъюнктивная нормальная форма*. Если квантор существования — первый слева квантор в префиксе: $(\exists x_1)(Q_2x_2)...(Q_nx_n)M$, то его можно элиминировать на основании правила экзистенциальной конкретизации. Выберем константу c , отличную от других констант, входящих в M , заменим все вхождения x_1 , встречающиеся в M , на c , и вычеркнем квантор $\exists x_1$ из префикса.

Если же перед квантором существования стоит квантор всеобщности, например, $\forall x \exists y M$, то переменная y попадает в область действия квантора всеобщности, и выражение $\forall x \exists y$ (для каждого x существует y) означает наличие некоторой функциональной зависимости $y = f(x)$. Если квантору существования предшествует несколько кванторов всеобщности, то функция зависит от всех переменных, по которым навешены эти кванторы. В общем случае, если Qs_1, \dots, Qs_m — список всех кванторов всеобщности, встречающихся левее $\exists x$, $1 \leq s_1 < s_2 < \dots < s_m < r$, мы выберем m -местный функциональный символ f , отличный от других функциональных символов, заменим все x_i в M на $f(x_{s_1}, \dots, x_{s_m})$ и вычеркнем $\exists x_r$ из префикса. Затем весь этот процесс применим для всех кванторов существования в префиксе; последняя из полученных формул есть *скулемовская стандартная форма* — для краткости, *стандартная форма* (ССФ) формулы A . Функции, используемые для замены переменных квантора существования, называются *скулемовскими функциями* (константы есть нульместные функции).

*** Пример.** Получим стандартную форму формулы $A = \exists x \forall y \forall z \exists u \forall v \exists w P(x, y, z, u, v, w)$. В этой формуле левее $\exists x$ нет никаких кванторов всеобщности, левее $\exists u$ стоят $\forall y$ и $\forall z$, а левее $\exists w$ стоят $\forall y$, $\forall z$ и $\forall v$. Следовательно, мы заменим переменную x на константу a , переменную u — на двуместную функцию $f(y, z)$, переменную w — на трехместную функцию $g(y, z, v)$. Таким образом, мы получаем следующую стандартную форму формулы A : $S = \forall y \forall z \forall v P(a, y, z, f(y, z), v, g(y, z, v))$.

Для рассмотренных выше посылок из примера 12.1 ССФ имеет вид:
 $\exists x \forall y ((\neg D(y) \vee L(x, y)) \& P(x)) \Rightarrow \forall y ((\neg D(y) \vee L(a, y)) \& P(a)),$
 $\forall x \forall y (\neg Q(y) \vee \neg L(x, y) \vee \neg P(x)).$

Если предваренная нормальная форма эквивалентна исходной формуле, то скулемовская стандартная форма формулы A , вообще говоря, не эквивалентна ей. Например, пусть $A = \exists x P(x)$ и $S = P(a)$ есть стандартная форма формулы A . Пусть I есть следующая интерпретация: область $D = \{a, b\}$, $P(a) = F$, $P(b) = T$. Тогда A истинна в I , но S ложна в I . Таким образом, A не эквивалентна S . Однако, если $P(a) = F$, $P(b) = F$, то $|A| = F$, и $S = P(a)$ также принимает значение F для любого a . Таким образом, $A \equiv S$ в том и только том случае, если A противоречива. Докажем, что это действительно так.

Теорема 13.2. Пусть S — стандартная форма формулы A . Тогда A противоречива в том и только том случае, когда S противоречива.

Доказательство. Пусть формула A находится в ПНФ, т.е. $A = (Q_1 x_1) \dots (Q_n x_n) M[x_1, \dots, x_n]$. (Запись $M[x_1, \dots, x_n]$ означает, что матрица M содержит переменные x_1, \dots, x_n). Пусть Q_r — первый слева квантор существования. Пусть $A_1 = (\forall x_1) \dots (\forall x_{r-1}) (Q_{r+1} x_{r+1}) \dots (Q_n x_n) M[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n]$, где f — скулемовская функция, соответствующая x_r , $1 \leq r \leq n$. Мы хотим показать, что A противоречива тогда и только тогда, когда A_1 противоречива. Предположим, что A противоречива. Если A_1 непротиворечива, то существует такая интерпретация I , что A_1 истинна в I , т.е. для всех x_1, \dots, x_{r-1} существует по крайней мере один элемент $f(x_1, \dots, x_{r-1})$, для которого $(Q_{r+1} x_{r+1}) \dots (Q_n x_n) M[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n]$ истинна в I . Таким образом, A истинна в I , что противоречит предположению, что A противоречива. Следовательно, A_1 должна быть противоречива. С другой стороны, предположим, что A_1 противоречива. Если A непротиворечива, то существует такая интерпретация I на области D , что A истинна в I , т.е. для всех x_1, \dots, x_{r-1} существует такой элемент x_r , что $(Q_{r+1} x_{r+1}) \dots (Q_n x_n) M[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n]$ истинна в I . Расширим интерпретацию I , включив в нее функцию $f(x_1, \dots, x_{r-1}) = x_r$, которая отображает (x_1, \dots, x_{r-1}) на x_r для всех x_1, \dots, x_{r-1} в D . Обозначим это расширение I' . Тогда для всех x_1, \dots, x_{r-1} $(Q_{r+1} x_{r+1}) \dots (Q_n x_n) M[x_1, \dots, x_{r-1}, f(x_1, \dots, x_{r-1}), x_{r+1}, \dots, x_n]$ истинна в I' , т.е. A_1 истинна в I' , что противоречит предположению, что A_1 противоречива. Следовательно, A должна быть противоречивой. Предположим теперь, что в A имеется m кванторов существования. Пусть $A_0 = A$. Пусть A_k получается из A_{k-1} заменой первого квантора существования в A_{k-1} скулемовской функцией, $k = 1, \dots, m$. Тогда стандартная форма $S = A_m$. Используя те же рассуждения, что были даны выше, мы можем показать, что A_{k-1} противоречива тогда и только тогда, когда A_k противоречива при $k = 1, \dots, m$. Следовательно, A противоречива тогда и только тогда, когда S противоречива, что и требовалось доказать. \bowtie

Определение 13.3. Предикатные буквы будем называть литерами. Дизъюнкция литер называется *дизъюнктом*, или *клаузой* (*clause*) (иногда — *клизом*). Однолитерный дизъюнкт называется *единичным дизъюнктом*. Когда дизъюнкт не содержит никаких литер, его называют *пустым дизъюнктом*. Так как пустой дизъюнкт не содержит литер, которые могли бы быть истинными при любых интерпретациях, то пустой дизъюнкт всегда ложен. Пустой дизъюнкт обозначается символом \square .

Пусть S — стандартная форма формулы A . Матрица формулы, представленной в ССФ, находится в конъюнктивной нормальной форме, т.е. в виде конъюнкции дизъюнктов. Будем представлять ССФ формулы A множеством дизъюнктов, где каждая переменная

считается управляемой квантором всеобщности. Множество дизъюнктов — это просто другая форма представления стандартной формы формулы A , поэтому в дальнейшем будем обозначать его так же, как и ССФ — символом S . Считаем, что множество дизъюнктов S есть конъюнкция всех дизъюнктов из S . Например, ССФ посылки из примера 12.1: $\forall y((\neg D(y) \vee L(a, y)) \& P(a))$ может быть представлена множеством дизъюнктов: $S = \{\neg D(y) \vee L(a, y), P(a)\}$.

Далее, если мы имеем $A = A_1 \& \dots \& A_n$, мы можем отдельно получить множества дизъюнктов S_i , $i = 1, \dots, n$, где каждое S_i представляет стандартную форму A_i . Затем пусть $S = S_1 \cup \dots \cup S_n$. Тогда A противоречива тогда и только тогда, когда S противоречиво. Говорят, что множество дизъюнктов *невыполнимо*, если соответствующая стандартная форма противоречива, и *выполнимо* в противном случае.

13.4. Эрбрановский универсум множества дизъюнктов

По определению, множество дизъюнктов невыполнимо тогда и только тогда, когда оно ложно при всех интерпретациях на всех областях. Так как невозможно рассматривать все интерпретации на всех областях, было бы удобно, если бы мы могли фиксировать одну такую специальную область H , что S невыполнимо тогда и только тогда, когда S ложно при всех интерпретациях на этой области. Эрбран показал, что такая область существует. Ее называют *эрбрановским универсумом* множества *дизъюнктов* S и определяют следующим образом.

↪ **Определение 13.4.** Пусть H_0 — множество констант, встречающихся в S . Если никакая константа не встречается в S , то H_0 состоит из одной произвольной константы, например, $H_0 = \{a\}$. Для $i = 1, 2, \dots$ пусть H_{i+1} есть объединение H_i и множества всех термов вида $f^n(t_1, \dots, t_n)$ (при всех n) для всех функций f^n , встречающихся в S , где t_j ($j = 1, \dots, n$) принадлежит H_i . Тогда каждое H_i называется *множеством констант* i -го уровня для S и H_∞ называется *эрбрановским универсумом* для S .

★ Примеры.

1. Пусть $S_1 = \{P(a), \neg P(x) \vee P(f(x))\}$. Тогда

$$H_0 = \{a\};$$

$$H_1 = \{a, f(a)\};$$

$$H_2 = \{a, f(a), f(f(a))\};$$

$$\dots\dots\dots$$

$$H_\infty = \{a, f(a), f(f(a)), f(f(f(a))), \dots\}.$$

2. Пусть $S_2 = \{P(x) \vee Q(x), \neg R(z), R(y) \vee \neg Q(y)\}$. Так как не существует никаких констант в S , положим $H_0 = \{a\}$. Поскольку не существует никаких функциональных символов в S , то $H = H_0 = H_1 = \dots = \{a\}$.

↪ **Определение 13.5.** Пусть S есть множество дизъюнктов. Тогда множество атомов вида $P^n(t_1, \dots, t_n)$ для всех n -местных предикатов P^n , встречающихся в S , где t_1, \dots, t_n — элементы эрбрановского универсума S , называется *множеством атомов множества* S , или *эрбрановским базисом* S .

★ **Пример.** Эрбрановский базис множества дизъюнктов $S_1 = \{P(a), \neg P(x) \vee P(f(x))\}$:

$$A = \{P(a), P(f(a)), P(f(f(a))), P(f(f(f(a)))), \dots\}.$$

Эрбрановский базис множества дизъюнктов $S_2 = \{P(x) \vee Q(x), R(z) \vee \neg Q(x)\}$:

$$A = \{P(a), Q(a), R(a)\}.$$

↪ **Определение 13.6.** Основной пример дизъюнкта C множества дизъюнктов S есть дизъюнкт, полученный заменой переменных в C на элементы эрбрановского универсума S .

★ **Пример.** Пусть $S = \{P(x), Q(f(y)) \vee R(y)\}$, $C = P(x)$ — дизъюнкт в S и $H = \{a, f(a), f(f(a)), \dots\}$ — эрбрановский универсум S . Тогда $P(a), P(f(a)), P(f(f(a)))$ есть основные примеры S .

↪ **Определение 13.7.** Пусть S — множество дизъюнктов, H — эрбрановский универсум S и I — интерпретация S над H . Говорят, что I есть *H -интерпретация множества* S , если она удовлетворяет следующим условиям:

1. I отображает все константы из S в самих себя;

2. пусть f есть n -местный функциональный символ и h_1, \dots, h_n — элементы H . В I через f обозначается функция, которая отображает (h_1, \dots, h_n) (элемент из H^n) в $f(h_1, \dots, h_n)$ (элемент из H).

При этом не возникает никаких ограничений при придании значения любому n -местному предикатному символу в S . Пусть $A = \{A_1, A_2, \dots, A_n, \dots\}$ — эрбрановский базис множества S . H -интерпретацию I удобно представлять в виде: $I = \{m_1, m_2, \dots, m_n, \dots\}$, где m_j есть A_j или $\neg A_j$ для $j = 1, 2, \dots$. Смысл этого множества в том, что если m_j есть A_j , то атому A_j присвоено значение «истинно», в противном случае — значение «ложно».

★ **Пример.** Рассмотрим множество $S = \{P(x) \vee Q(x), R(f(y))\}$. Эрбрановский универсум H для S есть $H = \{a, f(a), f(f(a)), \dots\}$. В S входят три предикатных символа: P , Q и R . Следовательно, эрбрановский базис S есть

$$A = \{P(a), Q(a), R(a), P(f(a)), Q(f(a)), R(f(a)), \dots\}.$$

Некоторые H интерпретации множества S :

$$I_1 = \{P(a), Q(a), R(a), P(f(a)), Q(f(a)), R(f(a)), \dots\},$$

$$I_2 = \{\neg P(a), \neg Q(a), \neg R(a), \neg P(f(a)), \neg Q(f(a)), \neg R(f(a)), \dots\},$$

$$I_3 = \{P(a), Q(a), \neg R(a), P(f(a)), Q(f(a)), \neg R(f(a)), \dots\}, \text{ и т.д.}$$

Можно показать, что для любой интерпретации найдется соответствующая ей H -интерпретация.

Теорема 13.3. Множество дизъюнктов S невыполнимо тогда и только тогда, когда S ложно при всех H -интерпретациях в S .

Доказательство. Первая половина теоремы очевидна, так как по определению S невыполнимо тогда и только тогда, когда S ложно при всех интерпретациях на этой области. Чтобы доказать вторую половину теоремы, предположим, что S ложно при всех H -интерпретациях в S . Положим, что S выполнимо. Тогда существует такая интерпретация I на некоторой области D , что S истинно при I . Пусть I^* есть H -интерпретация, соответствующая I . Тогда S истинно при I^* . Это противоречит предположению, что S ложно при всех H -интерпретациях в S . Следовательно, S должно быть невыполнимо, что и требовалось доказать. \bowtie

Таким образом, мы достигли цели, установленной в начале этого параграфа, т.е. нам необходимо рассматривать только интерпретации над эрбрановским универсумом, точнее, H -интерпретации, для проверки того, выполнимо множество дизъюнктов или нет. Поэтому впредь, упоминая интерпретацию, мы будем иметь в виду H -интерпретацию.

H -интерпретации можно представлять в виде семантических деревьев. Как будет видно впоследствии, нахождение доказательства невыполнимости множества дизъюнктов эквивалентно построению семантического дерева. Без потери общности можно рассматривать только бинарные семантические деревья.

↪ **Определение 13.8.** Если A — атом, то говорят, что две литеры A и $\neg A$ *контрарны* друг другу, и множество $\{A, \neg A\}$ называют *контрарной парой*.

Отметим, что дизъюнкт есть тавтология, если он содержит контрарную пару, так как $A \vee \neg A \equiv T$, и множество дизъюнктов невыполнимо, если оно содержит два единичных контрарных дизъюнкта, так как $A \ \& \ \neg A \equiv F$.

↪ **Определение 13.9.** Пусть S — множество дизъюнктов и A — его эрбрановский базис. *Семантическое (бинарное) дерево* для S есть растущее вниз дерево T , в котором каждому ребру приписан атом из A или его отрицание таким образом, что из каждого

узла N выходит два ребра, помеченные контрарными литерами, и каждая ветвь дерева не содержит контрарных литер.

Обозначим через $I(N)$ объединение всех литер, приписанных ребрам ветви, ведущей к узлу N . Тогда для каждого узла N $I(N)$ не содержит контрарных пар.

↪ **Определение 13.10.** Пусть $A = \{A_1, A_2, \dots, A_n, \dots\}$ — эрбрановский базис множества S . Говорят, что семантическое дерево для S будет *полным* тогда и только тогда, когда для каждого i ($i = 1, 2, \dots$) и каждого конечного узла N семантического дерева (т.е. для узла, из которого не выходит никаких ребер) $I(N)$ содержит либо A_i либо $\neg A_i$. Таким образом, в полном семантическом дереве каждая ветвь соответствует одной H -интерпретации.

Когда эрбрановский базис множества S бесконечен, всякое полное семантическое дерево для S будет тоже бесконечно. Полное семантическое дерево для S соответствует исчерпывающему перебору всех возможных интерпретаций для S . Если S невыполнимо, то S не сможет быть истинным в каждой из этих интерпретаций. Таким образом, мы можем остановить рост дерева из узла N , если $I(N)$ опровергает S . Это порождает следующие определения.

↪ **Определение 13.11.** Узел N называется *опровергающим*, если $I(N)$ опровергает некоторый основной пример дизъюнкта в S , но для любого предшествующего узла N' $I(N')$ не опровергает никакого основного примера дизъюнкта в S .

↪ **Определение 13.12.** Говорят, что семантическое дерево T *замкнуто* тогда и только тогда, когда каждая ветвь T оканчивается опровергающим узлом.

* Примеры.

1. Пусть $S = \{P, Q \vee R, \neg P \vee \neg Q, \neg P \vee \neg R\}$.

Эрбрановский базис множества S есть $A = \{P, Q, R\}$, невыполнимо множество основных примеров: $\{\neg P, \neg Q \vee \neg R, P \vee Q, P \vee R\}$. Семантическое дерево для S показано на рис. 13.1, замкнутое поддерево выделено более жирными линиями.

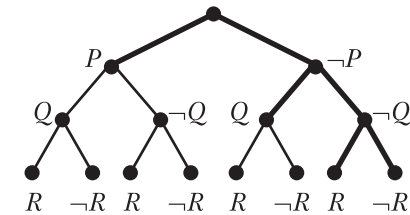


Рис. 13.1. Конечное семантическое дерево.

2. Пусть $S = \{P(x), \neg P(x) \vee Q(f(x)), \neg Q(f(a))\}$. Эрбрановский базис $A = \{P(a), Q(a), P(f(a)), Q(f(a)), \dots\}$. Невыполнимо множество основных примеров: $\{\neg P(a), P(a) \vee \neg Q(f(a)), Q(f(a))\}$.

↪ **Правило резолюций Робинсона.** Если для любых двух дизъюнктов C_1 и C_2 существует литера $L_1 \in C_1$ и контрарная ей литера $L_2 \in C_2$ ($L_2 = \neg L_1$), то вычеркнув L_1 из C_1 и L_2 из C_2 и построив дизъюнкт из оставшихся литер, получим *резольвенту* C_1 и C_2 : $C'_1 \vee C'_2$, где $C'_1 = C_1 \setminus L_1$, $C'_2 = C_2 \setminus L_2$.

Теорема 13.6. Резольвента C есть логическое следование дизъюнктов C_1 и C_2 , содержащих контрарные литеры L и $\neg L$:

$$L \vee C'_1, \neg L \vee C'_2 \models C'_1 \vee C'_2.$$

Доказательство. Предположим, что $|L \vee C'_1| = T$, $|\neg L \vee C'_2| = T$, $|C'_1 \vee C'_2| = F$. Тогда $|C'_1| = F$, $|C'_2| = F$. Если $|L \vee C'_1| = T$, то $|L| = T$, но $|\neg L \vee C'_2| = T$, следовательно, $|L| = F$. Полученное противоречие доказывает теорему. \simeq

Правило резолюций является обобщением многих известных нам правил вывода. Например, правило силлогизма: $A \rightarrow B, B \rightarrow C \models A \rightarrow C$ может быть переписано в виде: $\neg A \vee B, \neg B \vee C \models \neg A \vee C$, что соответствует правилу резолюций. Правило МР: $A, A \rightarrow B \models B$ может быть переписано в виде: $A, \neg A \vee B \models B$, что также соответствует правилу резолюций. Наконец, закон противоречия $A \& \neg A \equiv F$ равнозначен правилу: $A, \neg A \models \square$, согласно которому резольвента двух контрарных однолитерных дизъюнктов есть пустой дизъюнкт.

↪ **Определение 13.13.** Резолютивный вывод из множества дизъюнктов S есть последовательность C_1, C_2, \dots, C_k , такая, что каждое C_i либо принадлежит S , либо является резольвентой предшествующих C_i . Если последний дизъюнкт $C_k = \square$, то множество дизъюнктов S является невыполнимым, а весь вывод называется опровержением S . Если C_k не является пустым дизъюнктом и дальнейшее применение правила резолюций невозможно, то множество S является выполнимым.

