Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Саратовский государственный социально-экономический университет»

Кафедра прикладной математики и информатики

# ДИСКРЕТНАЯ МАТЕМАТИКА

*Рекомендовано*
*Учебно-методическим объединением в области экономики*
*и менеджмента, логистики и бизнес-информатики*
*в качестве учебного пособия*
*для студентов бакалавриата высших учебных заведений,*
*обучающихся по направлению подготовки 080500.62*
*«Бизнес-информатика»*

Саратов
2013

УДК 519.21
ББК 22.176
Д48

*Автор-составитель*
доктор физико-математических наук, профессор ***В.А. Молчанов***

Д48 **Дискретная** математика: учебное пособие для студентов, обучающихся по направлению подготовки 080500.62 «Бизнес-информатика» / авт.-сост. В.А. Молчанов / Саратовский государственный социально-экономический университет. – Саратов, 2013. – 132 с.

ISBN 978-5-4345-0215-3

В учебном пособии содержится материал основного курса «Дискретная математика», который в соответствии с федеральным государственным образовательным стандартом читается студентам направления 080500.62 «Бизнес-информатика». Излагаются основы теории множеств, общей алгебры, комбинаторики, алгебры логики, теории графов, теории кодирования, теории автоматов и теории алгоритмов. Приводятся методы и примеры решения типовых задач, контрольные вопросы для среза знаний.

Для студентов вузов, обучающихся по направлению подготовки 080500.62 «Бизнес-информатика» и другим направлениям (специальностям) математического профиля.

*Рецензенты:*
доктор физико-математических наук, профессор *С.И. Дудов,*
кандидат физико-математических наук *С.А. Акимова*

**ISBN 978-5-4345-0215-3**

# Введение

Учебное пособие «Дискретная математика» посвящено изложению основ современной дискретной математики в соответствии с учебным планом (базовая часть профессионального цикла) и рабочей программой данной дисциплины, входящих в состав документации основной образовательной программы по направлению подготовки 080500.62 «Бизнес-информатика» (профили «Информационные системы управления бизнесом» и «Электронный бизнес»).

Дискретная математика – это область математики, в которой изучаются свойства математических моделей объектов, процессов и зависимостей, существующих в реальном мире и применяемых в различных областях знаний. Отличительной чертой этих моделей является возможность их дискретной (т.е. скачкообразно прерывающейся) реализации в виде конечных или потенциально бесконечных структур. Примерами таких структур являются конечные алгебры, графы, автоматы, вычислительные сети функциональных элементов и многие другие. Традиционно дискретная математика имеет большое многообразие разделов, таких как комбинаторика, математическая логика, теория графов, теория автоматов, теория алгоритмов и т.д. Современная дискретная математика является фундаментальной основой математической кибернетики, компьютерных наук, программирования и информационных технологий.

В основу содержания настоящего курса положен принцип актуальности следующих приложений дискретной математики к компьютерной науке и математической кибернетике:

1) теория множеств и алгебра отношений имеют важные приложения к теории структур данных;

2) алгебраические системы являются основой алгебраического аппарата всей компьютерной науки;

3) комбинаторика является важным инструментом теории сложности вычислений;

4) теория кодирования является основой алгебраического аппарата теории связи;

5) теория графов имеет широкие приложения в теории разработки и анализа алгоритмов;

6) алгебра логики и схемы функциональных элементов широко используются при математическом моделировании вычислений;

7) теория автоматов является одним из основных разделов математической кибернетики и важным аппаратом теории вычислений;

8) теория алгоритмов является фундаментальной основой современной математики и, в частности, теории вычислений.

Все эти темы отражены в семи главах пособия, где излагаются основные теоретические положения вышеперечисленных направлений, подробно разбираются многочисленные примеры решения типовых задач и приводятся контрольные вопросы для среза остаточных знаний. Основы математической логики излагаются в учебном пособии [3].

Настоящее учебное пособие окажет существенную помощь студентам направления подготовки 080500.62 «Бизнес-информатика».