✱ **Пример.** Рассмотрим пример 10.1. (см. главу 10). Необходимо проверить логическое следование в логике высказываний: $P \rightarrow S, S \rightarrow R, P \models R$. Составим множество дизъюнктов S , для чего каждую формулу приведем к КНФ, а от заключения R возьмем отрицание. Получим:

1. $\neg P \vee S$
2. $\neg S \vee R$
3. P
4. $\neg R$
5. $\neg S$ резольвента 4, 2
6. $\neg P$ резольвента 5, 1
7. \square резольвента 3, 6

Правило резолюций — очень мощное средство логического доказательства. Можно показать [Чень, Ли, 1983] полноту метода резолюций, т.е. доказать, что множество дизъюнктов S невыполнимо тогда и тогда, когда существует резолютивный вывод пустого дизъюнкта из S .

13.7. Подстановка и унификация

Применение метода резолюций в логике предикатов усложняется тем, что дизъюнкты содержат термы, которые могут не совпадать в двух одинаковых литерях. Например, $C_1 = P(x) \vee Q(x)$, $C_2 = \neg P(f(a)) \vee V(a)$. В этих дизъюнктах нет контрарных литер, однако, если мы подставим $f(a)$ вместо x в C_1 , то получим $C'_1 = P(f(a)) \vee Q(f(a))$; теперь литеры $P(f(a))$ и $\neg P(f(a))$ будут уже контрарны. Получим резольвенту $Q(f(a)) \vee V(a)$.

Такая процедура подстановки одних термов вместо других с целью получения контрарных литер называется *унификацией*.

↪ **Определение 13.14.** Подстановка — это конечное множество вида $\{t_1/v_1, \dots, t_n/v_n\}$, где v_i — переменная, t_i — терм, отличный от v_i , и все v_i различны.

↪ **Определение 13.15.** Пусть $\theta = \{t_1/v_1, \dots, t_n/v_n\}$ и E — выражение. Тогда $E\theta$ — выражение, полученное из E заменой всех вхождений переменных v_i ($1 \leq i \leq n$) на термы t_i .

Определение 13.16. Пусть $\theta = \{t_1/v_1, \dots, t_n/v_n\}$, $\lambda = \{u_1/y_1, \dots, u_k/y_k\}$ — подстановки. Композиция подстановок $\theta^\circ \lambda$ получается из множества $\{t_1\lambda/v_1, \dots, t_n\lambda/v_n, u_1/y_1, \dots, u_k/y_k\}$ вычеркиванием всех элементов $t_j\lambda/v_j$ для которых $t_j\lambda = v_j$ (тождественная подстановка), и всех элементов u_i/y_i , таких, что $y_i \in \{v_1, \dots, v_n\}$.

✱ **Пример.** Пусть $\theta = \{t_1/v_1, t_2/v_2\} = \{f(y)/x, z/y\}$, $\lambda = \{u_1/y_1, u_2/y_2, u_3/y_3\} = \{a/x, b/y, y/z\}$. Тогда $\theta^\circ \lambda = \{t_1\lambda/v_1, t_2\lambda/v_2, u_1/y_1, u_2/y_2, u_3/y_3\} = \{f(b)/x, y/y, a/x, b/y, y/z\}$. Так как $t_2\lambda/v_2 = y/y$, то y/y должно быть вычеркнуто из множества $\theta^\circ \lambda$. Элементы $a/x, b/y$ также должны быть вычеркнуты, так как подстановки для x и y уже определены. В результате получаем: $\theta^\circ \lambda = \{f(b)/x, y/z\}$.

В процедуре доказательства методом резолюций необходимо находить такие подстановки, которые позволяют сделать два и более выражения тождественными.

↪ **Определение 13.17.** Подстановка θ называется *унификатором* множества $\{E_1, \dots, E_m\}$ тогда и только тогда, когда $E_1\theta = \dots = E_m\theta$. Множество $\{E_1, \dots, E_m\}$ называется *унифицируемым*, если для него существует унификатор. Унификатор σ для множества выражений $\{E_1, \dots, E_m\}$ называется *наиболее общим унификатором*, если для каждого унификатора θ этого множества существует такая подстановка λ , что $\theta = \sigma^\circ \lambda$.

Например, для двух дизъюнктов $\{P(a, y), P(x, f(b))\}$ подстановка $\{a/x, f(b)/y\}$ является наиболее общим унификатором.

Введя понятие унификации, мы можем рассмотреть метод резолюций для логики первого порядка.

↪ **Определение 13.18.** Если две или более литер (с одинаковым знаком) дизъюнкта C имеют наиболее общий унификатор σ , то $C\sigma$ называется *склежкой* C . Если $C\sigma$ — единичный дизъюнкт, то склейка называется *единичной склейкой*.

✱ **Пример.** Пусть $C = P(x) \vee P(f(y)) \vee \neg Q(x)$. Тогда первая и вторая литеры имеют наиболее общий унификатор $\sigma = \{f(y)/x\}$. Следовательно, $C\sigma = P(f(y)) \vee \neg Q(f(y))$ есть склейка C .

↪ **Определение 13.19.** Пусть C_1 и C_2 — два дизъюнкта (называемые *дизъюнктами-посылками*), которые не имеют никаких общих переменных. Пусть L_1 и $\neg L_2$ — две литеры в C_1 и C_2 соответственно. Если L_1 и L_2 имеют наиболее общий унификатор σ , то дизъюнкт $(C_1\sigma \setminus L_1\sigma) \vee (C_2\sigma \setminus L_2\sigma)$ называется (*бинарной*) *резольвентой* C_1 и C_2 . Литеры L_1 и L_2 называются *отрезаемыми литерами*.

↪ **Определение 13.20.** Резольвентой дизъюнктов-посылок C_1 и C_2 является одна из следующих резольвент:

- 1) бинарная резольвента C_1 и C_2 ;
- 2) бинарная резольвента C_1 и склейки C_2 ;
- 3) бинарная резольвента C_2 и склейки C_1 ;
- 4) бинарная резольвента склейки C_1 и склейки C_2 .

✱ **Пример.** Пусть $C_1 = P(x) \vee P(f(y)) \vee R(g(y))$ и $C_2 = \neg P(f(g(a))) \vee Q(b)$. Склейка C_1 есть $C_1' = P(f(y)) \vee R(g(y))$. Выполним подстановку $g(a)/y$. Бинарная резольвента C_1' и C_2 есть $R(g(g(a))) \vee Q(b)$. Следовательно, $R(g(g(a))) \vee Q(b)$ есть резольвента C_1 и C_2 .

13.8. Примеры использования метода резолюций

Пример 13.1. Завершим рассмотрение примера 12.1 главы 12. ССФ посылки мы получили в 13.3:

$$\forall y((\neg D(y) \vee L(a, y)) \& P(a)), \forall x \forall y(\neg Q(y) \vee \neg L(x, y) \vee \neg P(x)).$$

Найдем отрицание от заключения G и приведем его к ПНФ; получим:

$$\neg \forall y(D(y) \rightarrow \neg Q(y)) = \exists y \neg(\neg D(y) \vee \neg Q(y)) = \exists y(D(y) \& Q(y)).$$

Элиминируем квантор \exists и получим ССФ: $D(b) \& Q(b)$.

Построим резолютивный вывод:

1. $\neg D(y) \vee L(a, y)$
2. $P(a)$

$$3. \neg Q(y) \vee \neg L(x, y) \vee \neg P(x)$$

$$4. D(b)$$

$$5. Q(b)$$

$$6. \neg L(x, b) \vee \neg P(x) \quad \{b/y\}, \text{ резольвента } 5, 3$$

$$7. \neg L(a, b) \quad \{a/x\}, \text{ резольвента } 2, 6$$

$$8. \neg D(b) \quad \{b/y\}, \text{ резольвента } 1, 7$$

$$9. \square \quad \text{резольвента } 4, 8$$

Пример 13.2. Посылка: «Каждый, кто хранит деньги, получает проценты». Заключение: «Если не существует процентов, то никто не хранит денег». Пусть $S(x, y)$: « x хранит y », $M(x)$: « x есть деньги», $I(x)$: « x есть проценты» и $E(x, y)$: « x получает y ». Тогда посылка записывается в виде: $\forall x(\exists y(S(x, y) \& M(y)) \rightarrow \exists y(I(y) \& E(x, y)))$, а заключение: $\neg \exists x I(x) \rightarrow \forall x \forall y(S(x, y) \rightarrow \neg M(y))$.

Приведем посылку к ССФ:

$$\begin{aligned} & \forall x(\exists y(S(x, y) \& M(y)) \rightarrow \exists y(I(y) \& E(x, y))) = \\ & = \forall x(\neg \exists y(S(x, y) \& M(y)) \vee \exists y(I(y) \& E(x, y))) = \\ & = \forall x(\forall y(\neg S(x, y) \vee \neg M(y)) \vee \exists y(I(y) \& E(x, y))) = \\ & = \forall x(\exists z(I(z) \& E(x, z))) \vee \forall y(\neg S(x, y) \vee \neg M(y)) = \\ & = \forall x \exists z((I(z) \& E(x, z)) \vee \forall y(\neg S(x, y) \vee \neg M(y))) = \\ & = \forall x \exists z \forall y((I(z) \& E(x, z)) \vee (\neg S(x, y) \vee \neg M(y))) = \\ & = \forall x \exists z \forall y((\neg S(x, y) \vee \neg M(y) \vee I(z)) \& (\neg S(x, y) \vee \neg M(y) \vee E(x, z))). \end{aligned}$$

ССФ посылки:

$$\forall x \forall y((\neg S(x, y) \vee \neg M(y) \vee I(f(x)) \& (\neg S(x, y) \vee \neg M(y) \vee E(x, f(x)))).$$

В результате получим дизъюнкты:

1. $\neg S(x, y) \vee \neg M(y) \vee I(f(x))$,
2. $\neg S(x, y) \vee \neg M(y) \vee E(x, f(x))$.

Возьмем отрицание от заключения и приведем к ПНФ:

$$\begin{aligned} & \neg(\neg \exists x I(x) \rightarrow \forall x \forall y(S(x, y) \rightarrow \neg M(y))) = \\ & = \neg(\neg \neg \exists x I(x) \vee \forall x \forall y(\neg S(x, y) \vee \neg M(y))) = \\ & = \forall x \neg I(x) \& \neg \forall x \forall y(\neg S(x, y) \vee \neg M(y)) = \\ & = \forall z \neg I(z) \& \exists x \exists y(S(x, y) \& M(y)). \end{aligned}$$

Поскольку полученная формула представляет собой конъюнкцию двух формул в ПНФ, можно каждую из них приводить к ССФ отдельно: $\forall z \neg I(z) \& (S(a, b) \& M(b))$.

Из отрицания заключения получили дизъюнкты:

3. $\neg I(z)$,
4. $S(a, b)$,
5. $M(b)$.

Дальнейшее доказательство очень просто:

6. $\neg S(x, y) \vee \neg M(y)$ $\{f(x)/z\}$ в 3, резольвента 3, 1
7. $\neg M(b)$ $\{a/x, b/y\}$ в 6, резольвента 6, 4
8. \square резольвента 7, 5

Логическое следование доказано.

Пример 13.3. Посылка: «Студенты есть граждане». Заключение: «Голоса студентов есть голоса граждан.» Пусть $S(x)$: « x — студент», $C(x)$: « x — гражданин» и $V(x, y)$: « x есть голос y ». Тогда посылка и заключение запишутся следующим образом:

$\forall y(S(y) \rightarrow C(y))$ (посылка),
 $\forall x(\exists y(S(y) \& V(x, y)) \rightarrow \exists z(C(z) \& V(x, z)))$ (заключение).

Стандартная форма посылки есть $\forall y(\neg S(y) \vee C(y))$.

Отрицание заключения приведем к ССФ:

$\neg(\forall x(\exists y(S(y) \& V(x, y)) \rightarrow \exists z(C(z) \& V(x, z)))) =$
 $= \neg(\forall x(\forall y(\neg S(y) \vee \neg V(x, y)) \vee \exists z(C(z) \& V(x, z)))) =$
 $= \neg(\forall x\forall y\exists z(\neg S(y) \vee \neg V(x, y) \vee (C(z) \& V(x, z)))) =$
 $= \exists x\exists y\forall z((S(y) \& V(x, y)) \& (\neg C(z) \vee \neg V(x, z)));$

ССФ: $\forall z((S(b) \& V(a, b)) \& (\neg C(z) \vee \neg V(a, z)))$,

Запишем множество дизъюнктов и построим резольютивный вывод:

1. $\neg S(y) \vee C(y)$.
2. $S(b)$,
3. $V(a, b)$,
4. $\neg C(z) \vee \neg V(a, z)$.
5. $C(b)$ $\{b/y\}$ в 1, резольвента 1, 2
6. $\neg V(a, b)$ $\{b/z\}$ в 4, резольвента 5, 4
7. \square резольвента 6, 3.

Пример 13.4. Проверим логичность утверждения Лосева А. Ф.¹: «Вера в сущности своей и есть подлинное знание, и эти две сферы не только не разведимы, но даже неразличимы».

Доказательство Лосева заключается в следующем.

«Верующий верит в нечто. Вера свой предмет ясно отличает от всякого другого предмета. Тогда этот предмет определен. Но если он определен, он обладает признаками, отличающими его от всякого другого. Это значит, что мы знаем этот предмет. Мы знаем вещь, если по признакам можем отличить ее от всякого другого. Следовательно, вера и есть знание.»

¹ А. Ф. Лосев. Диалектика мифа. В кн. «Из ранних произведений». М.: Правда, 1990. (стр. 497).

Пусть $V(x, y)$: « x верит в y », $C(x, y)$: « x отличен от y », $N(x, y)$: « x знает y ». Формализуем посылки.

1. Верующий верит в нечто.
 $\forall x\exists yV(x, y)$.
2. Верующий свой предмет отличает от всякого другого предмета.
 $\forall x\exists y(V(x, y) \rightarrow \forall zC(y, z))$.
3. Мы знаем вещь тогда, когда мы отличаем ее от всякой другой вещи.
 $\forall x\exists y\forall z(C(y, z) \rightarrow N(x, y))$.
4. Следовательно, вера есть знание.
 $\forall x\exists y(V(x, y) \rightarrow N(x, y))$.

После приведения посылок и отрицания заключения к ССФ, получим множество дизъюнктов и резольютивный вывод:

1. $V(x, f(x))$ — x верит в предмет своей веры.
2. $C(f(x), z) \vee \neg V(x, f(x))$ — если x верит в $f(x)$,
то $f(x)$ отличен от z .
3. $N(x, f(x)) \vee \neg C(f(x), z)$ — x знает $f(x)$, если может
отличить его от z .
4. $V(b, y)$ — существует b , который верит в y .
5. $\neg N(b, y)$ — b не знает y .
6. $\neg C(f(b), z)$ — $\{b/x, f(b)/y\}$ в 2 и 4,
резольвента 5, 3.
7. $\neg V(b, f(b))$ — резольвента 6, 2.
8. \square — резольвента 1, 7.

Получаем, что вера и знание — одно и то же. Это заключение вызывает сомнения, несмотря на то, что логическое следование выполнено. Дело в том, что посылки этого утверждения принимаются автором за истинные, однако с их истинностью можно не согласиться. Например, утверждение «Мы знаем вещь тогда, когда мы отличаем ее от всякой другой вещи» вызывает сомнение, — осознание отличия одной вещи от другой еще не есть знание. Сомнение в истинности одной посылки приводит к тому, что и заключение вызывает сомнение, — ведь из противоречивой системы посылок можно вывести что угодно.

Пример 13.5. Согласно принципу Питера, служащий продвигается по служебной лестнице до тех пор, пока он не достигнет своего уровня некомпетентности. Следует ли из этого, что не существует компетентных начальников?

Проверим этот вывод, используя метод резолюций. Выберем предикаты: $C(x)$: x — служащий, $K(x)$: x — компетентный, $N(x)$: x — начальник, $P(x)$: x продвигается по служебной лестнице. Формализу-

ем свои знания о проблеме. В качестве первой посылки возьмем утверждение о том, что *компетентный служащий продвигается по служебной лестнице*: $\forall x(C(x) \& K(x) \rightarrow P(x))$.

Второй посылкой может служить утверждение о том, что *начальник перестает продвигаться по служебной лестнице*:

$\forall x(N(x) \rightarrow \neg P(x))$.

Учтем также тот факт, что *начальник – тоже служащий*:

$\forall x(N(x) \rightarrow C(x))$.

Тогда вывод, который нужно проверить, можно сформулировать так: «*Все начальники некомпетентны*»: $\forall x(N(x) \rightarrow \neg K(x))$.

Приведем посылки и отрицание заключения к ССФ и построим резолютивный вывод:

1. $N(a)$
2. $K(a)$
3. $\neg C(x) \vee \neg K(x) \vee P(x)$
4. $\neg N(x) \vee \neg P(x)$
5. $\neg N(x) \vee C(x)$
6. $\neg C(a) \vee P(a)$ $\{a/x\}$ в 3, резольвента 2, 3
7. $\neg N(a) \vee P(a)$ $\{a/x\}$ в 5, резольвента 5, 6
8. $\neg N(a)$ $\{a/x\}$ в 4, резольвента 4, 7
9. \square резольвента 1, 8

Итак, мы получили, что компетентных начальников не существует.

Пример 13.6. Рассмотрим задачу о брадобреях: *В одном селе брадобрей бреет тех и только тех жителей села, которые не бреются сами. Должен ли брадобрей брить самого себя?*

Возьмем предикаты: $P(x)$: x брадобрей, $Q(x, y)$: x бреет y .

Формализуем посылку и приведем ее к ССФ:

$\exists x(P(x) \& \forall y(Q(y, y) \rightarrow \neg Q(x, y)) \& (\neg Q(y, y) \rightarrow Q(x, y)))$.

ССФ: $(P(a) \& \forall y(\neg Q(y, y) \vee \neg Q(a, y)) \& (Q(y, y) \vee Q(a, y)))$.

Проверим, бреет ли брадобрей самого себя: $Q(a, a)$. Построим вывод:

1. $P(a)$
2. $\neg Q(y, y) \vee \neg Q(a, y)$
3. $Q(y, y) \vee Q(a, y)$
4. $\neg Q(a, a)$
5. $Q(a, a)$ подстановка $\{a/y\}$ в 3, склейка 3
6. \square резольвента 4, 5

Логическое следование выполнено, т.е. брадобрей должен брить самого себя.

Поставим противоположный вопрос: брадобрей не должен брить самого себя: $\neg Q(a, a)$, и построим резолютивный вывод:

1. $P(a)$
2. $\neg Q(y, y) \vee \neg Q(a, y)$
3. $Q(y, y) \vee Q(a, y)$
4. $Q(a, a)$
5. $\neg Q(a, a)$ подстановка $\{a/y\}$ в 2, склейка 2
6. \square резольвента 4, 5

Логическое следование также выполнено, т.е. брадобрей не должен брить самого себя.

В этой задаче на два противоположных вопроса мы получаем одинаковый ответ, поскольку исходное утверждение противоречиво само по себе.

Метод резолюций — это очень сильный метод поиска доказательства общезначимости формул (в другой формулировке — логических следований). Именно поэтому он породил новую парадигму программирования — логическое программирование. Наиболее распространенным языком логического программирования является ПРОЛОГ. В логическом программировании любая задача ставится как задача доказательства логического следования некоторого предложения из заданных посылок. Выполнение программы заключается в поиске доказательства методом резолюций.