ГЛАВА 1

# ТЕОРИЯ МНОЖЕСТВ И АЛГЕБРА ОТНОШЕНИЙ

## 1.1. Множества и действия над ними

При изложении математических дисциплин широко используются основные положения теории множеств. Понятие множества является одним из первоначальных понятий математики и обычно трактуется на интуитивном уровне: *множество* понимается как совокупность объектов, удовлетворяющих некоторому свойству. Множества обозначаются прописными латинскими буквами (возможно с индексами): $A,B,\ldots, A_1, A_2,\ldots$. Объекты, входящие в состав множества, называются его *элементами* и обозначаются строчными латинскими буквами (возможно с индексами): $a,b,\ldots, a_1, a_2,\ldots$. Утверждение «объект $a$ есть элемент множества $A$» символически записывается с помощью *символа принадлежности* $\in$ формулой $a \in A$, которая читается «$a$ принадлежит $A$» или «$a$ – элемент $A$». Если объект $a$ не входит в множество $A$, то пишут $a \notin A$ и говорят, что «$a$ не принадлежит $A$» или «$a$ не является элементом $A$».

Если множество $A$ есть совокупность объектов $x$, удовлетворяющих свойству $P(x)$, то пишут $A = \{x : P(x)\}$.

> **Пример**. Отрезок $[0;1]$ числовой прямой $\boldsymbol{R}$ с концами 0 и 1 есть множество вещественных чисел $x$, удовлетворяющих условию $0 \le x \le 1$. Следовательно, такое множество определяется формулой:
>
> $$[0;1] = \{x : x \in \boldsymbol{R} \text{ и } \ 0 \le x \le 1\}.$$

Конечное множество $A$, состоящее из элементов $a_1,\ldots,a_n$, обозначается также $A = \{a_1,\ldots,a_n\}$. В частности, множество $A$, состоящее из одного элемента $a$, обозначается $A = \{a\}$. Множество, не содержащее элементов, называется *пустым* и обозначается символом $\varnothing$.

**Пример.** Множество делителей числа 10 записывается в виде $\{1,2,5\}$, множество вещественных корней уравнения $x^2-1=0$ записывается в виде $\{-1,1\}$ и множеством вещественных корней уравнения $x^2+1=0$ является пустое множество $\varnothing$.

Для некоторых особо важных множеств используются стандартные обозначения. Так, основные числовые множества натуральных, целых, рациональных и вещественных чисел обозначаются соответственно ***N,Z,Q*** и ***R.*** Символом $\boldsymbol{R}_+$ обозначается множество положительных вещественных чисел.

***Основные действия над множествами.***

1. *Сравнение множеств*: множество $A$ называется *подмножеством* множества $B$, если каждый элемент множества $A$ принадлежит множеству $B$. С помощью *символа включения* $\subset$ этот факт выражается формулой $A\subset B$, которая читается «$A$ – подмножество $B$» или «$A$ включается в $B$».

Если для множеств $A,B$ выполняются включения $A\subset B$ и $B\subset A$, то такие множества состоят из одних и тех же элементов. В этом случае множества $A,B$ называются *равными*. С помощью знака равенства «=» этот факт выражается формулой $A=B$, которая читается «$A$ равно $B$». Если множества $A,B$ не равны, то пишут $A\neq B$.

Множество $A$ называется *собственным подмножеством* множества $B$, если $A\subset B$ и $A\neq B$.

2. *Объединение множеств*: объединением множеств $A$ и $B$ называется множество $A\cup B$, которое состоит из тех и только тех элементов, которые принадлежат хотя бы одному из множеств $A,B$, т.е.

$$A\cup B=\{\, x: x\in A \ \text{ или } \ x\in B\,\}.$$

3. *Пересечение множеств*: пересечением множеств $A$ и $B$ называется множество $A\cap B$, которое состоит из тех и только тех элементов, которые одновременно принадлежат обоим множествам $A$ и $B$, т.е.

$$A\cap B=\{\, x: x\in A \ \text{ и } \ x\in B\,\}.$$

Если $A\cap B=\varnothing$, то множества $A,B$ называются *непересекающимися*.