СВОЙСТВА ТЕОРИЙ ПЕРВОГО ПОРЯДКА

Успехи развития дедуктивного метода породили большое количество работ по формализации основных разделов математики. Идея создания универсального языка для всей математики и формализации математических доказательств средствами этого языка выдвигалась еще Лейбницем. В середине 19-го века работы Буля и де Моргана по формализации аристотелевой логики создали предпосылки для построения такого языка. После того, как Г. Фреге (1879) и Ч. Пирс (1885) ввели в язык логики предикаты, предметные переменные и кванторы, возникла реальная возможность применить этот язык к формализации оснований математики. В работах Вейерштрасса, Дедекинда и Кантора была показана возможность «арифметизации» анализа и теории функций, в результате чего арифметика натуральных чисел стала рассматриваться как фундамент всей классической математики. Поэтому вполне естественно было начать формализацию оснований математики с аксиоматизации арифметики. Наиболее удобная система аксиом арифметики была предложена Пеано (1891). В начале 20-го века возникло направление в математике, целью которого было представить всю чистую математику как часть формальной логики. Уайтхед и Рассел в 1910 — 1913 г.г. опубликовали свой фундаментальный труд «Principia Mathematica», посвященный математической логике и основаниям математики. В этой работе была усовершенствована аксиоматика арифметики и на ее основе формализованы некоторые другие разделы математики. Однако, не все обстояло гладко на этом пути. Так, например, оказалось невозможным вывести из чисто логических аксиом существование бесконечных множеств. Открытие парадоксов, связанных с основными понятиями теории множеств, еще больше поколебало уверенность математиков в достижении поставленной цели. Основная проблема заключалась в доказательстве непротиворечивости выбранной системы аксиом. Д. Гильберт поставил перед собой задачу развития теории доказательств. Заслуга Гильберта состоит в том, что он указал путь для исследования непротиворечивости аксиоматических систем. Непротиворечивость теории означает, что в ней нельзя вывести противоречие. Тогда для доказательства непротиворечивости формальной теории нужно доказать невыводимость в ней каких-либо утверждений. Таким образом математическая теория, непротиворечивость которой нужно доказать, становится объектом изучения другой математической науки, которую Гильберт назвал метаматематикой или теорией доказательств. Двухтомная монография Д. Гильберта и П. Бернаиса «Основания математики. Логические исчисления и формализация арифметики», вышедшая в 30-х г.г., подвела итог процессу

становления математической логики как самостоятельной математической дисциплины.

В 1930 г. австрийский математик Курт Гёдель доказал теорему о полноте исчисления предикатов, согласно которой множество логически общезначимых формул логики предикатов совпадает с множеством теорем исчисления предикатов. Однако уже в 1931 г. появилась другая работа Гёделя: «О формально неразрешимых предложениях Principia Mathematica и родственных систем». Доказанная в ней теорема о неполноте формальной арифметики признана одним из величайших достижений современной математики. Гёделю в это время было 25 лет. Согласно этой теореме, если формальная система, содержащая арифметику, непротиворечива, то в ней существуют истинные, но не выводимые из аксиом этой теории предложения. Отсюда следует, что формальная теория, средствами которой можно построить арифметику, существенно неполна, т.е. никакое расширение ее системы аксиом не сделает ее полной, так как в новой системе все равно найдутся истинные, но не выводимые ее средствами предложения. Другой результат Гёделя заключается в том, что нельзя доказать непротиворечивость формальной теории первого порядка, включающей формальную арифметику, средствами, выразимыми в этой теории. Для доказательства непротиворечивости необходимо привлечение средств, выходящих за рамки формальной арифметики. Такие доказательства непротиворечивости арифметики были получены позже Г. Генценом и П. С. Новиковым. Результаты, полученные Гёделем, показали, что возможности аксиоматического метода определенным образом ограничены, причем ограничения таковы, что даже арифметика натуральных чисел не может быть полностью аксиоматизирована. Открытия Гёделя разрушили надежды логиков о полной формализации математики. Однако работы Гёделя обогатили математическую науку совершенно новыми методами рассуждений и имели огромное значение для развития философии науки. Результаты Гёделя показывают, что возможности нашего мышления не сводятся к полностью формализуемым процедурам дедуктивных рассуждений. Человеческое мышление и способы человеческих рассуждений гораздо богаче, и для их формализации (даже частичной), необходимо привлечение средств, выходящих за рамки дедуктивных рассуждений.

14.1. Свойства исчисления предикатов первого порядка

Рассмотрим свойства исчисления предикатов: непротиворечивость и полноту. Напомним, что исчисление предикатов первого порядка содержит только логические аксиомы и не содержит собственных аксиом.

Теорема 14.1. Всякое исчисление предикатов первого порядка непротиворечиво.

Доказательство. Для любой произвольной формулы A введем преобразование $h(A)$: в A опускаются все кванторы и термы вместе с соответствующими скобками и запятыми. Результат преобразования h всегда есть пропозициональная форма, в которой роль пропозициональных букв играют предикатные символы. Например, $h(\neg \forall x(P(x, y) \rightarrow \exists y Q(y))) = \neg P \rightarrow Q$. Очевидно, что $h(\neg A) = \neg h(A)$ и $h(A \rightarrow B) = h(A) \rightarrow h(B)$. При применении преобразования $h(A)$ к схемам аксиом A1 – A3? теории K они не изменятся. Схема аксиомы A4: $\forall x A(x) \rightarrow A(y)$ преобразуется в тавтологию $A \rightarrow A$, а схема A5: $\forall x(A \rightarrow B(x)) \rightarrow (A \rightarrow \forall x B(x))$ – в тавтологию $(A \rightarrow B) \rightarrow (A \rightarrow B)$. Если $h(A)$ и $h(A \rightarrow B)$ – тавтологии, то и $h(B)$ – тоже тавтология, а если $h(A)$ – тавтология, то и $h(\forall x A(x))$ – тавтология, так как результаты применения преобразования h к A и $\forall x A(x)$ совпадают. Следовательно, если A есть теорема теории K , то $h(A)$ есть тавтология. Если бы существовала формула B в K такая, что $\vdash_K B$ и $\vdash_K \neg B$, то оба выражения $h(B)$ и $h(\neg B)$ были бы тавтологиями, что невозможно. Таким образом, K непротиворечиво. \square

Теорема 14.2. Во всяком исчислении предикатов первого порядка всякая теорема является логически общезначимой.

Доказательство. Аксиомы, задаваемые схемами A1 – A3, являются логически общезначимыми формулами, так как каждая из них является тавтологией логики высказываний. Схемы аксиом A4, A5 являются логически общезначимыми в логике предикатов, следовательно, любая аксиома, порожденная этими схемами, общезначима. Правила вывода MP и Gen сохраняют свойство общезначимости, следовательно, всякая теорема исчисления предикатов логически общезначима. \square

Теорема 14.2 представляет собой лишь половину теоремы о полноте исчисления предикатов: необходимо еще доказать обратную теорему о том, что всякая логически общезначимая формула теории предикатов является теоремой исчисления предикатов. Эта теорема была доказана Гёделем в 1930 г. и известна как теорема о полноте. Здесь мы приведем ее без доказательства.

Теорема 14.3. (Теорема Гёделя о полноте). Во всяком исчислении предикатов первого порядка теоремами являются те и только те формулы, которые логически общезначимы.

Для исчисления высказываний теорема о полноте теории L приводит к решению проблемы разрешимости: с помощью построения таблицы истинности для любой формулы исчисления высказываний можно проверить, является она теоремой или нет. Однако для

теорий первого порядка нельзя получить разрешающую процедуру для доказательства общезначимости, или, что то же самое, для выводимости формулы из множества гипотез. Этот результат, а также некоторые другие результаты, будут рассмотрены в главе 15.

14.2. Формальная арифметика

14.2.1. Система аксиом Пеано

Именно с арифметики натуральных чисел были начаты попытки формализации математики. Первое, полуаксиоматическое построение этой дисциплины было предложено Пеано и усовершенствовано Дедекиндом в 1901 г. Эту систему можно сформулировать следующим образом.

(P1) 0 есть натуральное число.

(P2) Для любого натурального числа x существует другое натуральное число, которое обозначается x' и называется (*непосредственно*) *следующее* за x .

(P3) $0 \neq x'$ для любого натурального числа x .

(P4) Если $x' = y'$, то $x = y$.

(P5) Если Q есть свойство, которым обладают одни и, может быть, не обладают другие натуральные числа, и если

(I) натуральное число 0 обладает свойством Q и

(II) для всякого натурального числа x из того, что x обладает свойством Q , следует, что и натуральное число x' обладает свойством Q , то свойством Q обладают все натуральные числа (принцип индукции).

Этих аксиом, вместе с некоторым фрагментом теории множеств, достаточно для построения не только арифметики, но и теории рациональных, вещественных и комплексных чисел. Поэтому можно построить теорию первого порядка S , основанную на системе аксиом Пеано, которая достаточна для вывода всех основных результатов элементарной арифметики.

14.2.2. Формальная теория S

⇨ **Определение 14.1.** Теория первого порядка S имеет единственную предикатную букву A_1^2 : $t = s$, единственную предметную константу $a_1 = 0$ и три функциональные буквы $f_1^1(t)$: t' , $f_2^2(t, s)$: $t + s$, $f_2^2(t, s)$: $t \cdot s$, где t и s – термы. Собственные аксиомы теории S :

S1. $x_1 = x_2 \rightarrow (x_1 = x_3 \rightarrow x_2 = x_3)$;

S2. $x_1 = x_2 \rightarrow x_1' = x_2'$;

S3. $0 \neq x_1'$;

S4. $x_1' = x_2' \rightarrow x_1 = x_2$;

S5. $x_1 + 0 = x_1$;

$$S6. x_1 + x_2' = (x_1 + x_2)';$$

$$S7. x_1 \cdot 0 = 0;$$

$$S8. (x_1 \cdot x_2)' = (x_1 \cdot x_2) + x_1;$$

S9. $A(0) \rightarrow (\forall x(A(x) \rightarrow A(x')) \rightarrow \forall x A(x))$, где $A(x)$ — произвольная формула теории S .

Аксиомы $S1 - S8$ являются конкретными формулами, в то время, как $S9$ представляет собой схему аксиом, порождающую бесконечное множество аксиом. При этом схема аксиом $S9$, которая называется *принципом математической индукции*, не соответствует полностью аксиоме (P5) системы аксиом Пеано, поскольку в (P5) свойства натуральных чисел не определяются конструктивно, а в S они определяются формулами теории.

С помощью МР из схемы аксиом $S9$ можно получить следующее *правило индукции*:

$$A(0), \forall x(A(x) \rightarrow A(x')) \vdash \forall x A(x).$$

Интерпретация теории S , в которой:

(a) множество всех неотрицательных целых чисел служит областью определения,

(b) целое число 0 интерпретирует символ 0,

(c) операция взятия последующего (прибавление единицы) интерпретирует функцию $'$ (т.е. функциональную букву $f_1'(t)$),

(d) обычные сложение и умножение интерпретируют функции $+$ и \cdot ,

(e) предикатная буква A_1^2 интерпретируется отношением тождества $=$, называется *стандартной моделью теории S*.

14.3. Прimitивно рекурсивные и рекурсивные функции

14.3.1. Прimitивно рекурсивные функции

↪ **Определение 14.2.** Арифметическими функциями называются функции, у которых область определения и множество значений состоят из натуральных чисел, а арифметическим отношением называются отношения, заданные на множестве натуральных чисел.

Так, например, умножение есть арифметическая функция с двумя аргументами, а выражение $x + y < z$ определяет арифметическое отношение с тремя аргументами.

↪ **Определение 14.3.**

(1). Следующие функции называются *исходными функциями*.

(I) **Нуль-функция:** $Z(x) = 0$ для каждого x .

(II) **Прибавление единицы** (следующий за): $N(x) = x + 1$ для каждого x .

(III) **Проектирующие функции:** $U_i^n(x_1, \dots, x_n) = x_i$ при всех x_1, \dots, x_n ($i = 1, \dots, n$; $n = 1, 2, \dots$).

(2). Следующие два правила: подстановка и примитивная рекурсия, — служат для получения новых функций, исходя из уже имеющихся.

(IV) **Подстановка.** Говорят, что функция f получена с помощью подстановки из функций $g(y_1, \dots, y_n), h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n)$, если $f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$.

(V) **Схема примитивной рекурсии.** Функция f получена из функций g и h с помощью рекурсии, если

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n),$$

$$f(x_1, \dots, x_n, y + 1) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)).$$

При этом исключается случай $n = 0$, для которого отдельно:

$$f(0) = k \text{ (где } k \text{ — фиксированное целое неотрицательное число),}$$

$$f(y + 1) = h(y, f(y)).$$

Заметим, что функция f вполне определена: значение $f(x_1, \dots, x_n, 0)$ определяется из первого равенства, а если мы уже знаем значение $f(x_1, \dots, x_n, y)$, то из второго равенства мы можем найти значение $f(x_1, \dots, x_n, y + 1)$.

(3). Функция f называется *примитивно рекурсивной*, если она может быть получена из исходных функций с помощью конечного числа подстановок (IV) и рекурсий (V), т.е. если существует такая конечная последовательность функций f_1, \dots, f_n , что $f_n = f$ и для каждого i , $0 \leq i \leq n$, функция f_i либо исходная, либо может быть получена из некоторых предшествующих ей в этой последовательности функций с помощью применения правила (IV) (подстановки) или правила (V) (рекурсии).

Теорема 14.4. Следующие функции являются примитивно рекурсивными.

(a) $x + y$ (сложение).

Доказательство.

По правилу рекурсии (V):

$$x + 0 = x, \text{ т.е. } f(x, 0) = U_1^1(x) = x.$$

$$x + (y + 1) = N(x + y), \text{ т.е. } f(x, y + 1) = N(f(x, y)).$$

(b) $x \cdot y$ (умножение).

Доказательство.

$$x \cdot 0 = 0, \text{ т.е. } g(x, 0) = Z(x).$$

$$x \cdot (y + 1) = (x \cdot y) + x, \text{ т.е. } g(x, y + 1) = f(x, g(x, y)), \text{ где } f \text{ есть функция сложения.}$$

(с) x^y (возведение в степень).

Доказательство.

$$x^0 = 1, x^{y+1} = (x^y) \cdot x.$$

(d) $\delta(x) = x - 1$, если $x > 0$, и $\delta(x) = 0$, если $x = 0$ (вычитание единицы).

Доказательство.

$$\delta(0) = 0, \delta(y + 1) = y.$$

(e) $x \div y = x - y$, если $x \geq y$, и $x \div y = 0$, если $x < y$ (ограниченная разность).

Доказательство.

$$x \div 0 = x, x \div (y + 1) = \delta(x \div y).$$

(f) $|x - y| = x - y$, если $x \geq y$, $|x - y| = y - x$, если $x < y$ (модуль разности).

Доказательство.

$$|x - y| = (x \div y) + (y \div x) \text{ (подстановка)}.$$

(g) $sg(x) = 0$, если $x = 0$, $sg(x) = 1$, если $x \neq 0$ (сигнум x).

Доказательство.

$$sg(0) = 0, sg(y + 1) = 1.$$

(h) $unsg(x) = 1$, если $x = 0$, $unsg(x) = 0$, если $x \neq 0$;

Доказательство.

$$unsg(x) = 1 \div sg(x).$$

(i) $x!$ (факториал x).

Доказательство.

$$0! = 1, (y + 1)! = (y!) \cdot (y + 1).$$

(j) $\min(x, y)$ = наименьшему из чисел x и y ;

Доказательство.

$$\min(x, y) = x \div (x \div y).$$

(k) $\min(x_1, \dots, x_n)$.

Доказательство.

Предположим, что функция $\min(x_1, \dots, x_n)$ — примитивно рекурсивная. Для $\min(x_1, \dots, x_{n+1})$ имеем $\min(x_1, \dots, x_{n+1}) = \min(\min(x_1, \dots, x_n), x_{n+1})$.

(l) $\max(x, y)$ = наибольшему из чисел x и y .

Доказательство.

$$\max(x, y) = y + (x \div y).$$

(m) $\max(x_1, \dots, x_n)$;

Доказательство.

$$\max(x_1, \dots, x_{n+1}) = \max(\max(x_1, \dots, x_n), x_{n+1}).$$

(n) $rm(x, y)$ = остатку от деления y на x , если $x \neq 0$, и y , если $x = 0$.

Доказательство.

$$rm(x, 0) = 0, rm(x, y + 1) = N(rm(x, y)) \cdot sg(|x - N(rm(x, y))|).$$

(o) $qt(x, y)$ = частному от деления y на x .

Доказательство.

$$qt(x, 0) = 0, qt(x, y + 1) = qt(x, y) + unsg(|x - N(rm(x, y))|).$$

Определения (ограниченных сумм и произведений).

$$\begin{aligned} \hookrightarrow 14.4. \quad & \sum_{y < z} f(x_1, \dots, x_n, y) = 0, \text{ если } z = 0, \\ & \sum_{y < z} f(x_1, \dots, x_n, y) = f(x_1, \dots, x_n, 0) + \dots + f(x_1, \dots, x_n, z - 1), \\ & \text{если } z > 0. \end{aligned}$$

$$\hookrightarrow 14.5. \quad \sum_{y \leq z} f(x_1, \dots, x_n, y) = \sum_{y < z+1} f(x_1, \dots, x_n, y).$$

$$\begin{aligned} \hookrightarrow 14.6. \quad & \prod_{y < z} f(x_1, \dots, x_n, y) = 1, \text{ если } z = 0, \\ & \prod_{y < z} f(x_1, \dots, x_n, y) = f(x_1, \dots, x_n, 0) \cdot \dots \cdot f(x_1, \dots, x_n, z - 1), \\ & \text{если } z > 0. \end{aligned}$$

$$\hookrightarrow 14.7. \quad \prod_{y \leq z} f(x_1, \dots, x_n, y) = \prod_{y < z+1} f(x_1, \dots, x_n, y).$$

Эти *ограниченные суммы и произведения* являются функциями аргументов x_1, \dots, x_n, z . Суммы и произведения, ограниченные с двух сторон, можно теперь определить через введенные только что ограниченные суммы и произведения, например:

$$\begin{aligned} \sum_{u \leq y < v} f(x_1, \dots, x_n, y) &= f(x_1, \dots, x_n, u + 1) + \dots + f(x_1, \dots, x_n, v - 1) = \\ &= \sum_{y < (y+u)+1} f(x_1, \dots, x_n, y + u + 1). \end{aligned}$$

14.3.2. Рекурсивные функции

Введем еще одно правило получения новых функций.

\hookrightarrow (VI) **μ -оператор (оператор минимизации).** Пусть функция $g(x_1, \dots, x_n, y)$ такова, что для любых x_1, \dots, x_n существует по крайней мере одно значение y , при котором $g(x_1, \dots, x_n, y) = 0$. Обозначим через $\mu y(g(x_1, \dots, x_n, y) = 0)$ наименьшее значение y , при котором $g(x_1, \dots, x_n, y) = 0$. Тогда функция f получена из функции g с помощью μ -оператора, если $f(x_1, \dots, x_n) = \mu y(g(x_1, \dots, x_n, y) = 0)$.

При применении μ -оператора можно использовать не только отношение равенства, но и другие отношения: $<$, \leq , $>$, \geq . Вообще, для всякого отношения $R(x_1, \dots, x_n, y)$ будем обозначать через $\mu y R(x_1, \dots, x_n, y)$ то наименьшее значение y , при котором $R(x_1, \dots, x_n, y)$ истинно, если вообще такие значения существуют.

\hookrightarrow (4). Функция f называется *рекурсивной*, если она может быть получена из исходных функций с помощью конечного числа применений подстановки (IV), рекурсии (V) и μ -оператора (VI).

Это последнее определение отличается от определения примитивно рекурсивной функции лишь дополнительным разрешением применять μ -оператор. Поэтому всякая примитивно рекурсивная

функция является также и рекурсивной функцией. Обратное, впрочем, не всегда верно. (В литературе вместо термина «рекурсивный» иногда употребляется термин «частично рекурсивный».)

↪ **Определение 14.8.** *Ограниченный μ -оператор* определим так: $\mu_{y < z} R(x_1, \dots, x_n, y)$ равно наименьшему y такому, что $y < z$ и $R(x_1, \dots, x_n, y)$ истинно, если такое y существует, и z в противном случае.

Неограниченный μ -оператор (определенный в (VI)) задает следующую схему вычислений n -местной функции $f(x_1, \dots, x_n)$. Для фиксированных значений аргументов x_1, \dots, x_n находится решение уравнения $g(x_1, \dots, x_n, y) = x_{n+1}$ для $y = 0, 1, 2, \dots$. Наименьшее значение $y = b$, для которого $g(x_1, \dots, x_n, b) = x_{n+1}$ и есть значение функции $f(x_1, \dots, x_n) = \mu y (g(x_1, \dots, x_n, y) = x_{n+1})$, полученной из функции g с помощью μ -оператора. Этот процесс нахождения значения функции f будет продолжаться бесконечно, если: (1) значение $g(x_1, \dots, x_n, 0)$ не определено; (2) значения $g(x_1, \dots, x_n, y)$ определены для $y = 0, 1, \dots, b-1$, но отличны от x_{n+1} , а $g(x_1, \dots, x_n, b)$ не определено; (3) значения $g(x_1, \dots, x_n, y)$ определены для всех y , но отличны от x_{n+1} . Во всех этих случаях вычисления продолжаются бесконечно и значение функции $f(x_1, \dots, x_n)$ считается неопределенным. Таким образом, применение μ -оператора позволяет получить частично определенные функции, что и объясняет термин «частично рекурсивные» функции. Применение ограниченного μ -оператора позволяет остановить процесс вычислений, введя верхнюю границу перебора $y < z$, и доопределить функцию $f(x_1, \dots, x_n)$, присвоив ей некоторое произвольное значение, например, z .

μ -оператор является удобным средством для построения обратных функций. Если заданная функция g одноместна, то $f(x) = g^{-1}(x) = \mu y (g(y) = x)$. Для многоместных функций запись g^{-1} не употребляется.

✱ Примеры.

1. Для функции $sg(x)$ обратную функцию можно определить как $sg^{-1}(x) = \mu x (sg(x) = 1)$. Тогда $sg^{-1}(x) = x$, если $x = 0, 1$, и $sg^{-1}(x)$ не определено, если $x > 1$.
2. Определим функцию $y = [z/x]$ (частное от деления z на x) как функцию, обратную умножению: $z = y \cdot x$. Тогда $y = \mu_{y \leq z} (|y \cdot x - z| = 0)$, т.е. это будет наименьшее значение y , при котором существует решение уравнения $|y \cdot x - z| = 0$. Функция не полностью определена, так как не каждые два числа делятся друг на друга без остатка.
3. Функция $y = [\sqrt{x}]$ (целая часть \sqrt{x}) может быть определена с помощью ограниченного μ -оператора как $y = \mu_{y \leq x} (y^2 = x)$. Эта функция также является частично определенной.

Теорема 14.5. Если f — примитивно рекурсивная (или рекурсивная) функция, то ограниченные суммы и произведения этой функции являются также примитивно рекурсивными (или рекурсивными) функциями.

Доказательство.

Пусть $g(x_1, \dots, x_n, z) = \sum_{y < z} f(x_1, \dots, x_n, y)$.

Тогда можно записать рекурсивное определение:

$$g(x_1, \dots, x_n, 0) = 0,$$

$$g(x_1, \dots, x_n, z + 1) = g(x_1, \dots, x_n, z) + f(x_1, \dots, x_n, z).$$

Если $h(x_1, \dots, x_n, z) = \sum_{y \leq z} f(x_1, \dots, x_n, y)$, то имеем в результате подстановки: $h(x_1, \dots, x_n, z) = g(x_1, \dots, x_n, z + 1)$.

Аналогично можно получить соответствующие выражения для сумм и произведений, ограниченных с двух сторон.

14.3.3. Рекурсивные отношения

↪ **Определение 14.9.** *Характеристической функцией* отношения $R(x_1, \dots, x_n)$ называется функция $C_R(x_1, \dots, x_n)$, задаваемая условиями:

$$C_R(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } R(x_1, \dots, x_n) = T \\ 1, & \text{если } R(x_1, \dots, x_n) = F \end{cases}$$

↪ **Определение 14.10.** Отношение $R(x_1, \dots, x_n)$ называется *примитивно рекурсивным* (рекурсивным) отношением, если примитивно рекурсивной (соответственно рекурсивной) является его характеристическая функция $C_R(x_1, \dots, x_n)$.

Поскольку каждому отношению можно поставить в соответствие предикат, это определение является также определением примитивно рекурсивного (рекурсивного) предиката.

✱ Примеры.

1. Отношение $x_1 = x_2$ примитивно рекурсивно, так как его характеристическая функция совпадает с функцией $sg(|x_1 - x_2|)$, которая примитивно рекурсивна, в силу предложений (f), (g) теоремы 14.4.
2. Примитивно рекурсивная функция $unsg(x_2 \div x_1)$ служит характеристической функцией отношения $x_1 < x_2$, которое, таким образом, примитивно рекурсивно.
3. Отношение $x_1 | x_2$ (x_1 делится на x_2 без остатка) примитивно рекурсивно, так как его характеристической функцией является примитивно рекурсивная функция $sg(rm(x_1, x_2))$.
4. Отношение $Pr(x)$, т.е. « x есть простое число», примитивно рекурсивно, так как $C_{Pr}(x) = sg((D(x) \div 2) + unsg(|x - 1| + unsg(|x - 0|)))$, где функция $D(x)$ равна 1, если $x = 0$, и числу делителей x , если

$x > 0$. Функция $D(x)$ примитивно рекурсивна, так как $D(x) = \sum_{y < x} \text{unsg}(rm(y, x))$.

Теорема 14.6. Отношения, которые можно получить из примитивно рекурсивных (или рекурсивных) с помощью пропозициональных связок и ограниченных кванторов, также примитивно рекурсивны (соответственно, рекурсивны); применение ограниченных μ -операторов $\mu_{y < z}$ или $\mu_{y \leq z}$ к примитивно рекурсивным (рекурсивным) отношениям приводит к примитивно рекурсивным (рекурсивным) функциям.

Доказательство.

Пусть отношения $P(x_1, \dots, x_n)$ и $Q(x_1, \dots, x_n)$ примитивно рекурсивны (рекурсивны). Это означает, что примитивно рекурсивными (рекурсивными) являются их характеристические функции C_P и C_Q . Тогда примитивно рекурсивными (рекурсивными) являются и отношения: $\neg P(x_1, \dots, x_n)$ (его характеристическая функция: $C_{\neg P} = 1 \div C_P$), $P(x_1, \dots, x_n) \vee Q(x_1, \dots, x_n)$ (характеристическая функция: $C_{P \vee Q} = C_P \cdot C_Q$), $P(x_1, \dots, x_n) \& Q(x_1, \dots, x_n)$ (характеристическая функция: $C_{P \& Q} = \text{sg}(C_P + C_Q)$). Отсюда нетрудно получить характеристические функции для формул: $R1 = \forall y_{y < z} P(x_1, \dots, x_n, y)$ и $R2 = \exists y_{y < z} P(x_1, \dots, x_n, y)$ с помощью ограниченной суммы и ограниченного произведения: $C_{R1} = \text{sg}(\sum_{y < z} C_P(x_1, \dots, x_n, y))$ и $C_{R2} = \prod_{y < z} C_P(x_1, \dots, x_n, y)$.

Покажем теперь, что применение ограниченного μ -оператора к примитивно рекурсивному (рекурсивному) отношению приводит к примитивно рекурсивной (рекурсивной) функции.

Функция $\prod_{u \leq z} C_P(x_1, \dots, x_n, u) = 1$ при каждом u , для которого $P(x_1, \dots, x_n, u)$ ложно при всех $u \leq y$, и принимает значение 0 всякий раз, когда существует такое $u \leq y$, при котором $P(x_1, \dots, x_n, u)$ истинно (по определению характеристической функции). Поэтому, если для данного z существуют числа y меньше, чем z , и такие, что $P(x_1, \dots, x_n, y)$ истинно, то значение функции $\sum_{y < z} \prod_{u \leq y} C_P(x_1, \dots, x_n, u)$ равно числу целых неотрицательных чисел, меньших, чем наименьшее из таких чисел y . В противном случае значение функции $\sum_{y < z} \prod_{u \leq y} C_P(x_1, \dots, x_n, u)$ равно z . Но это значит, что $\sum_{y < z} \prod_{u \leq y} C_P(x_1, \dots, x_n, u) = \mu_{y < z} P(x_1, \dots, x_n, y)$, т.е. функция, полученная в результате применения ограниченного μ -оператора, является примитивно рекурсивной (рекурсивной).

14.3.4. Арифметические функции и отношения в теории S

Рассмотрим выразительные возможности теории S . Термы $0, 0', 0'', 0''', \dots$ в дальнейшем будем называть *цифрами* и обозначать жирными символами **0, 1, 2, 3, ...**, и для любого целого неотрицательного числа n соответствующую цифру будем обозначать через ***n***.

↪ **Определение 14.11.** Арифметическое отношение $R(x_1, \dots, x_n)$ называется *выразимым* в теории S , если существует формула $A(x_1, \dots, x_n)$ теории S с n свободными переменными такая, что для любых натуральных чисел k_1, \dots, k_n :

- (1) если $R(k_1, \dots, k_n)$ истинно, то $\vdash_S A(\mathbf{k}_1, \dots, \mathbf{k}_n)$,
- (2) если $R(k_1, \dots, k_n)$ ложно, то $\vdash_S \neg A(\mathbf{k}_1, \dots, \mathbf{k}_n)$.

Так, например, отношение равенства между натуральными числами выразимо в S формулой $x_1 = x_2$. В самом деле, если $k_1 = k_2$, то термы \mathbf{k}_1 и \mathbf{k}_2 совпадают, и тогда $\vdash_S \mathbf{k}_1 = \mathbf{k}_2$. Аналогично, если $k_1 \neq k_2$, то $\vdash_S \mathbf{k}_1 \neq \mathbf{k}_2$. В свою очередь, формулой $x_1 < x_2$ выразимо в S отношение «меньше». Если $k_1 < k_2$, то существует отличное от нуля число n , такое что $k_2 = k_1 + n$, и тогда $\vdash_S \mathbf{k}_2 = \mathbf{k}_1 + \mathbf{n}$, а в силу (S3) и $n \neq 0$, $\vdash_S \mathbf{n} \neq 0$. Следовательно, в S можно вывести формулу $\exists \omega(\mathbf{k}_2 = \mathbf{k}_1 + \omega \& \omega \neq 0)$, т.е. $\mathbf{k}_1 < \mathbf{k}_2$. Если же $\neg(k_1 < k_2)$, то $k_1 = k_2$ или $k_2 < k_1$, причем в этом последнем случае, так же, как и для случая $k_1 < k_2$, доказывается $\vdash_S \mathbf{k}_2 < \mathbf{k}_1$. Наконец, если $k_1 = k_2$, то $\vdash_S \mathbf{k}_1 = \mathbf{k}_2$. Итак, в обоих случаях $\vdash_S \mathbf{k}_2 \leq \mathbf{k}_1$ и тогда, $\vdash_S \neg(\mathbf{k}_1 < \mathbf{k}_2)$.

Будем обозначать $\exists_1 x A(x)$ высказывание: «существует единственное x , такое, что $A(x)$ истинно».

↪ **Определение 14.12.** Арифметическая функция $f(x_1, \dots, x_n)$ называется *представимой* в S , если существует формула $A(x_1, \dots, x_{n+1})$ теории S со свободными переменными x_1, \dots, x_{n+1} такая, что для любых натуральных чисел k_1, \dots, k_{n+1} :

- (1) если $f(k_1, \dots, k_n) = k_{n+1}$, то $\vdash_S A(\mathbf{k}_1, \dots, \mathbf{k}_n, \mathbf{k}_{n+1})$,
- (2) $\vdash_S \exists_1 x_{n+1} A(\mathbf{k}_1, \dots, \mathbf{k}_n, x_{n+1})$.

Если в этом определении условие (2) заменить условием

$$(2') \vdash_S \exists_1 x_{n+1} A(x_1, \dots, x_n, x_{n+1}),$$

то мы получим определение *сильно представимой* в S функции. Заметим, что, в силу правил Gen и A4 из (2'), следует (2). Следовательно, всякая сильно представимая функция является также представимой функцией.

★ Примеры.

1. Нуль-функция $Z(x) = 0$ сильно представима в S с помощью формулы $x_1 = x_1 \& x_2 = 0$. В самом деле, если $Z(k_1) = k_2$, то $k_2 = 0$ и $\vdash_S \mathbf{k}_1 = \mathbf{k}_1 \& 0 = 0$ т.е. выполнен пункт (1) определения сильно представимой функции. Кроме того, очевидно $\vdash_S \exists_1 x_2 (x_1 = x_1 \& x_2 = 0)$, т.е. выполнен и пункт (2') этого определения.

2. Функция $N(x) = x + 1$ сильно представима в S формулой $x_2 = x_1'$. Действительно, при любом k_1 из $N(k_1) = k_2$, т.е. из $k_2 = k_1 + 1$, следует, что термы \mathbf{k}_2 и $(\mathbf{k}_1)'$ совпадают и потому $\vdash_S \mathbf{k}_2 = (\mathbf{k}_1)'$. Кроме того, $\vdash_S \exists_1 x_2 (x_2 = x_1')$.

3. Проектирующая функция $U_i^n(x_1, \dots, x_n) = x_i$ сильно представима в S с помощью формулы $x_1 = x_1 \& \dots \& x_n = x_n \& x_{n+1} = x_i$. Если $U_i^n(k_1, \dots, k_n) = k_{n+1}$, то $k_{n+1} = k_i$ и $k_{n+1} = k_i$. Следовательно, $\vdash k_1 = k_1 \& \dots \& k_n = k_n \& k_{n+1} = k_i$ и условие (1) выполнено. Кроме того, $\vdash \exists x_{n+1}(x_1 = x_1 \& \dots \& x_n = x_n \& x_{n+1} = x_i)$, т.е. выполнено и условие (2') определения сильно представимой в S функции.

4. Предположим, что функции $g(x_1, \dots, x_m), h(x_1, \dots, x_n), h_m(x_1, \dots, x_n)$ (сильно) представимы в S соответственно формулами $B(x_1, \dots, x_m, x_{m+1}), A_1(x_1, \dots, x_{n+1}), \dots, A_m(x_1, \dots, x_{n+1})$. Зададим новую функцию f равенством $f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$, т.е. функция f получена из g, h_1, \dots, h_m с помощью *подстановки*. Функция f также (сильно) представима в S , например, с помощью формулы

$$\exists y_1 \dots \exists y_m (A_1(x_1, \dots, x_n, y_1) \& \dots \& A_m(x_1, \dots, x_n, y_m) \& B(y_1, \dots, y_m, x_{n+1})).$$

Теорема 14.7. Если отношение $R(x_1, \dots, x_n)$ выразимо в S , то характеристическая функция $C_R(x_1, \dots, x_n)$ этого отношения сильно представима в S , а если функция $C_R(x_1, \dots, x_n)$ представима в S , то в S выразимо и отношение $R(x_1, \dots, x_n)$.

Доказательство. Не составляет труда проверить, что:

1) если отношение $R(x_1, \dots, x_n)$ выразимо в S с помощью формулы $A(x_1, \dots, x_n)$, то функция $C_R(x_1, \dots, x_n)$ сильно представима в S с помощью формулы

$$(A(x_1, \dots, x_n) \& x_{n+1} = 0) \vee (\neg A(x_1, \dots, x_n) \& x_{n+1} = 1), \text{ и}$$

2) если функция $C_R(x_1, \dots, x_n)$ представима в S с помощью формулы $B(x_1, \dots, x_n, x_{n+1})$, то отношение $R(x_1, \dots, x_n)$ выразимо в S с помощью формулы $B(x_1, \dots, x_n, 0)$.

Теорема 14.8. Всякая рекурсивная функция представима в S .

Доказательство.

Исходные функции Z, N, U_i^n представимы в S , согласно примерам 1–3. В силу примера 4, правило подстановки (IV) не выводит за пределы класса представимых функций. Доказательство для правила рекурсии и μ -оператора см. [Мендельсон Э., стр. 147–150].

Следствие. Всякое рекурсивное отношение выразимо в S .

Доказательство.

Пусть $R(x_1, \dots, x_n)$ — рекурсивный предикат. Характеристическая функция C_R этого предиката рекурсивна. В силу теоремы 14.8, функция C_R представима в S и, следовательно, в силу теоремы 14.7, предикат R выразим в S .

Теорема 14.9. Всякая функция $f(x_1, \dots, x_n, z)$, представимая в S , рекурсивна.

Теорема 14.9 вместе с теоремой 14.8 показывает, что класс рекурсивных функций совпадает с классом функций, представимых в S .

Следствие. Всякий заданный на множестве натуральных чисел предикат $R(x_1, \dots, x_n)$ рекурсивен тогда и только тогда, когда он выразим в теории S .

Доказательство.

Согласно определению, предикат $R(x_1, \dots, x_n)$ рекурсивен тогда и только тогда, когда рекурсивна функция C_R . С другой стороны, предикат R выразим в S тогда и только тогда, когда функция C_R представима в S (теорема 14.7).

14.4. Гёделева нумерация

Гёдель предложил способ кодирования символов и выражений любой формальной теории так, что каждому символу, выражению и последовательности выражений однозначно соответствует некоторое натуральное число. Это способ кодирования получил название «гёделева нумерации». Рассмотрим его.

Каждому символу u произвольной теории первого порядка K следующим образом поставим в соответствие положительное число $g(u)$, называемое *гёделевым номером* символа u :

$$\begin{aligned} g(() &= 3; \\ g() &= 5; \\ g(.) &= 7; \\ g(\neg) &= 9; \\ g(\rightarrow) &= 11; \\ g(x_k) &= 5 + 8k \text{ для } k = 1, 2, \dots; \\ g(a_k) &= 7 + 8k \text{ для } k = 1, 2, \dots; \\ g(f_k^n) &= 9 + 8(2^n 3^k) \text{ для } k, n \geq 1; \\ g(A_k^n) &= 11 + 8(2^n 3^k) \text{ для } k, n \geq 1; \end{aligned}$$

при этом положим $g(\forall x_i) = g((x_i))$.

Таким образом, различным символам поставлены в соответствие различные гёделевы номера, являющиеся положительными числами. Например, $g(x_2) = 21, g(a_4) = 39, g(f_1^2) = 105, g(A_2^1) = 155$.

Пусть дано выражение $u_0 u_1 \dots u_r$, представляющее, например, формулу теории первого порядка. Гёделев номер $g(u_0 u_1 \dots u_r)$ этого выражения определим как $2^{g(u_0)} 3^{g(u_1)} \dots p_r^{g(u_r)}$, где p_i есть i -е простое число и $p_0 = 2$. Например, $g(A_1 \rightarrow (A_2 \rightarrow A_1)) = 2^{g(A_1)} 3^{g(\rightarrow)} 5^{g(A_2)} 11^{g(\rightarrow)} 13^{g(A_1)} 17^{g(A_1)}$. Заметим, что, в силу единственности разложения натуральных чисел в произведения степеней простых чисел, различные выражения получают при этом разные гёделевы номера. Кроме того, гёделевы номера выражений

четны и потому отличны от гёделевых номеров символов. (Всякий символ можно рассматривать как выражение, и тогда он снабжается гёделевым номером, отличным от того, который ставится ему в соответствие как символу. Это не должно, однако, приводить к недоразумению.)

Наконец, гёделев номер произвольной последовательности e_0, \dots, e_r выражений (например, вывода формулы e_r в теории K) определим следующим образом: $g(e_0, \dots, e_r) = 2^{g(e_0)} \dots 3^{g(e_1)} \dots p_r^{g(e_r)}$. Как и прежде, различные последовательности выражений имеют различные гёделевы номера, а так как эти последние четны и, кроме того, имеют четный показатель степени при 2, то они отличны и от гёделевых номеров символов, и от гёделевых номеров выражений.

Таким образом, функция g взаимно однозначно отображает множество всех символов, выражений и конечных последовательностей выражений в множество целых положительных чисел. Множество значений функции g не совпадает, однако, с множеством всех целых положительных чисел, так как не все числа являются гёделевыми номерами, например, число 12 не является гёделевым номером.

Такая нумерация символов, выражений и последовательностей выражений была предложена Гёделем в 1931 г. с целью *арифметизации* математики, т.е. с целью замены утверждений о формальной системе эквивалентными высказываниями о натуральных числах с последующим выражением этих высказываний в формальной системе. Поскольку каждому выражению исчисления приписан гёделев номер, то каждое метаматематическое высказывание о выражениях исчисления и отношениях между ними можно выразить как высказывание о соответствующих гёделевых номерах и отношениях между ними. Таким образом метаматематика оказывается полностью «арифметизированной», и язык арифметики становится языком метаматематики. Изучение метаматематических вопросов сводится к изучению соотношений и свойств некоторых чисел.