4. *Вычитание множеств*: разностью множеств $A$ и $B$ называется множество $A\setminus B$, которое состоит из тех и только тех элементов, которые принадлежат множеству $A$, но не принадлежат множеству $B$, т.е.

$$A\setminus B=\{\, x: x\in A \ \text{ и } \ x\notin B\,\}.$$

Для наглядного представления действий над множествами используют их схематическое изображение областями плоскости, которые принято называть *диаграммами Эйлера-Венна*. Например, включение множеств $A \subset B$ схематически изображается диаграммой (рис.1.1), пересечение множеств $A \cap B$ схематически изображается заштрихованной областью на рис.1.2, разность множеств $A \setminus B$ схематически изображается заштрихованной областью на рис.1.3.

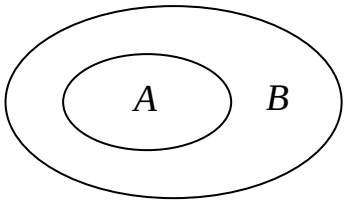



Рис. 1.1.
Включение множеств

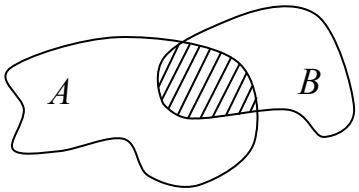



Рис. 1.2.
Пересечение множеств

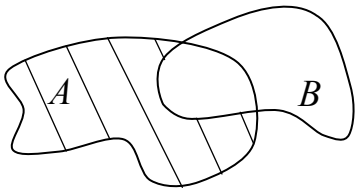



Рис. 1.3.
Разность множеств

**Примеры**.

1. Пусть $A$ – множество простых делителей числа 210 и $B$ – множество простых делителей числа 231. Тогда $A=\{2,3,5,7\}$, $B=\{3,7,11\}$, $A\cap B=\{3,7\}$, $A\cup B=\{2,3,5,7,11\}$, $A\setminus B=\{2,5\}$ и $B\setminus A=\{11\}$. Очевидно, что произведение элементов множества $A\cap B$ равно наибольшему общему делителю чисел 210 и 231 и произведение элементов множества $A\cup B$ равно наименьшему общему кратному этих чисел, т.е. $\text{НОД}(210,221) = 3\cdot 7 = 21$ и $\text{НОК}(210,221) = 2\cdot 3\cdot 5\cdot 7\cdot 11 = 1155$.

2. Пусть $A$ – множество решений неравенства $f(x)\le 0$ и $B$ – множество решений неравенства $g(x)\le 0$. Тогда по определению *система неравенств*

$$\begin{cases} f(x)\le 0, \\ g(x)\le 0 \end{cases}$$

имеет множество решений $A\cap B$ и *совокупность неравенств*

$$\begin{cases} f(x)\le 0, \\ g(x)\le 0 \end{cases}$$

имеет множество решений $A\cup B$.

3. Пусть $X=\{(x,y)\in \boldsymbol{R}^2 : y-x\ge 0\}$ и $Y=\{(x,y)\in \boldsymbol{R}^2 : x+y\ge 0\}$. Построим на координатной плоскости эти множества и найдем их пересечение $X\cap Y$ объединение $X\cup Y$ и разности $X\setminus Y$, $Y\setminus X$.

Для построения множества решений неравенства $y - x \geq 0$ рассмотрим уравнение $y - x = 0$, которое определяет на числовой плоскости линию, разбивающую эту плоскость на две области знакопостоянства выражения $y - x$. В данном случае эта линия является прямой – биссектрисой 1-го и 3-го координатных углов, которая разбивает плоскость на две полуплоскости (рис.1.4).