14.5. Теорема Гёделя о неполноте

Детали доказательства знаменитой теоремы Гёделя довольно сложны, поэтому мы опустим доказательства некоторых предварительных утверждений. (С полным доказательством можно ознакомиться в [Мендельсон, 1976]).

Пусть для данной теории первого порядка K следующие отношения примитивно рекурсивны (рекурсивны):

(а) $IC(x)$, что означает « x есть гёделев номер предметной константы теории K »,

(б) $FL(x)$, что означает « x есть гёделев номер функциональной буквы теории K »,

(с) $PL(x)$, что означает « x есть гёделев номер предикатной буквы теории K ».

Тогда, на основе этих отношений можно определить новые отношения и функции, так что эти отношения будут определять высказывания относительно выражений и операций формальной теории S , причем эти отношения и функции также будут примитивно рекурсивны (рекурсивны). Здесь мы рассмотрим (без доказательства) только одно отношение, которое, как можно показать, является примитивно рекурсивным: $W(u, y)$: « u есть гёделев номер формулы $A(x_1)$, содержащей свободную переменную x_1 , и y есть гёделев номер вывода в S формулы $A(u)$ ».

Введем еще дополнительное понятие непротиворечивости формальной теории.

↪ **Определение 14.13.** Пусть K — теория первого порядка с теми же самыми символами, что и S . Теория K называется ω -непротиворечивой, если для всякой формулы $A(x)$ этой теории из того, что при любом $n \vdash_K A(n)$, следует невозможность $\vdash_K \exists x \neg A(x)$.

Очевидно, что если принять стандартную интерпретацию теории S в качестве модели этой теории, то тогда теорию S следует признать ω -непротиворечивой.

Теорема 14.10. Если теория K ω -непротиворечива, то она непротиворечива.

Доказательство.

Пусть теория K ω -непротиворечива. Рассмотрим какую-нибудь выводимую в K формулу $A(x)$ со свободной переменной, например $x = x \rightarrow x = x$. При любом n имеем $\vdash_K n = n \rightarrow n = n$. Поэтому формула $\exists x \neg(x = x \rightarrow x = x)$ не выводима в K . Следовательно, теория K непротиворечива (ибо, в силу тавтологии $\neg A \rightarrow (A \rightarrow B)$, из противоречивости K следовала бы выводимость в K любой формулы). ∞

Перейдем к формулировке теоремы Гёделя. Рассмотрим отношение $W(u, y)$.

Отношение $W(u, y)$ примитивно рекурсивно и потому выразимо в S некоторой формулой $W(x_1, x_2)$ с двумя свободными переменными x_1, x_2 . Это значит, что если $W(k_1, k_2)$ истинно, то $\vdash_S W(k_1, k_2)$, и если $W(k_1, k_2)$ ложно, то $\vdash_S \neg W(k_1, k_2)$. Рассмотрим теперь формулу

$$\forall x_2 \neg W(x_1, x_2). \quad (*)$$

Это формула с одной свободной переменной x_1 . Пусть m есть гёделев номер формулы $(*)$. Подставив в $(*)$ m вместо свободной переменной x_1 , мы получим замкнутую формулу

$$\forall x_2 \neg W(m, x_2). \quad (G)$$

Вспомним, что утверждение $W(u, y)$ истинно тогда и только тогда, когда u есть гёделев номер некоторой формулы $A(x_1)$, содержащей свободную переменную x_1 , а y есть гёделев номер вывода в S формулы $A(u)$. Следовательно,

(I) $W(m, x_2)$ истинно тогда и только тогда, когда x_2 есть гёделев номер вывода в S формулы G .

Теорема 14.11. (Теорема Гёделя для теории S).

- (1) Если теория S непротиворечива, то формула G невыводима в S .
- (2) Если теория S ω -непротиворечива, то формула $\neg G$ невыводима в S .

(Таким образом, в силу теоремы 14.10, если теория S ω -непротиворечива, то замкнутая формула G невыводима и неопровержима в S . Замкнутые формулы, обладающие таким свойством, называются *неразрешимыми предложениями* теории S .)

Доказательство.

(1) Предположим, что теория S непротиворечива и $\vdash_S \forall x_2 \neg W(m, x_2)$. Пусть тогда k — гёделев номер какого-нибудь вывода в S этой последней формулы. В силу предложения (I), справедливо $W(m, k)$. Так как W выражает W в S , то $\vdash_S W(m, k)$. Из $\forall x_2 \neg W(m, x_2)$ по правилу A4 (универсальной конкретизации) мы можем вывести $\neg W(m, k)$. Таким образом, в S оказываются выводимыми формулы $W(m, k)$ и $\neg W(m, k)$, что противоречит предположению о непротиворечивости S . \simeq

(2) Предположим, что теория S ω -непротиворечива и $\vdash_S \neg \forall x_2 \neg W(m, x_2)$, т.е. $\vdash_S \neg G$. На основании теоремы 14.10, заключаем, что теория S непротиворечива и, следовательно, не $\vdash_S G$. Поэтому, каково бы ни было натуральное число n , n не есть гёделев номер вывода в S формулы G , т.е. $W(m, n)$ ложно для любого n . А это значит, что $\vdash_S \neg W(m, n)$ для любого n . Взяв в качестве формулы $A(x_2)$ формулу $\neg W(m, x_2)$, мы, на основании предположения об ω -непротиворечивости теории S , заключаем, что не $\vdash_S \exists x_2 \neg \neg W(m, x_2)$ и, следовательно, не $\vdash_S \exists x_2 W(m, x_2)$. Мы пришли, таким образом, к противоречию с предположением, что $\vdash_S \exists x_2 W(m, x_2)$. \simeq

Рассмотрим стандартную интерпретацию неразрешимого предложения G : $\forall x_2 \neg W(m, x_2)$. Так как W выражает в S отношение W , то, в соответствии со стандартной интерпретацией, G утверждает, что $W(m, x_2)$ ложно для каждого натурального числа x_2 . Согласно (I), это означает, что не существует вывода формулы G в S . Другими словами, *формула G утверждает свою собственную невыводимость в S* . По теореме же Гёделя, если только теория S

непротиворечива, эта формула и в самом деле невыводима в S и потому истинна при стандартной интерпретации.

Итак, для натуральных чисел, соответствующих обычной интерпретации, формула G верна, но в S невыводима. Это означает, что в содержательной арифметике (в стандартной интерпретации теории S) существует истинное утверждение, которому, однако, не соответствует никакая теорема теории S . Таким образом, теория S неполна.

Может показаться, что теорема Гёделя потому справедлива для теории S , что первоначально выбранная для этой теории система аксиом оказалась слишком слабой и что, если бы мы усилили теорию S , добавив к ней новые аксиомы, то новая теория могла бы оказаться полной. Так, например, чтобы получить некоторую более сильную теорию S_1 , мы могли бы добавить к S истинную формулу G . Однако всякая рекурсивная функция, будучи представимой в S , представима также и в такой теории S_1 . Точно так же и теоремы 14.6, 14.7, 14.8 остаются, очевидно, в силе, если их переформулировать для S_1 . Но это и есть все, что требуется для того, чтобы получить результат Гёделя; и потому, если теория S_1 ω -непротиворечива, то и она имеет некоторое неразрешимое предложение B . (B имеет ту же форму $\forall x_2 \neg (W)_{S_1}(k, x_2)$, но, разумеется, будет отличаться от G , поскольку отношение W для S_1 отлично от отношения W для S , и, следовательно, формула $(W)_{S_1}$, и входящая в B цифра k отличны от формулы W и цифры m в G .) Таким образом, добавление формулы G к аксиомам теории S не делает эту теорию полной, т.е. теория S является не только неполной, но и неполнополной.

14.6. Вторая теорема Гёделя

Определим $Neg(x)$ так, что если x есть гёделев номер формулы A , то $Neg(x)$ есть гёделев номер формулы $\neg A$. Функция Neg , очевидно, рекурсивна и, следовательно, представима в S некоторой формулой $Neg(x_1, x_2)$. Введем предикат $Pf(y, x)$, истинный тогда и только тогда, когда x есть гёделев номер некоторой формулы A теории S , а y есть гёделев номер некоторого вывода A в S . Предикат Pf примитивно рекурсивен, и потому выразим в S с помощью некоторой формулы $Pf(x_1, x_2)$.

Обозначим через Con_S формулу:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \neg (Pf(x_1, x_3) \& Pf(x_2, x_4) \& Neg(x_3, x_4)).$$

Содержательно, т.е. в соответствии со стандартной интерпретацией, Con_S выражает невозможность вывода в S какой-либо формулы вместе с ее отрицанием и является истинной в том и только том случае, когда теория S непротиворечива. Иными словами, формулу Con_S можно интерпретировать как утверждение о

непротиворечивости теории S . Вспомним теперь, что, в соответствии со стандартной интерпретацией, гёделева неразрешимая формула G содержательно выражает свою собственную невыводимость. Тогда формула $Con_S \rightarrow G$ содержательно утверждает, что если теория S непротиворечива, то формула G в ней невыводима. Но в этом и состоит первая часть теоремы Гёделя.

Математические рассуждения, доказывающие теорему Гёделя, могут быть выражены и проведены средствами теории S , так что в результате оказывается возможным получить вывод формулы $Con_S \rightarrow G$ в теории S . (Доказательство этого утверждения см. в [Гильберт, Бернайс, 1979]). Итак, $\vdash_S Con_S \rightarrow G$. Предположим, что $\vdash_S Con_S$, т.е. средствами теории S можно доказать непротиворечивость S . Тогда по правилу МР получим $\vdash_S G$. Согласно теореме Гёделя, однако, если теория S непротиворечива, то формула G в ней невыводима. Отсюда следует, что если теория S непротиворечива, то в ней невыводима и формула Con_S . Иными словами, *если теория непротиворечива, то в ней невыводима некоторая формула, содержательно утверждающая непротиворечивость теории S* .

Этот результат носит название *второй теоремы Гёделя*. Грубо говоря, эта теорема утверждает, что если теория S непротиворечива, то доказательство непротиворечивости теории не может быть проведено средствами самой теории S , т.е. всякое такое доказательство обязательно должно использовать невыразимые в S идеи или методы. Примерами могут служить доказательства непротиворечивости теории S , предложенные Генценом в 1936, 1938 г.г. и Шютте в 1951 г., в которых применяются понятия и методы (например, один фрагмент теории счетных порядковых чисел), очевидно, не формализуемые средствами теории S .

Глава 15.

ТЕОРИЯ АЛГОРИТМОВ

15.1. Интуитивное понятие алгоритма

Функция $f(x_1, \dots, x_n)$ называется эффективно вычислимой, если для каждого набора аргументов a_1, \dots, a_n из ее области определения может быть вычислено значение функции $f(a_1, \dots, a_n)$. Если функция эффективно вычислима, то говорят, что существует *алгоритм* ее вычисления.

Понятие алгоритма интуитивно ясно и часто используется в математике. Сложение и умножение чисел «столбиком», которое известно еще со школы, формула нахождения корней квадратного уравнения, перемножение двух матриц по правилу «строка на столбец» являются алгоритмами. Множество примеров можно продолжить. В современной практике под алгоритмом часто понимают программу, а критерием существования алгоритма считают возможность его запрограммировать. Однако это не совсем так. Сначала дадим *понятие* алгоритма.

Под алгоритмом понимают точное предписание о выполнении в определенном порядке точно указанной последовательности операций для решения всех задач из данного класса задач.

Приведенное выше понятие алгоритма не является точным математическим определением. Это понятие характеризуется набором свойств, присущих алгоритму.

15.1.1. Свойства алгоритма

- **Дискретность информации.** Каждый алгоритм имеет дело с данными – входными, промежуточными и выходными. Эти данные представляются в виде конечных слов в некотором алфавите.
- **Дискретность работы алгоритма.** Алгоритм выполняется по шагам и при этом на каждом шаге выполняется только одна операция.
- **Выполнимость операций.** В алгоритме не должно быть невыполнимых операций. Например, нельзя в программе присвоить переменной значение «бесконечность», – такая операция была бы невыполнимой. Каждая операция обрабатывает определенный участок в обрабатываемом слове.
- **Конечность алгоритма.** Конечность алгоритма означает, что описание алгоритма должно быть конечным.
- **Детерминированность алгоритма.** Каждый шаг алгоритма строго определен. После каждого шага точно указывается, какой шаг сделать дальше, либо указывается, что алгоритм должен закончить свою работу на данном шаге. К каждому участку слова на каждом шаге применима только одна операция.

• **Массовость алгоритма.** Массовость алгоритма означает, что алгоритм должен решать все задачи из данного класса задач. Если найдется хотя бы одна задача, для которой алгоритм неприменим, то эту последовательность операций нельзя считать алгоритмом для решения данного класса задач.

15.2. Алфавиты и слова

15.2.1. Основные понятия

↪ **Определение 15.1.** Будем называть произвольное конечное множество A *алфавитом*, а элементы этого множества — *буквами* алфавита A . Тогда произвольные конечные последовательности букв называются *словами* в данном алфавите.

Здесь и далее для удобства чтения будем обозначать: буквы-константы — малыми начальными символами латинского алфавита (a, b, c, \dots), буквы-переменные — последними латинскими символами (x, y, z, \dots), алфавиты и множества — большими начальными символами латинского алфавита (A, B, C, \dots), слова — большими символами латинского алфавита (P, Q, R, \dots). Греческие символы будут использоваться для обозначения выделенных букв заданного алфавита, отличных от букв-констант и букв-переменных. Любой алфавит содержит пустой символ. Будем обозначать его символом Λ . Пустой символ является и пустым словом. Множество слов алфавита A будем обозначать A^* .

↪ **Определение 15.2.** Количество букв в слове называется его *длиной* и обозначается вертикальными скобками. Например, длина слова $aaaa$ равна $|aaaa| = 4$, длина пустого слова $|\Lambda| = 0$.

Основной операцией над словами является *конкатенация*.

↪ **Определение 15.3.** *Конкатенацией* двух слов P и Q назовем слово PQ , полученное дописыванием слова Q после P .

Например, конкатенация слов aab и ba есть слово $aabba$. Операция конкатенации некоммутативна, но ассоциативна.

↪ **Определение 15.4.** Если X — некоторое слово алфавита A и если X представимо в виде конкатенации слов PQR , то P, Q, R называют *подсловами* слова X .

Например, слово acb содержит подслова a, b, c, ac, cb . Если $X \in A^*$ и $X = P_1QP_2QP_3$, то говорят о первом, втором и т. д. *вхождении* слова Q в слово X . Слова, составленные из последовательности одинаковых букв, иногда записываются в виде степени, например, $aaabbb = a^3b^2$, где степень обозначает количество вхождений буквы в слово.

15.2.2. Кодирование и нумерация

↪ **Определение 15.5.** Пусть даны два алфавита A и B . *Кодирование* слов алфавита A словами в алфавите B есть функция $\varphi(P)$, которая осуществляет отображение множества слов в алфавите A в множество слов в алфавите B : $\varphi(P): A^* \rightarrow B^*$, где $P \in A^*, \varphi(P) \in B^*$.

* **Пример.** Пусть $A = \{a, b\}$, $B = \{a, b, c\}$. Отображение $\varphi(P): P \rightarrow cPc$ определяет кодирование слов в алфавите A словами в алфавите B , например, $ab \rightarrow cabcs$.

↪ **Определение 15.6.** Кодирование называется *блочным*, если каждой букве алфавита A соответствует слово в алфавите B .

* **Пример.** Отображение $\varphi(a): a \rightarrow ac, \varphi(b): b \rightarrow bc$ является блочным кодированием. Например, $\varphi(ab) = acbc$.

Любые множества слов в некотором алфавите A можно упорядочить в лексикографическом порядке: если R_1xR_2, R_1yR_2 и $x < y$, $x, y \in A$, то $R_1xR_2 < R_1yR_2$. Например, лексикографическое упорядочение слов алфавита $A = \{a, b\}$ есть последовательность: $\Lambda, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa$, и т.д.

15.2.3. Словарные примитивно рекурсивные функции

Исходные функции для алфавита A :

1. Нуль-функция $O(P) = \Lambda$ преобразует любое слово в пустое.
2. Добавление символа x в конец слова: $N_x(P) = Px$, где $x \in A$.
3. Проектирующая функция $U_i^j(P) = x_i$, где j — количество букв в слове P , x_i — i -я буква слова P , — выделяет заданный символ в слове.

Подстановка. Функция f получена с помощью подстановки из функций $g(P_1, \dots, P_m), h_1(X_1, \dots, X_n), \dots, h_m(X_1, \dots, X_n)$, если $f(X_1, \dots, X_n) = g(h_1(X_1, \dots, X_n), \dots, h_m(X_1, \dots, X_n))$.

Схема примитивной рекурсии для алфавита A .

Пусть $g(X_1, \dots, X_n), h_1(X_1, \dots, X_{n+2}), h_2(X_1, \dots, X_{n+2})$, — некоторые функции. Тогда функция $f(X_1, \dots, X_{n+1})$ получена по схеме примитивной рекурсии, если

$$f(X_1, \dots, X_n, \Lambda) = g(X_1, \dots, X_n), \\ f(X_1, \dots, X_n, \xi) = h_1(X_1, \dots, X_n, \xi, f(X_1, \dots, X_{n+1})), \xi \in A.$$

Функции, полученные из исходных с помощью операций подстановки и примитивной рекурсии, являются примитивно рекурсивными.

* **Пример.** Обозначим операцию конкатенации $con(X_1, X_2)$, $X_1, X_2 \in A^*$, $A = \{a, b\}$, и покажем, что она является примитивно рекурсивной.

$$con(X_1, \Lambda) = X_1 = U_1^2(X_1, \Lambda) = X_1; \\ con(X_1X_2, a) = X_1X_2a = N_a(con(X_1, X_2)); \\ con(X_1X_2, b) = X_1X_2b = N_b(con(X_1, X_2)).$$

15.2.4. Ассоциативные исчисления

↪ **Определение 15.7.** Подстановка слова P вместо подслова Q в слове W означает замену Q на P в слове W . Подстановка обозначается: $P \rightarrow Q$. Подстановка $Q \rightarrow P$ называется обратной подстановкой. Подстановка $Q \rightarrow P$ неприменима к слову W , если W не содержит Q .

✱ **Пример.** Пусть дан алфавит $A = \{a, b\}$ и подстановка $ab \rightarrow ba$. Тогда результат последовательного выполнения этой подстановки над словом $ababbbab$ будет следующим: 1. $ababbbab$, 2. $baabbbab$, 3. $ababbbab$, 4. $bbaabbbab$, 5. $bbababab$, 6. $bbbaabab$, 7. $bbbabaab$, 8. $bbbbaaab$, 9. $bbbbaaba$, 10. $bbbbbaaa$, 11. $bbbbbaaa$.

↪ **Определение 15.8.** Совокупность всех слов алфавита A вместе с конечной системой допустимых подстановок называется *ассоциативным исчислением*.

Если слово R может быть преобразовано в слово S путем однократного применения допустимой подстановки, то и S может быть преобразовано в R применением обратной подстановки. В этом случае слова R и S называют *смежными* словами. Последовательность слов R_1, R_2, \dots, R_n , таких, что каждые два слова R_i, R_{i+1} смежны, называется *дедуктивной цепочкой*. Если существует дедуктивная цепочка от слова R к слову S , то существует и дедуктивная цепочка от S к R . В этом случае слова R и S называют эквивалентными и обозначают: $R \sim S$. Очевидно, что, если $R \sim S$, то $S \sim R$.

Основной проблемой ассоциативных исчислений является *проблема эквивалентности слов*: для любых двух слов R и S в ассоциативном исчислении определить, существует ли дедуктивная цепочка от R к S , или нет. В дальнейшем мы покажем, что эта проблема для произвольного ассоциативного исчисления алгоритмически неразрешима.