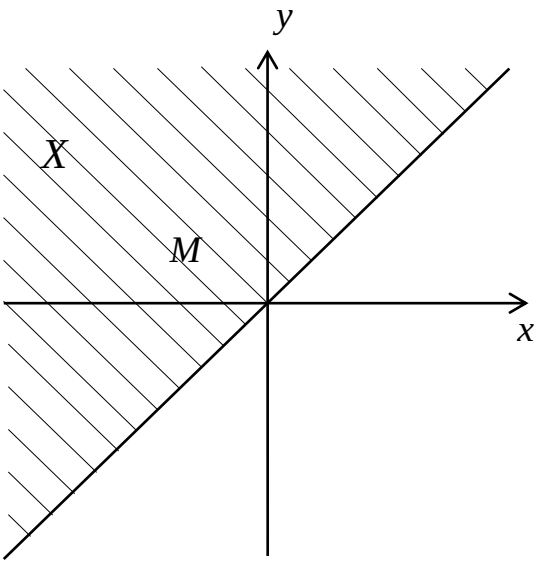



Рис. 1.4.
Множество $X$

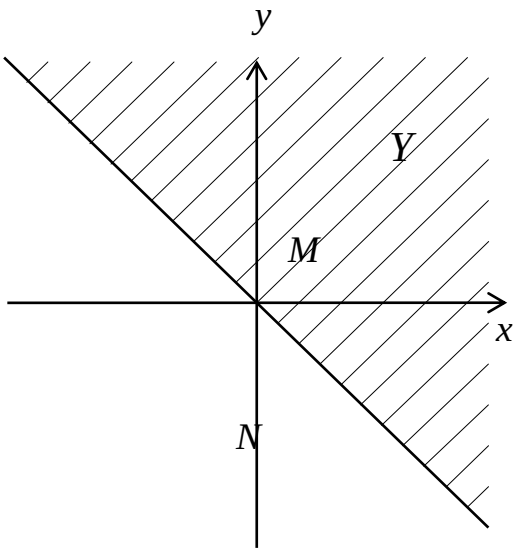



Рис. 1.5.
Множество $Y$

Возьмем произвольную точку в верхней полуплоскости, например точку $M(0;1)$, и определим в ней знак выражения $y - x$: $1 - 0 = 1 > 0$. Так как в точке $M$ выполняется $y - x > 0$, то выражение $y - x$ будет положительно во всей верхней полуплоскости. По аналогии нетрудно проверить, что в нижней полуплоскости выражение $y - x$ будет отрицательно. Таким образом, множество $X$ изображается на рис.1.4 заштрихованной областью.

Для построения множества решений неравенства $x + y \geq 0$ рассмотрим уравнение $x + y = 0$, которое определяет на числовой плоскости прямую – биссектрису 2-го и 4-го координатных углов. Эта линия разбивает плоскость на две полуплоскости (рис.1.5) – области знакопостоянства выражения $x + y$.

С помощью пробных точек (например, $M(0;1)$ – в верхней полуплоскости и $N(0;-1)$ – в нижней полуплоскости) убеждаемся, что выражение $x + y$ в верхней полуплоскости положительно, а

в нижней полуплоскости отрицательно. Значит, множество $Y$ изображается на рис.1.5 заштрихованной областью.

Тогда пересечение $X \cap Y$ и объединение $X \cup Y$ изображаются заштрихованными областями на рис.1.6 и 1.7.

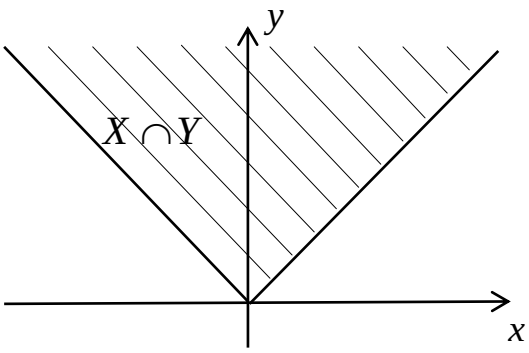



Рис. 1.6.
Пересечение множеств $X,Y$

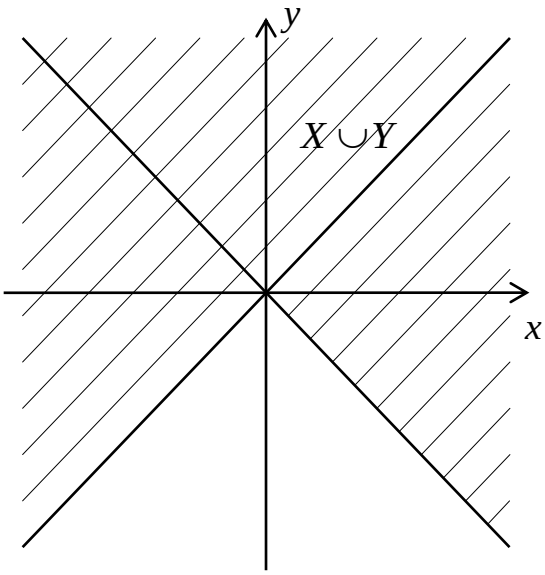



Рис. 1.7.
Объединение множеств $X,Y$

Разности множеств $X \setminus Y, Y \setminus X$ изображаются заштрихованными областями на рис.1.8 и 1.9.