15.3. Машина Тьюринга

15.3.1. Определение машины Тьюринга

Машина Тьюринга была первой алгоритмической схемой, предложенной Тьюрингом в качестве математического определения алгоритма в 1937 г. Машина Тьюринга является гипотетической машиной: Тьюринг не ставил задачи сконструировать это устройство. Концепция вычислительной машины принадлежит фон Нейману, но ее основой послужила машина Тьюринга. Задача машины Тьюринга — перерабатывать входное слово W в алфавите A в некоторое выходное слово W^* . Таким образом, машина Тьюринга является знакоперерабатывающим устройством.

Машина Тьюринга состоит из трех частей.

1). Внешняя память машины Тьюринга представляется как бесконечная в обе стороны лента, разбитая на ячейки. Конечное множество знаков $A = \{a, b, c, \dots\}$ образует *внешний алфавит* машины. В каждой ячейке может находиться один (и только один) символ внешнего алфавита. Информация записывается на ленте в виде слова в алфавите A . Внешний алфавит содержит и пустой символ Λ . Считается, что каждая ячейка ленты хранит пустой символ, если в ней не записан никакой другой символ. Если на ленте записано слово, то оно ограничено слева и справа пустыми символами.

2). Считывающая головка машины Тьюринга в один дискретный момент времени обозревает одну ячейку и может находиться в одном из внутренних состояний $q_i \in Q$, где Q — алфавит внутренних состояний. Считывающая головка распознает записанный в ячейке символ внешнего алфавита, записывает вместо него другой символ (возможно, тот же самый), переходит в другое состояние (возможно — в прежнее), после чего сдвигается вправо, влево или остается на месте (см. рис. 15.1). Движение головки машины Тьюринга будем обозначать символами: П — вправо, Л — влево, Н — на месте.

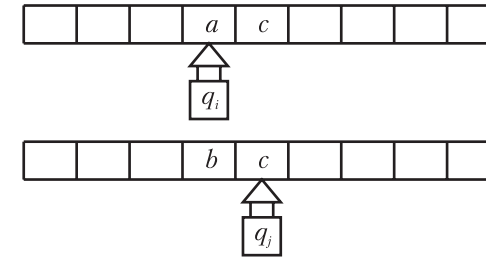


Рис. 15.1. Схема машины Тьюринга.

Множество внутренних состояний Q представляет собой внутреннюю память машины Тьюринга: когда машина в разных состояниях видит один и тот же самый символ, она может выполнить разные действия. Говорят, что в данный момент времени головка машины обозревает определенную ячейку ленты. Таким образом, в каждый дискретный момент времени состояние машины характеризуется словом, записанным на ленте, положением головки и ее состоянием. Слово, записанное на ленте, вместе с положением головки машины Тьюринга, находящейся в одном из своих внутренних состояний, будем называть *конфигурацией* машины Тьюринга.

3). Следующая часть машины Тьюринга — это программа, управляющая головкой и состоящая из команд вида:

$$aq_i \rightarrow bq_j\xi, \text{ где } \xi \in \{\text{П}, \text{Л}, \text{Н}\}, q_i, q_j \in Q, a, b \in A.$$

В результате выполнения этой команды символ a на ленте будет заменен символом b , головка сдвинется влево, вправо или останется на месте в зависимости от ξ и внутреннее состояние изменится с q_i на q_j . После этого будет выполняться следующая команда. Применимость той или иной команды определяется конфигурацией на ленте в текущий момент времени. Команда вида $aq_i \rightarrow bq!\xi$, где $q!$ (или просто «!») — *заключительное состояние*, называется заключительной командой и вызывает окончание (останов) работы машины Тьюринга. При выполнении заключительной команды символ a заменяется на символ b , головка сдвигается влево, вправо или остается на месте, и переходит в заключительное состояние.

Последовательность команд задает алгоритм переработки слова. Для работы алгоритма необходимо задать начальную конфигурацию: на ленту машины Тьюринга записывается исходное слово W в алфавите A и указывается, какой символ обозревает головка машины Тьюринга в начальном состоянии q_0 . Работа машины Тьюринга происходит по *тактам*, или по *шагам*. На каждом шаге выполняется одна команда, в результате которой конфигурация на ленте меняется. При работе машины Тьюринга возможно расширение внешнего алфавита A вспомогательными символами, которые после переработки слова заменяются символами алфавита A или стираются.

В процессе работы возможны две ситуации:

1. Машина Тьюринга перерабатывает исходное слово P в R и останавливается; тогда говорят, что данная машина *применима* к слову P .
2. Машина Тьюринга, начиная работу со слова P , никогда не остановится; тогда говорят, что данная машина Тьюринга *не применима* к слову P .

* Примеры.

1. Пусть задан алфавит $A = \{ |, * \}$, исходное слово в котором может иметь вид: $P = ||*|*||$. В начальном состоянии q_0 машина обозревает крайний левый символ. Машина Тьюринга должна преобразовать это слово в пустое слово, т.е. должна реализовывать алгоритм вычисления нуль-функции: $O(X) = \Lambda$. Для этого она должна, двигаясь слева направо, заменить каждый символ на ленте на пустой символ и остановиться, как только увидит крайний справа пустой символ (табл. 15.1).

Таблица 15.1.

$A \backslash Q$	q_0
$ $	$\Lambda q_0 \Pi$
$*$	$\Lambda q_0 \Pi$
Λ	$!$

Программу для машины Тьюринга обычно записывают в виде таблицы, строки которой помечаются символами внешнего алфавита, столбцы — символами алфавита состояний. Каждой строке и столбцу соответствует одна конфигурация на ленте (левая часть команды), в соответствующей

клетке записывается правая часть команды, указывающая, как должна измениться конфигурация на ленте. Некоторые конфигурации могут никогда не возникнуть в процессе переработки слова, тогда соответствующие им клетки остаются пустыми.

2. Рассмотрим программу для алгоритма добавления символа $|$ к слову в том же алфавите. Пусть исходное слово имеет вид: $P = ||$. Это слово можно рассматривать как число 3, а добавление символа $|$ — как вычисление функции $f(X) = X + 1$ в унарной системе счисления. Программа для вычисления этой функции на самом деле очень проста: головка машины пропускает все символы $|$, двигаясь слева направо, и, дойдя до крайнего правого пустого символа Λ , дописывает туда еще один символ $|$, после чего останавливается в своем заключительном состоянии (см. табл. 15.2).

Очевидно, что точно так же можно составить программу для добавления любого символа алфавита A в конце слова, т.е. такой алгоритм реализует исходную рекурсивную функцию $N_y(X) = Xu$, где $y \in A$.

Третья исходная функция: функция проекции $U_i^j(X) = x_j$ есть не что иное, как элементарное действие машины Тьюринга — распознавание символа.

3. Рассмотрим теперь вычисление более сложной функции: $F(X, Y) = X + Y$, где X, Y — слова, заданные в унарной системе счисления. Пусть исходная конфигурация на ленте задана так, что в начальном состоянии головка обозревает крайний левый символ $|$ (см. рис. 15.2), слово на ленте представляет собой два числа, разделенные символом $*$.

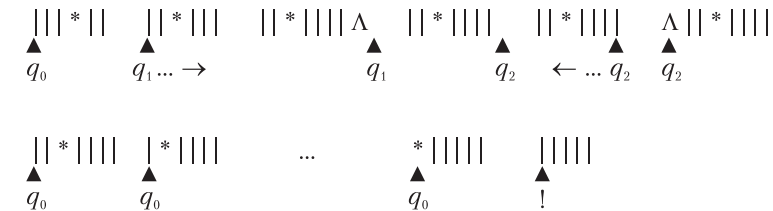


Рис. 15. 2. Вычисление функции $F(X, Y) = X + Y$

Составим машину Тьюринга, работающую по следующему алгоритму. В начальном состоянии q_0 машина видит крайнюю левую палочку, стирает ее и, перейдя в состояние q_1 , движется вправо, пока не увидит крайний справа пустой символ. Тогда на месте пустого символа машина записывает палочку, переходит в новое состояние q_2 и движется влево в том же состоянии q_2 , пропуская все символы, пока не дойдет до крайнего слева пустого символа.

Таблица 15.2.

	q_0
$ $	$ q_0 \Pi$
Λ	$! \Pi$

Тогда машина оставляет его на месте, сдвигается вправо и переходит в состояние q_0 . После этого процесс повторяется до тех пор, пока в состоянии q_0 машина не увидит символ $*$. Это означает, что уже все палочки перенесены слева направо, машина может стереть символ $*$ и остановиться, т.е. перейти в заключительное состояние. Программа для машины представлена в таблице 15.3.

Таблица 15.3.

	q_0	q_1	q_2
	$\Lambda q_1 \Pi$	$q_1 \Pi$	$q_2 \Pi$
*	$\Lambda ! \Pi$	* $q_1 \Pi$	* $q_2 \Pi$
Λ	$\Lambda ! \Pi$	$q_2 \Pi$	$\Lambda q_0 \Pi$

Нетрудно заметить, что процесс вычисления суммы рекурсивен: он основан на предыдущем алгоритме, когда к одному из слагаемых (в данном случае, к правому слову) добавляется столько единиц, сколько их содержится в другом слагаемом. Для сравнения воспроизведем процесс вычисления суммы двух слагаемых с помощью рекурсивной функции:

$$f(X, 0) = X,$$

$$f(X, Y + 1) = f(X, Y) + 1.$$

$$f(2, 3) = f(2, 2) + 1 = (f(2, 1) + 1) + 1 = ((f(2, 0) + 1) + 1) + 1.$$

На этом завершается прямой ход рекурсии: составлена рекурсивная схема вычисления функции. Теперь обратный ход рекурсии вычисляет ее значение: $((2 + 1) + 1) + 1 = (3 + 1) + 1 = 4 + 1 = 5$.

15.3.2. Распознающая машина Тьюринга

Распознающая машина Тьюринга – это машина, которая вычисляет предикат $P(W)$ таким образом, что если $P(W) = T$, то машина останавливается в состоянии «да!», а если $P(W) = F$, то в состоянии «нет!».

Таблица 15.4.

	q_0	q_1
	$q_1 \Pi$	$q_0 \Pi$
Λ	$\Lambda да!$	$\Lambda нет!$

Например, машина, распознающая четность числа, представленного в унарной системе счисления, приведена в таблице 15.4. Двигаясь слева направо, машина останавливается на пустом символе в состоянии «да!», если число

четное, и в состоянии «нет!», если нечетное.

15.3.3. Композиция машин Тьюринга

Можно выделить некоторый набор элементарных алгоритмов, из которых можно получать более сложные алгоритмы по правилам композиции машин Тьюринга. Можно показать, что элементарные функции:

- нуль-функция $O(X) = \Lambda$;
- добавление символа ζ : $N\zeta(X) = X\zeta$, где $\zeta \in A$;
- проектирующая функция $U_i^j(X) = x_j$;
- тождественное преобразование $T(X) = X$;
- алгоритм копирования слова $Copy(X) = X^*X$;
- заменяющий алгоритм $Rep_{x_i}^{x_j}(x)$, где $x_i, x_j \in A$ и B , и B – вспомогательный алфавит (алгоритм заменяет символ x_i на символ x_j в слове X), вычислимы на машине Тьюринга. Из этих элементарных алгоритмов можно образовывать более сложные с помощью композиции машин Тьюринга.

1. Последовательная композиция. Пусть M_1 и M_2 – две машины Тьюринга. Тогда, отождествив заключительное состояние машины M_1 с начальным состоянием машины M_2 и, при необходимости, перенумеровав внутренние состояния машины M_2 , получим новую машину Тьюринга, которая, начиная работу со слова W , сначала будет выполнять над ним преобразования, выполняемые машиной M_1 , а затем будет работать как машина M_2 . Последовательную композицию машин Тьюринга обозначим: $M_1 \circ M_2 = M_2(M_1(W))$. Таким образом, последовательная композиция машин Тьюринга осуществляет суперпозицию функций.

2. Параллельная композиция. Если на ленте записано слово W , которое представимо как конкатенация двух слов $P||R$, то можно составить такую машину Тьюринга, которая будет работать как машина M_1 над подсловом P и как машина M_2 над подсловом R , а затем осуществит конкатенацию результатов: $M_1(P)||M_2(R)$.

3. Разветвляющаяся композиция. Если существуют машины Тьюринга M_1 и M_2 и распознающая машина Тьюринга P , то можно составить такую машину Тьюринга M , что, начиная работу со слова W , машина Тьюринга работает сначала как распознающая машина $P(W)$. Если она заканчивает обработку исходного слова в состоянии «да!», то далее работает машина $M_1(W)$, а если в состоянии «нет!», то машина $M_2(W)$ (см. рис. 15.3).

4. Циклическая композиция. Можно построить такую машину Тьюринга M , которая, начиная работу со слова W_0 , сначала работает как распознающая машина P , вычисляющая предикат $P(W_0)$. Если она завершает свою работу в состоянии «да», то далее она работает как машина Тьюринга M_1 над словом W_0 и завершает свою работу с выходным словом W_1 . Затем управление передается распознающей машине P , вычисляющей предикат $P(W_1)$, и так далее, до тех пор, пока распознающая машина Тьюринга P не остановится в состоянии «нет» на слове W_k . Тогда машина Тьюринга M останавливается в своем заключительном состоянии (см. рис. 15.4).

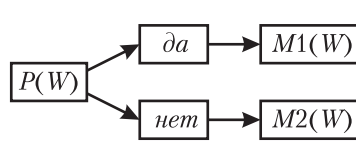


Рис. 15.3. Разветвляющаяся композиция машин Тьюринга.

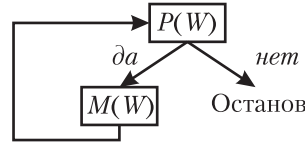


Рис. 15.4. Циклическая композиция машин Тьюринга.

Было математически доказано, что для реализации любых алгоритмов достаточно этих четырех структур¹.

15.4. Нормальные алгоритмы Маркова

15.4.1. Работа алгоритма Маркова

☞ **Определение 15.12.** Нормальный алгоритм Маркова — это конечный упорядоченный набор подстановок вида $P_i \rightarrow Q_i$, или $P_i \rightarrow Q_i, i = 1, 2, \dots, n$. $P_i \rightarrow Q_i$ — обычная подстановка, которая означает, что крайнее левое вхождение подслова P_i в слове W заменяется на Q_i . $P_i \rightarrow Q_i$ — заключительная подстановка, т.е. после ее выполнения работа алгоритма завершается.

Исходное слово $W \in A^*$ перерабатывается с помощью алгоритма следующим образом. Начиная с первой подстановки, ищется первое левое вхождение подслова P_i в слове W . Если оно найдено, то оно заменяется на Q_i , после чего список подстановок просматривается с самого начала. Если же вхождения P_i не было найдено, то выбирается следующая подстановка. Если на некотором шаге была выполнена заключительная подстановка, то процесс переработки слова завершается и тогда говорят, что алгоритм применим к данному слову. Может оказаться, что процесс не завершается, т.е. ни одна из заключительных подстановок не применялась в процессе переработки слова. В этом случае говорят, что алгоритм не применим к данному слову.

* Примеры.

1. Нормальный алгоритм Маркова для сложения двух чисел в унарной системе, т.е. алгоритм вычисляет функцию $f(X, Y) = X + Y$ в алфавите $A = \{*, \cdot\}$. Алгоритм состоит из двух подстановок:

1. $* \mid \rightarrow \cdot$
2. $* \rightarrow \cdot$

¹ Композиция машин Тьюринга включает в себе основную идею структурного программирования. Именно Тьюрингу принадлежит доказательство полноты этих четырех схем композиции для реализации любого, сколь угодно сложного алгоритма.

Процесс переработки слова заключается в следующем (в скобках указан номер применяемой подстановки):

$|||*||| \Rightarrow (1) |||*||| \Rightarrow (1) ||||*|| \Rightarrow (1) ||||*|| \Rightarrow (1) ||||*|| \Rightarrow (1) ||||*|| \Rightarrow (2) |||||$

2. Алгоритм обращения слова в алфавите $A = \{a, b, c, \dots, z\}$. Например, исходное слово abc обращается в слово cba . Ниже приведен список подстановок, в котором переменные x, y обозначают любой символ из алфавита A , греческими символами α, β обозначены вспомогательные символы, необходимые для работы алгоритма.

1. $\alpha\alpha \rightarrow \beta$
2. $\beta x \rightarrow x\beta$
3. $\beta\alpha \rightarrow \beta$
4. $\beta \rightarrow \Lambda$
5. $\alpha y x \rightarrow x\alpha y$
6. $\Lambda \rightarrow \alpha$

Для слова abc процесс работы алгоритма заключается в следующем:
 $\Lambda abc \Rightarrow (6) \alpha abc \Rightarrow (5) b\alpha ac \Rightarrow (5) bc\alpha a \Rightarrow (6) abc\alpha a \Rightarrow (5) c\alpha b\alpha a \Rightarrow (6) \alpha c\alpha b\alpha a \Rightarrow (6) \alpha\alpha c\alpha b\alpha a \Rightarrow (1) \beta c\alpha b\alpha a \Rightarrow (2) c\beta\alpha b\alpha a \Rightarrow (3) c\beta b\alpha a \Rightarrow (2) cb\beta\alpha a \Rightarrow (3) cb\beta a \Rightarrow (2) cba\beta \Rightarrow (4) cba$.

15.4.2. Эквивалентность нормальных алгоритмов и машины Тьюринга

Теорема 15.1. Пусть M — машина Тьюринга с внешним алфавитом A и внутренним алфавитом Q . Тогда существует нормальный алгоритм Маркова с алфавитом $A \cup Q$, эквивалентный данной машине Тьюринга.

Доказательство. Пусть дана машина Тьюринга M с внешним алфавитом $A = \{x_i\}$, где $i = 1, 2, \dots, n$, и внутренним алфавитом $Q = \{q_j\}$, $j = 0, 1, \dots, m$. Двумерную конфигурацию на ленте можно записать как последовательность $x_1 x_2 \dots q_j x_{i+1} \dots x_k$, где символ текущего состояния q_j стоит перед символом, который обозревает головка машины Тьюринга в данный момент времени. Мы получим слово в алфавите $A \cup Q$. Тогда можно заменить каждую команду машины Тьюринга на последовательность подстановок следующим образом.

1. Команда вида $q_j x_i \rightarrow x_k q_r$ заменяется подстановкой $q_j x_i \rightarrow q_r x_k$.
2. Команда вида $q_j x_i \rightarrow x_k q_r$ заменяется списком подстановок $q_j x_{i+1} \rightarrow x_k q_r x_{i+1}, \forall x_i \in A$.
3. Команда вида $q_j x_i \rightarrow x_k q_r$ заменяется списком подстановок $x_{i-1} q_j x_i \rightarrow q_r x_{i-1} x_k, \forall x_i \in A$.
4. Дописывается подстановка $q_k \rightarrow \Lambda$, где q_k — конечное состояние.
5. В конец списка вводится подстановка $\Lambda \rightarrow q_0$.

Таким образом, если имеется некоторая программа для машины Тьюринга, то с помощью этих пяти правил ее можно преобразовать в алгоритм Маркова. \simeq

★ **Пример.** Пусть задана программа для машины Тьюринга в алфавите $A = \{ \mid, * \}$ (табл. 15.5).

Таблица 15.5. Нормальный алгоритм Маркова, эквивалентный этой машине Тьюринга, имеет вид:

	q_0
\mid	$\mid q_0 \Pi$
Λ	$\mid ! H$
$*$	$* q_0 \Pi$

1. $q_0 \mid \mid \rightarrow \mid q_0 \mid$
2. $q_0 \mid * \rightarrow \mid q_0 *$
3. $q_0 \mid \Lambda \rightarrow \mid q_0 \Lambda$
4. $q_0 \Lambda \rightarrow \cdot \mid$
5. $\Lambda \rightarrow q_0$

Процесс переработки слова: $\mid \mid * \mid \Rightarrow q_0 \mid \mid * \mid \Rightarrow \mid q_0 \mid * \mid \Rightarrow \mid \mid q_0 * \mid \Rightarrow \mid \mid * q_0 \mid \Rightarrow \mid \mid * \mid q_0 \Lambda \Rightarrow \mid \mid * \mid \mid$.

Теорема 15.2. (обратная). Для каждого нормального алгоритма Маркова можно построить эквивалентную ему машину Тьюринга.

Схема доказательства.

1. Построить машину Тьюринга, осуществляющую поиск подслова P в слове W ; головка машины Тьюринга, в результате, будет стоять на первом символе подслова P .

2. Построить машину Тьюринга, заменяющую подслово P на слово Q (для каждой подстановки алгоритма Маркова можно построить машину Тьюринга, выполняющую ее).

Полученная композиция машин Тьюринга будет выполнять ту же процедуру переработки слов, что и алгоритм Маркова. \simeq

Для нормального алгоритма Маркова можно определить распознающий алгоритм Маркова как вычисляющий некоторый предикат и имеющий заключительные подстановки $P \rightarrow_{da} Q$ и $P \rightarrow_{nem} Q$; аналогично можно определить понятие композиции (по тем же схемам, что и для машины Тьюринга).

Приведенные выше две теоремы утверждают эквивалентность машины Тьюринга и нормального алгоритма Маркова. Отсюда следует, что, если построена машина Тьюринга для решения какой-либо задачи, т.е., если функция вычислима по Тьюрингу, то для нее существует и нормальный алгоритм Марков, т.е. она вычислима по Маркову, и наоборот, если функция вычислима по Маркову, то она вычислима по Тьюрингу. Иными словами, классы функций, вычисляемых по Тьюрингу и по Маркову, совпадают. Рассмотрим теперь, какой класс функций вычислим по Тьюрингу.

15.4.3. Класс функций, вычисляемых по Тьюрингу

Теорема 15.3. Функция $F(x_1, x_2, \dots, x_n)$ рекурсивна (частично рекурсивна) тогда и только тогда, когда она вычислима по Тьюрингу.

Доказательство.

1. Всякая рекурсивная функция вычислима по Тьюрингу.

$O(X) = \Lambda$ — нуль-функция вычислима на машине Тьюринга, которая уничтожает любое слово на ленте.

$N(X) = X + 1$ — вычислима на машине Тьюринга, которая к любому слову W на ленте дописывает заданный символ $a : Wa$.

$U_j^n(X) = x_i$ — функция проекции, которая в слове W выделяет символ x_i , вычислима на машине Тьюринга.

$\Phi(X_1, X_2) = g(F_1(X_1, X_2), F_2(X_1, X_2))$ — суперпозиция функций, реализуется посредством композиции машин Тьюринга: $M_\Phi = \text{copy}2(X_1 * X_2)^\circ (MF_1 \parallel MF_2)^\circ \text{зам}^* \parallel \text{Mg}$. Машина M_Φ сначала копирует исходное слово, реализуя функцию $\text{Copy}2(X_1 * X_2)$, результатом которой является слово $X_1 * X_2 \parallel X_1 * X_2$. Затем оно перерабатывается параллельной композицией машин $MF_1 \parallel MF_2$ в слово $F_1(X_1 * X_2) \parallel F_2(X_1 * X_2)$, затем алгоритм $\text{зам}^* \parallel$ заменяет вспомогательный разделяющий символ \parallel на $*$, и далее работает машина, вычисляющая функцию $g(F_1(X_1, X_2), F_2(X_1, X_2))$: $M_g(F_1(X_1 * X_2) * F_2(X_1 * X_2))$. Результатом ее работы является функция $\Phi(X_1, X_2)$.

Схема примитивной рекурсии также вычисляется посредством композиции машин Тьюринга. Например, самая простая схема примитивной рекурсии: $\Phi(0) = c$, $\Phi(X + 1) = F(\Phi(X))$, — вычислима как композиция, реализующая итерацию. Для этого строятся машины:

M_D , которая перерабатывает тройку чисел $X \# m \# z$ в тройку $X \# m + 1 \# F(z)$;

M_C , которая перерабатывает число X в тройку $X \# 0 \# c$;

Φ , которая распознает свойство $m < X$ в тройке чисел $X \# m \# z$.

Композиция $M_C \circ \text{пока } \Phi \text{ повторить } M_D$ задает алгоритм, который, исходя из слова X , вырабатывает тройку $X \# 0 \# c$, потом $X \# 1 \# F(c)$, потом $X \# 2 \# F(F(c))$, и так далее, до тех пор, пока не будет получена тройка $X \# X \# \Phi(X)$. Тогда выделяющий алгоритм, примененный к этому слову, выделит крайнюю правую компоненту слова, которая является результатом вычисления функции $\Phi(X)$.

Машина Тьюринга, вычисляющая μ -оператор, будет находить минимальное слово в лексикографическом упорядочивании слов, удовлетворяющее данному предикату.

Поскольку все шесть пунктов определения рекурсивных функций реализуемы в виде композиций машин Тьюринга, то всякая рекурсивная функция вычислима на машине Тьюринга.

2. Всякая функция, вычисляемая по Тьюрингу, рекурсивна (частично рекурсивна).

Доказательство можно найти в [Трахтенброт, 1976; Кузнецов, 1980].

Таким образом, показано, что класс функций, вычисляемых на машине Тьюринга, является частично рекурсивным классом. \asymp

Кроме машины Тьюринга и нормального алгоритма Маркова было найдено и предложено много других алгоритмических схем, например, машина фон Неймана, машина Поста, блок-схемы Поста, формальное исчисление рекурсивных функций Эрбрана — Гёделя и другие. Оказалось, что все они эквивалентны между собой, и, следовательно, вычисляют рекурсивные или частично рекурсивные функции. Это обстоятельство послужило причиной тому, что ряд ученых (Чёрч, Тьюринг, Марков) высказали гипотезу, которая известна как тезис Чёрча.

15.4.4. Тезис Чёрча

Каждая функция является эффективно вычислимой тогда и только тогда, когда она рекурсивна.

Иными словами, тезис Чёрча предлагает понимать под эффективной вычислимостью существование алгоритмической схемы, а поскольку все найденные алгоритмические схемы вычисляют только класс рекурсивных (частично рекурсивных) функций, то под эффективной вычислимостью тогда понимается рекурсивность.

Мы уже говорили, что понятие алгоритма не является точным математическим определением. Попытки найти такое определение привели к созданию математически строгих алгоритмических схем. Значение гипотезы, высказанной в тезисе Черча, заключается в том, что она уточняет интуитивно понятное, но неточное и расплывчатое понятие алгоритма через более специальное, но математически точное понятие алгоритмической схемы. Теперь можно говорить о разрешимости некоторого класса задач в терминах существования машины Тьюринга (или алгоритма Маркова, или какой-либо другой из известных алгоритмических схем).

Тезис Черча не является теоремой, о его доказательстве речи не идет, — это утверждение, предлагающее отождествить эффективную вычислимость с существованием алгоритмической схемы. Его можно принимать или не принимать,

Уверенность в справедливости тезиса Чёрча основана, прежде всего, на опыте: в результате многочисленных исследований не удалось найти какой-либо другой алгоритмической схемы, которая вычисляла бы более широкий класс функций, чем рекурсивный. Все найденные алгоритмические схемы оказались эквивалентны между собой и, следовательно, эквивалентны машине Тьюринга.

Поэтому вычислимыми функциями, согласно тезису Чёрча, являются те и только те, которые являются рекурсивными (частично рекурсивными). Однако, не все арифметические функции являются рекурсивными. Это нетрудно показать.

Если принимать тезис Черча, то множество эффективно вычисляемых функций совпадает с множеством всех машин Тьюринга, так как каждая машина Тьюринга вычисляет какую-либо арифметическую функцию. Любая программа для машины Тьюринга может быть закодирована некоторым кодом. Пусть M есть некоторая машина Тьюринга. Тогда программу машины M вместе с входным словом W можно записать в виде последовательности: $x_i q_i x_k P q_j; x_i q_i x_k P q_n; \dots x_i q_m x_n P q_k^* W$, где каждая команда $x_i q_i \rightarrow x_k \xi q_j$, записана как $x_i q_i x_k \xi q_j$ ($\xi \in \{P, L, H\}$), команды разделены символом «;». Такая последовательность называется кодом машины Тьюринга и обозначается $d(M)$. Код машины Тьюринга можно представить числом в некоторой системе счисления. Будем обозначать состояния машины Тьюринга десятичными числами, тогда для обозначения состояний потребуется 10 символов. В качестве входного алфавита выберем алфавит из двух символов 0 и 1 (возможность кодирования слов любого алфавита в двоичной системе счисления не вызывает сомнений). Сохраним символы движения головки: L , P , H , и разделительные символы «;» и «*». Тогда коду каждой машины Тьюринга будет соответствовать число в пятнадцатичной системе счисления, которое можно перевести в десятичную систему счисления, и различным машинам будут соответствовать различные числа. Это число, соответствующее коду машины, называют *индексом* машины Тьюринга. Вычисление индекса определяет инъекцию множества всех машин Тьюринга в бесконечное подмножество натуральных чисел. Отсюда следует, что множество машин Тьюринга счетно. Однако множество всех арифметических функций несчетно, откуда следует, что существуют невычислимые функции и алгоритмически неразрешимые проблемы.

15.5. Алгоритмически неразрешимые проблемы

15.5.1. Универсальная машина Тьюринга

Машина Тьюринга содержит основные идеи современных вычислительных машин, в которых последовательность вычислений управляется программой. Тьюрингу принадлежит также идея построения универсальной вычислительной машины, которая сначала проверяет правильность введенной в нее программы, а затем выполняет ее над заданными исходными данными. Эта идея реализована в современных вычислительных машинах. Целью Тьюринга

при разработке универсальной машины было создание математического аппарата для моделирования работы любой машины Тьюринга.

Можно построить такую машину $M'(d(M)*W)$, на вход которой будет подаваться код машины Тьюринга $d(M)$ вместе с входным словом W . Тогда машина M' сначала проверяет, является ли $d(M)$ синтаксически правильным программным кодом для машины Тьюринга, и если это так, то выполняет программу машины M над словом W ; если же нет, то она останавливается в состоянии «нет!». Такая машина Тьюринга называется *универсальной машиной Тьюринга*.

Аналогично можно построить и универсальный алгоритм Маркова.

15.5.2. Проблема останова для машины Тьюринга

Исторически первой алгоритмически неразрешимой проблемой, доказанной Тьюрингом, была проблема останова для машины Тьюринга. Она формулируется так: можно ли построить такую универсальную машину Тьюринга M' , что будучи примененной к слову $(d(M)*W)$, она будет останавливаться в «да!» состоянии, если машина Тьюринга M применима к слову W , т.е. останавливается на этом слове, и останавливаться в «нет!» состоянии, если машина M не применима к слову W .

Теорема 15.5. Проблема останова для машины Тьюринга алгоритмически неразрешима.

Доказательство.

Предположим, что универсальная машина Тьюринга M' , распознающая останов для любой машины Тьюринга, построена. Тогда в ее программе есть команды: $q'\sigma \rightarrow \sigma da!$ и $q''\tau \rightarrow \tau нет!$, т.е. в состоянии q' на символе σ машина M' останавливается в да!-состоянии, а в состоянии q'' на символе τ — в нет!-состоянии.

Построим теперь машину Тьюринга M'' так, что изменим в ней только одну команду: в состоянии q' на символе σ машина M'' выдает сигнал da (переходит в состояние da), но не останавливается, а продолжает бесконечно писать символ σ в одну и ту же ячейку. Тогда в программе машины M'' будут команды: $q'\sigma \rightarrow \sigma daH$ и $q''\tau \rightarrow \tau нет!$.

Теперь на вход машины M' подадим ее собственный код, а в качестве входного слова — код машины M'' : $M'(d(M')*d(M''))$. Сможет ли теперь машина M' распознать, остановится ли она сама на коде машины Тьюринга M'' ?

Универсальная машина Тьюринга работает так, как машина, код которой подан на ее ленту, следовательно, дойдя до символа σ в состоянии q' в коде машины M'' , машина M' остановится в

состоянии «да!», в то время как M'' не останавливается! И наоборот, когда в состоянии q'' машина M'' видит символ τ , она выдает сообщение «нет» и останавливается, а машина M' для этой ситуации тоже останавливается в состоянии «нет», т.е. она выдает сообщение о том, что машина M'' не останавливается! \approx

Таким образом, машина Тьюринга M' не распознает свой собственный останов на коде машины M'' . Сам факт возможности построения такой машины Тьюринга, которая не может распознать останов, доказывает алгоритмическую неразрешимость этой проблемы.

15.5.3. Проблема самоприменимости

Будем говорить, что машина Тьюринга M *самоприменима*, если она останавливается на своем собственном коде $d(M)$, и не самоприменима, если она не останавливается на своем коде $d(M)$.

Теорема 15.6. Проблема распознавания самоприменимости машины Тьюринга алгоритмически не разрешима.

Доказательство. Предположим, что построена универсальная распознающая машина Тьюринга M' , которая останавливается в «да!» состоянии, если машина, код которой подается на ее вход, самоприменима, и в «нет!» состоянии, если не самоприменима. Тогда в программе машины Тьюринга M' присутствуют две команды вида: $q'\sigma \rightarrow \sigma da!$, $q''\tau \rightarrow \tau нет!$. Аналогично предыдущему доказательству, построим машину M'' , изменив одну команду: $q'\sigma \rightarrow \sigma daH$ (т.е. в состоянии q' машина не останавливается, а бесконечно пишет символ σ на ленте). Теперь, если на вход M' подать $d(M'')$: $M'(d(M''))$ машина будет выдавать «да!», — т.е. сообщать, что M'' самоприменима, в то время как она несамоприменима, так как не останавливается, и, наоборот, она будет выдавать сообщение «нет!», если машина M'' не останавливается, т.е. если она самоприменима. \approx

Таким образом, доказательство неразрешимости проблемы самоприменимости сводится к доказательству невозможности распознавания останова машины Тьюринга. Отсюда возник и общий метод доказательства алгоритмической неразрешимости других задач: метод сведения проблем. Он заключается в том, что новая проблема сводится к некоторой другой проблеме, для которой уже доказана алгоритмическая неразрешимость. Особенно часто проблема сводится в проблеме самоприменимости. В качестве примера рассмотрим проблему эквивалентности слов в ассоциативных исчислениях.

Теорема 15.7. (Маркова – Поста). Существует ассоциативное исчисление, в котором проблема распознавания эквивалентности слов алгоритмически неразрешима.

Доказательство. Пусть машина Тьюринга M начинает работу со слова R с начальной конфигурацией q_0a и заканчивает работу словом S с конечной конфигурацией q_kb . Проблема распознавания эквивалентности слов R и S в такой постановке заключается в нахождении алгоритма, который по коду машины M распознает, остановится ли она в состоянии q_k , начиная работу с конфигурации q_0a , или нет. Подадим код этой машины вместе со словом R на вход универсальной машины M' : $M'(d(M)*R)$. Для машины M' проблема останова неразрешима. Отсюда следует, что проблема распознавания эквивалентности слов также алгоритмически неразрешима. Покажем, что она неразрешима также и в некотором ассоциативном исчислении. Для этого воспользуемся тем свойством, что для любой машины Тьюринга можно построить эквивалентное ему ассоциативное исчисление.

Последнее свойство было доказано нами для нормальных алгоритмов Маркова. Нормальный алгоритм Маркова можно рассматривать как ассоциативное исчисление с однонаправленными подстановками, что непосредственно следует из определения этих систем. При необходимости для каждой подстановки нормального алгоритма можно определить обратную подстановку и получить ассоциативное исчисление с двунаправленными подстановками.

Построим ассоциативное исчисление $G(M)$, выполняющее тот же алгоритм, что и машина M , в частности, перерабатывающее слово R в слово S , и присоединим к нему систему подстановок вида $q_ka_i \rightarrow q_k$. Получим новое исчисление $G'(M)$. В этом исчислении также перерабатываются слова вида R в слова вида S , но все заключительные конфигурации M в $G'(M)$ эквивалентны. Поэтому в $G(M)$ слова q_0a и q_k эквивалентны, если и только если машина M , начав работу со слова q_0a , остановится. Ввиду неразрешимости проблемы останова для M' , проблема эквивалентности слов q_0a и q_k также неразрешима. \asymp

Из этой теоремы следует, что проблема распознавания эквивалентности слов в общем случае (т.е. для всего множества ассоциативных исчислений) алгоритмически неразрешима. Отсюда следует также, что проблема эквивалентности алгоритмов неразрешима: по двум заданным алгоритмам в общем случае невозможно определить, вычисляют они одну и ту же функцию или нет.

Исторически алгоритмическая неразрешимость сначала была установлена для проблем, возникающих в математической логике, — проблем выводимости в формальных теориях. Доказательство неразрешимости проблем самоприменимости и эквивалентности показало, что алгоритмические схемы могут служить аппаратом исследования разрешимости и полноты формальных теорий. Проб-

лему выводимости в формальной теории можно интерпретировать как проблему распознавания эквивалентности слов: с помощью заданной системы правил вывода необходимо определить, является ли формула выводимой из заданной системы аксиом и исходного множества посылок. Тогда из алгоритмической неразрешимости распознавания эквивалентности слов следует неразрешимость (в общем случае!) проблемы выводимости. Мы знаем, что исчисление высказываний разрешимо: построение таблицы истинности формулы является алгоритмом, с помощью которого доказывается, что формула является (или не является) тавтологией логики высказываний, а, следовательно, и теоремой исчисления высказываний. Существование неразрешимых предложений формальной арифметики (теорема Гёделя о неполноте) доказывает ее неразрешимость. Доказательство теоремы Гёделя существенно основывалось на рекурсивности представимых в S функций и отношений. Следовательно, тот же самый результат можно получить, используя аппарат алгоритмических схем, в частности, машины Тьюринга. В 1936 г. этот результат: *проблема распознавания выводимости в исчислении предикатов алгоритмически неразрешима*, — был получен Чёрчем. Для дальнейших доказательств введем некоторые новые понятия.

15.5.4. Рекурсивные и рекурсивно перечислимые множества

➔ **Определение 15.13.** Рекурсивно перечислимым множеством является либо пустое множество, либо множество значений некоторой рекурсивной функции $F(x)$.

Принимая тезис Чёрча, это можно интерпретировать так, что для рекурсивно перечислимого множества существует эффективная процедура последовательного порождения (перечисления) всех его элементов; иными словами, существует машина Тьюринга, которая, начиная работу с пустой ленты, выписывает на нее все элементы этого множества.

➔ **Определение 15.14.** Множество S является рекурсивным, если существует рекурсивная функция $f(x)$ такая, что

$$f(x) = \begin{cases} 1, & \text{если } x \in S, \\ 0, & \text{если } x \notin S. \end{cases}$$

В терминах эффективной вычислимости это означает, что существует эффективная процедура для выяснения вопроса, принадлежит или не принадлежит произвольный элемент этому множеству. Тогда существует машина Тьюринга, которая для любого x останавливается в «да!» состоянии, если x принадлежит множеству S , и в «нет!» состоянии, если x не принадлежит S .

Рекурсивные множества называют также *разрешимыми* множествами.

Можно доказать следующие теоремы о рекурсивных и рекурсивно перечисливых множествах.

Теорема 15.8. Если множества R и S рекурсивно перечислимы, то их объединение $R \cup S$ и пересечение $R \cap S$ также рекурсивно перечислимы.

Доказательство.

Из условия теоремы следует, что существуют две машины M_R и M_S , которые порождают элементы множеств R и S соответственно. Тогда можно построить машину Тьюринга $M_{R \cup S}$, выписывающую на ленту последовательно элементы $r_1, s_1, r_2, s_2, \dots$, удаляя повторяющиеся элементы. Можно построить также машину $M_{R \cap S}$, которая в этой последовательности будет оставлять только те элементы, которые входят одновременно и в R , и в S . \simeq

Теорема 15.9. Множество S рекурсивно тогда и только тогда, когда S и его дополнение S' рекурсивно перечислимы.

Доказательство.

1. Предположим, что $S \subseteq \mathbf{N}$ и S рекурсивно. Тогда существует машина Тьюринга M_S , которая для каждого натурального числа $n \in \mathbf{N}$ распознает, принадлежит ли оно множеству S , или нет. Тогда можно построить такую композицию, что если $M_S(n)$ останавливается в состоянии «да!», т.е. $n \in S$, то начинает работу машина M_1 , которая выписывает на свою ленту все элементы S , а если $M_S(n)$ останавливается в состоянии «нет!», т.е. $n \notin S$, то начинает работать машина M_2 , которая выписывает все элементы, не принадлежащие S , на свою ленту. Тогда машина M_1 порождает все элементы S , а M_2 — его дополнения S' . Согласно определению, это означает, что S и его дополнение S' рекурсивно перечислимы.

2. Предположим, что S и S' рекурсивно перечислимы. Следовательно, существуют порождающие их машины M_S и $M_{S'}$. Тогда можно построить машину $M(x)$, которая для каждого x будет запускать попеременно M_S и $M_{S'}$ и сравнивать x с очередным элементом s_i . Если $x = s_i$, порожденному машиной M_S , то машина $M(x)$ останавливается в «да!» состоянии, а если машиной $M_{S'}$ — то в «нет!» состоянии. Тогда машина $M(x)$ работает как распознающая машина Тьюринга для вычисления предиката $x \in S$. Существование такой машины означает, что множество S рекурсивно. \simeq

Теорема 15.10. Существуют рекурсивно перечислимые, но нерекурсивные множества.

В силу теоремы 15.9 это означает, что существует такое множество S , которое рекурсивно перечислимо, но его дополнение S' не является рекурсивно перечислимым.

Доказательство.

Предположим, что все рекурсивно перечислимые множества мы можем переписать в виде списка (занумеровать): $S_1, S_2, \dots, S_j, \dots$. Тогда существует машина Тьюринга $M(n)$, такая, что для каждого натурального числа $n = 1, 2, 3, \dots$ она проверяет, принадлежит ли число n , соответствующее индексу множества S_n , самому этому множеству, (т.е. $n \in S_n$), или нет. Тогда, если $n \in S_n$, она выдает сообщение «да» и записывает это число в множество U , а если $n \notin S_n$, то она выдает «нет», и записывает число n в множество U' . Таким образом, U будет содержать некоторое подмножество натуральных чисел и будет рекурсивно перечислимо. Очевидно, что U' будет дополнением множества U до множества всех натуральных чисел. Докажем теперь, что множество U' не рекурсивно перечислимо.

Действительно, если U' рекурсивно перечислимо, то U' входит в наш пересчет с некоторым номером k , т.е. $U' = S_k$. Тогда, если $k \in S_k$, то $k \in U$, т.е. $k \notin U'$, но тогда $k \notin S_k$; а если $k \notin S_k$, то $k \in U'$, т.е. $k \in S_k$.

Таким образом, существует элемент k , который нельзя отнести ни к тому, ни к другому множеству. Полученное противоречие доказывает, что наше предположение о существовании такой распознающей машины Тьюринга было неверным, и множество U' не рекурсивно перечислимо, и, следовательно, U не рекурсивно. \simeq

Из доказательства этой теоремы становится понятным, что алгоритмическая неразрешимость и нерекурсивность — это взаимосвязанные свойства. Способ кодирования программ машин Тьюринга, описанный выше, задает эффективную процедуру, порождающую множество индексов машин Тьюринга. Отсюда следует, что множество всех машин Тьюринга рекурсивно перечислимо. Рекурсивно перечислимым является также множество всех машин, которые заканчивают свою работу за конечное число шагов. При доказательстве алгоритмической неразрешимости проблемы останова для машины Тьюринга было показано, что можно построить такую машину Тьюринга, для которой невозможно распознать останов. Это построение доказывает, что множество всех машин Тьюринга, которые не останавливаются на некотором слове, не является рекурсивно перечислимым. Следовательно, множество всех машин, которые останавливаются, нерекурсивно (неразрешимо). Нерекурсивность множества означает, что его характеристическая функция, распознающая принадлежность элемента этому множеству, является невычислимой. Построим такую функцию.

15.6. Невычислимые функции

Определим предикат $T(i, a, x)$, где i — индекс машины Тьюринга, которая, будучи применима к слову a , заканчивает работу в момент времени x , вычисляя при этом функцию $\varphi_i(a)$. Существование момента времени x — гарантия останова машины. Этот предикат будет разрешимым (т.е. истинным при некоторых значениях i, a, x). Действительно, можно построить такую универсальную машину Тьюринга M' , которая для любой машины будет определять, является ли i правильным кодом машины Тьюринга. Если i не является кодом, то M' остановится в состоянии «нет!»; тогда $|T(i, a, x)| = F$. Если i является правильным кодом машины Тьюринга, то M' будет работать над словом a и остановится в состоянии «да!», если в момент x машина вычислит значение функции $\varphi_i(a)$. Тогда $|T(i, a, x)| = T$.

Эти рассуждения показывают, что предикат $T(i, a, x)$ разрешим в интуитивном смысле. Если принимать тезис Чёрча, то этот предикат разрешим и в строгом смысле, т.е. можно построить такую машину Тьюринга, которая вычисляет характеристическую функцию предиката:

$$\tau(i, a, x) = \begin{cases} 0, & \text{если } T(i, a, x) = F, \\ 1, & \text{если } T(i, a, x) = T. \end{cases}$$

Таким образом, во-первых, предикат $T(i, a, x)$ разрешим, а во-вторых, $\varphi_i(a)$ вычислима как частичная функция от x . Действительно, она определена не для всех i и a , только для тех, для которых существует момент времени x , когда машина Тьюринга остановится. Поэтому $\varphi_i(a)$ является частично определенной функцией и вычислима как частичная функция от i и x , т.е. тогда, когда $|\forall a \exists x T(i, a, x)| = T$.

Определим теперь следующую функцию:

$$\psi(a) = \begin{cases} \varphi_a(a) + 1, & \text{если } \exists x T(a, a, x), \\ 0 & \text{в противном случае.} \end{cases}$$

Теорема 15.11. (Чёрча). Функция $\psi(a)$ невычислима.

Доказательство.

Предположим, что $\psi(a)$ вычислима. Тогда существует машина Тьюринга M_p , вычисляющая $\psi(a)$, и p — индекс этой машины, т.е. $\psi(a) = \varphi_p(a)$ для всех a . Подставляя p вместо a , получим: $\psi(p) = \varphi_p(p)$. Тогда предикат $|\exists x T(p, a, x)| = T$ для данного p и для любого a , в том числе и для $a = p$, т.е. $|\exists x T(p, p, x)| = T$. Но тогда, по определению функции $\psi(a)$, $\psi(p) = \varphi_p(p) + 1$, что противоречит полученному ранее равенству. Полученное противоречие доказывает утверждение теоремы. \asymp

Теорема Чёрча дает конструктивный способ построения невычислимой функции.

✱ **Пример.** В качестве примера определения невычислимой функции рассмотрим следующую задачу. Представим себе большую библиотеку, в которой книги расставлены по разделам. Для каждого раздела составлен каталог. Каждая книга имеет назначенную ей цену, а поскольку каталог раздела содержит сведения обо всех книгах, он должен быть самой ценной книгой. Поэтому его стоимость определена как функция от стоимости самой дорогой книги в разделе: $C_\kappa = C_{\max} + 1$. Книг в библиотеке оказалось настолько много, что все каталоги были составлены в отдельный раздел — раздел каталогов, для которого также был составлен каталог — каталог каталогов. Ему также должна быть назначена цена по определенному выше правилу: стоимость его C_κ должна быть самой высокой в этом разделе, т.е. $C_\kappa = C_{\kappa \max} + 1$, и должна быть на единицу больше цены самой дорогой книги в разделе: $C_\kappa = C_{\kappa \max} + 1$. Но поскольку каталог каталогов сам является каталогом, то его цена должна быть на единицу больше его собственной стоимости: $C_\kappa = C_\kappa + 1$. Таким образом, оказалось, что стоимость его невозможно вычислить по заданному правилу.

Невычислимая функция Чёрча уже встречалась нам и ранее: при доказательстве несчетности множества всех арифметических функций, при доказательстве нерекursивности множества, имеющего не перечислимое рекурсивно дополнение. Но в теореме Чёрча эта функция определена через предикат $T(p, a, x)$, существенно использующий условие останова для машины Тьюринга — переменную x . Предикат $\exists x T(p, p, x)$ формулирует условие останова машины Тьюринга на своем собственном коде, т.е. условие самоприменимости. Полученное в теореме противоречие доказывает, что этот предикат неразрешим (т.е. предположение о его разрешимости было ложным). Тем самым теорема Чёрча еще раз доказывает неразрешимость проблемы самоприменимости, а в терминах теории предикатов — существование неразрешимого предложения: предложения о распознавании останова для машины Тьюринга на своем собственном коде. Существование неразрешимого предиката доказывает неразрешимость исчисления предикатов, содержащего арифметику, — вспомним, что формула G , построенная Гёделем, также утверждает свою собственную невыводимость, а поскольку ее действительно нельзя ни доказать, ни опровергнуть, то это равнозначно неразрешимости проблемы самоприменимости.

Интуитивно нам уже понятно, что неразрешимость теории предикатов связана с нерекursивностью множества всех теорем формальной теории. Арифметизация формальной теории S (и

способ, предложенный Гёделем для арифметизации любой формальной теории) позволяет нам говорить о них в терминах рекурсивных и рекурсивно перечислимых множеств. Тогда становится понятным, что существование неразрешимого предложения, истинного в содержательной теории, но невыводимого в формальной теории, означает существование такого гёделева номера (натурального числа), которое не принадлежит ни множеству гёделевых номеров теорем (выводимых предложений), ни множеству гёделевых номеров невыводимых предложений. Иными словами, это означает, что множество гёделевых номеров теорем (и, следовательно, множество самих теорем) теории предикатов первого порядка не рекурсивно.

Формально это доказывается следующей теоремой, доказательство которой известно как доказательство Россера теоремы Гёделя.

Теорема 15.12. Пусть существуют два рекурсивно перечислимых непустых множества C_0 и C_1 , такие, что $C_0 \cap C_1 = \emptyset$, и существуют два рекурсивно перечислимых множества D_0 и D_1 , такие, что $C_0 \subseteq D_0$, $C_1 \subseteq D_1$ и $D_0 \cap D_1 = \emptyset$. Тогда можно найти такое число f , что $f \notin D_0$ и $f \notin D_1$.

Доказательство.

Определим множества C_0 и C_1 следующим образом:

$$C_0 = \{a \mid \varphi_a(a) \text{ определена и } \varphi_a(a) = 0\},$$

$$C_1 = \{a \mid \varphi_a(a) \text{ определена и } \varphi_a(a) \neq 0\}.$$

Понятно, что множества C_0 и C_1 непусты и не пересекаются.

Пусть существуют множества D_0 и D_1 , удовлетворяющие условиям теоремы.

Тогда из того, что D_0 рекурсивно перечислимо, следует существование машины Тьюринга, перечисляющей элементы D_0 , т.е. вычисляющей функцию $\varphi_0(D_0)$, и из того, что D_1 рекурсивно перечислимо, следует существование машины Тьюринга, перечисляющей элементы D_1 , т.е. вычисляющей функцию $\varphi_1(D_1)$. Тогда можно построить машину Тьюринга M , которая для любого числа a определяет, принадлежит это число нумерации φ_0 или нумерации φ_1 . При этом, если машина Тьюринга M находит число a в нумерации φ_0 , то она печатает «1» и останавливается, а если число a принадлежит нумерации φ_1 , то машина печатает «0» и останавливается. Если $a \notin \varphi_0$ и $a \notin \varphi_1$, то машина Тьюринга не останавливается.

Предположим, что существует число $f \in D_0$. Тогда $f \notin D_1$. Следовательно, число $f \in \varphi_0$, т.е. встречается в нумерации φ_0 , и $f \notin \varphi_1$ (не встречается в нумерации φ_1).

Подадим число f на вход машины Тьюринга M . Так как $f \in \varphi_0$, то машина напечатает «1», т.е. $\varphi_f(f) = 1$. Тогда, по определению

множеств C_0 и C_1 , число f следует отнести к C_1 : $f \in C_1$; а поскольку $C_1 \subseteq D_1$, то $f \in D_1$, т.е. $f \notin D_0$. И наоборот, если $f \in D_1$, то $\varphi_f(f) = 0$, следовательно, $f \in C_0$, а значит и $f \in D_0$, следовательно, $f \notin D_1$. Таким образом, f не попадает ни в одно, ни в другое множество. Это противоречие доказывает теорему. \asymp

Теорема Россера не только доказывает теорему Гёделя в других терминах, но и показывает, что о вычислимости, выводимости и разрешимости можно говорить в терминах рекурсивных и рекурсивно перечислимых множеств. Поэтому можно сделать следующие выводы, обобщающие результаты, полученные Гёделем, Чёрчем, Россером и другими математиками относительно разрешимости формальных теорий.

Теорема 15.13. (Теорема Гёделя в форме Россера). Пусть K — теория первого порядка с теми же символами, что и теория S , и пусть, кроме того, K удовлетворяет следующим условиям:

- (1) всякое рекурсивное выражение выразимо в K ;
- (2) множество гёделевых номеров собственных аксиом теории K рекурсивно;
- (3) выполнены условия: имеется формула $u \leq v$ такая, что
 - (i) для всякой формулы $A(x)$ и для всякого натурального k

$$\vdash_K A(0) \& A(1) \& \dots \& A(k) \rightarrow \forall x(x \leq k \rightarrow A(x));$$
 - (ii) для всякого натурального числа
$$\vdash_K x \leq k \vee k \leq x.$$

Тогда для теории K справедлива теорема Гёделя в форме Россера: если теория K непротиворечива, то существует неразрешимое в этой теории предложение. (Заметим, что условие (1) выполняется, если в K представима каждая рекурсивная функция).

↪ **Определение 15.15.** Назовем теорию K *рекурсивно аксиоматизируемой*, если существует такая теория K' с тем же, что и у K , множеством теорем, что множество гёделевых номеров собственных аксиом K' рекурсивно.

↪ **Определение 15.16.** Теория называется *эффективно аксиоматизированной*, если существует эффективная процедура, позволяющая для каждой формулы этой теории узнавать, является ли она ее аксиомой.

Следствие. Теорема Гёделя в форме Россера справедлива для каждого непротиворечивого рекурсивно аксиоматизируемого расширения теории S , т.е. для каждого такого расширения существует предложение, неразрешимое в нем.

Доказательство.

Так как все рекурсивные отношения выразимы в S , то они выразимы и во всяком расширении S . Точно так же, если условия (i) — (ii) выполнены в S , то они выполнены и во всяком расширении S . Поэтому, на основании теоремы 14.9, теорема Гёделя в форме Россера применима к любому непротиворечивому рекурсивно аксиоматизируемому расширению теории S .

Если принимать тезис Чёрча, то последнее следствие утверждает, что теория S *существенно неполна*, т.е., что любое непротиворечивое эффективно аксиоматизированное расширение теории S имеет неразрешимые предложения.

Список литературы

1. Арбиб М. Мозг, машина и математика. — М.: Наука, 1968.
2. Берж К. Теория графов и ее приложения. — М.: Изд-во иностр. лит., 1962.
3. Биркгоф Г. Теория решеток. — М.: Наука, 1984.
4. Булос Дж., Джеффри Р. Вычислимость и логика. — М.: Мир, 1994.
5. Гильберт Д., Бернайс П. Основания математики. Логические исчисления и формализация арифметики. — М.: Наука, 1979.
6. Гиндикин С. Г. Алгебра логики в задачах. — М.: Наука, 1972.
7. Глушков В. М. Введение в кибернетику. — К.: Изд-во АН УССР, 1964.
8. Горбатов В. А. Основы дискретной математики. — М.: Высш. шк., 1986.
9. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.
10. Донской В. И. Дискретная математика. — Симферополь: СОНАТ, 2000.
11. Ершов Ю. А., Палютин Е. А. Математическая логика. — М.: Наука, 1979.
12. Заде Л. Понятие лингвистической переменной и его применение к принятию проблемных решений. — М.: Мир, 1976.
13. Карри Х. Б. Основания математической логики. — М.: Мир, 1969.
14. Клини С. К. Введение в метаматематику. — М.: Мир, 1957.
15. Клини С. К. Математическая логика. — М.: Мир, 1973.
16. Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. — М.: Изд-во Моск. ун-та, 1982.
17. Кофман А. Введение в теорию нечетких множеств. — М.: Радио и связь, 1982.
18. Козн П. Дж. Теория множеств и континуум-гипотеза. — М.: Мир, 1973.
19. Кузин Л. Т. Основы кибернетики: В 2 т. — Т. 2. — М.: Энергия, 1979.
20. Кузнецов О. П., Адельсон-Вельский Г. М. Дискретная математика для инженера. — М.: Энергия, 1980.
21. Куратовский К., Мостовский А. Теория множеств. — М.: Мир, 1970.
22. Кэррол Л. История с узелками. — М.: Мир, 1973.
23. Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов. — М.: Наука, 1975.
24. Линдон Р. Заметки по логике. — М.: Мир, 1968.
25. Логический подход к искусственному интеллекту / Тейз Ф., Грибомон П., Луи Ж. и др. — М.: Мир, 1990.
26. Мальцев А. И. Алгебраические системы. — М.: Наука, 1975.
27. Манин. Ю. И. Вычислимое и невычислимое. — М.: Сов. Радио, 1980.
28. Мендельсон Э. Введение в математическую логику. — М.: Наука, 1976.
29. Нагель Э., Ньюмен Д. Теорема Гёделя. — М.: Знание, 1970.
30. Нефедов В. Н., Осипова В. А. Курс дискретной математики. — М.: МАИ, 1992.
31. Новиков П. С. Элементы математической логики. — М.: Физматгиз, 1959.
32. Ньюсом К. В., Ивс Г. О математической логике и философии математики. — М.: Знание, 1968.
33. Оре О. Теория графов. — М.: Наука, 1968.
34. Робертс Ф. С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. — М.: Наука, 1986.
35. Столл Р. Множество, логика, аксиоматические теории. — М.: Просвещение, 1968.

36. *Таран Т. А.* Основы дискретной математики: Учеб. пособие. — К.: Просвіта, 1998.
37. *Таран Т. А.* Основы математической логики. — К.: КПИ, 1996.
38. *Таран Т. А., Мыценко Н. А., Темникова Е. Л.* Сборник задач по дискретной математике. — К.: Просвіта, 2001.
39. *Трахтенброт В. А.* Алгоритмы и вычислительные автоматы. — М.: Сов. радио, 1974.
40. *Трахтенброт В. А.* Алгоритмы и машинное решение задач. — М.: Физматгиз, 1960.
41. *Успенский В. А.* Теорема Гёделя о неполноте. — М.: Наука, 1982.
42. *Харари Ф.* Теория графов. — М.: Мир, 1973.
43. *Хаусдорф Ф.* Теория множеств. — М.: ОНТИ, 1937.
44. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. — М.: Наука, 1983.
45. *Черч А.* Введение в математическую логику. — М.: Изд-во иностр. лит., 1961.
46. *Шиханович Ю. А.* Введение в современную математику. — М.: Наука, 1965.
47. *Шрейдер Ю. А.* Равенство, сходство, порядок. — М.: Наука, 1971.
48. *Яблонский С. В.* Введение в дискретную математику. — М.: Наука, 1979.

Оглавление

Предисловие	3
Глава 1. МНОЖЕСТВА	5
Глава 2. ТЕОРИЯ ОТНОШЕНИЙ	15
Глава 3. ОТОБРАЖЕНИЯ. ФУНКЦИИ	25
Глава 4. МОЩНОСТЬ МНОЖЕСТВ	37
Глава 5. ОТНОШЕНИЕ ПОРЯДКА	61
Глава 6. РЕШЕТКИ	74
Глава 7. СТРОЕНИЕ И ПРЕДСТАВЛЕНИЕ РЕШЕТОК	90
Глава 8. ГРАФЫ	109
Глава 9. БУЛЕВА АЛГЕБРА	148
Глава 10. ЛОГИКА ВЫСКАЗЫВАНИЙ	168
Глава 11. ФОРМАЛЬНЫЕ ТЕОРИИ. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ	181
Глава 12. ТЕОРИЯ ПРЕДИКАТОВ ПЕРВОГО ПОРЯДКА	198
Глава 13. АВТОМАТИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМ	223
Глава 14. СВОЙСТВА ТЕОРИЙ ПЕРВОГО ПОРЯДКА	242
Глава 15. ТЕОРИЯ АЛГОРИТМОВ	261
Список литературы	287