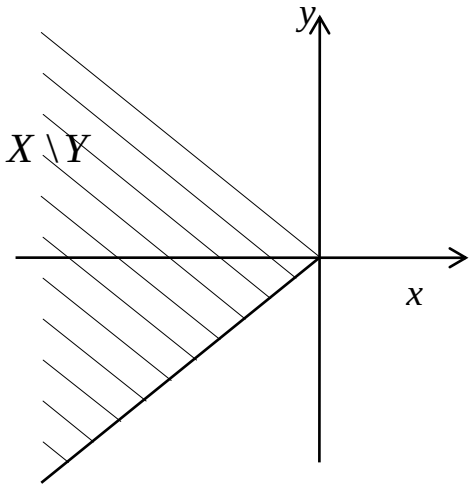



Рис. 1.8.
Разность множеств $X$ и $Y$

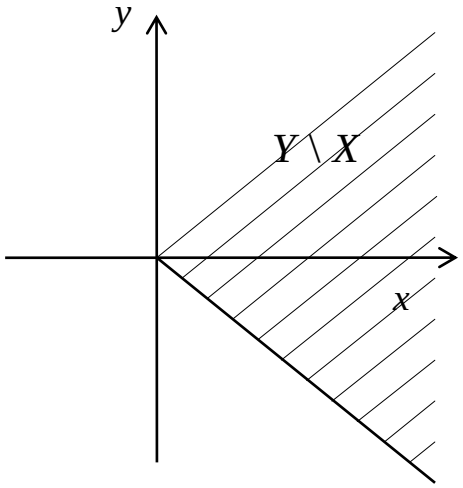



Рис. 1.9.
Разность множеств $Y$ и $X$

***Свойства операций над множествами.***

С помощью диаграмм Эйлера-Венна легко проверяются следующие равенства множеств.

1. $A \cup B = B \cup A$, $A \cap B = B \cap A$ – свойства *коммутативности* объединения и пересечения (или *перестановочные законы*);

2. $A\cup(B\cup C)=(A\cup B)\cup C$, $A\cap(B\cap C)=(A\cap B)\cap C$ – свойства *ассоциативности* объединения и пересечения (или *сочетательные законы*);

3. $A\cup A=A$, $A\cap A=A$ – свойства *идемпотентности* объединения и пересечения;

4. $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$, $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ – свойства дистрибутивности соответственно пересечения относительно объединения и объединения относительно пересечения (или *распределительные законы*);

5. $(A\cap B)\cup A=A$, $(A\cup B)\cap A=A$ – *законы поглощения*;

6. $A\setminus(B\cap C)=(A\setminus B)\cup(A\setminus C)$, $A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C)$ – *законы де Моргана*;

7. $A\cup\varnothing=A$, $A\cap\varnothing=\varnothing$ – характерные свойства пустого множества.

Таким образом, с операциями объединения $\cup$ и пересечения $\cap$ множеств можно оперировать по известным из элементарной математики свойствам операций сложения + и умножения × вещественных чисел. Принципиальным отличием теоретико-множественных операций от арифметических операций являются их свойства идемпотентности и законы поглощения. Кроме того, из перечисленных выше свойств видно, что для теоретико-множественных операций объединения $\cup$ и пересечения $\cap$ справедлив *принцип двойственности*: свойство таких операций остается справедливым при одновременной замене символов этих операций друг на друга (символа $\cup$ – на символ $\cap$ и символа $\cap$ – на символ $\cup$).

В заключение отметим, что действия объединения и пересечения двух множеств легко обобщаются для любого семейства множеств. Если $I$ – непустое множество и каждому элементу $i\in I$ поставлено в соответствие некоторое множество $A_i$, то множество $\{A_i : i\in I\}$ называется *семейством множеств* (индексированным элементами множества $I$) и обозначается $\{A_i\}_{i\in I}$ или просто $\{A_i\}$. В частности, если $I=\{1,..n\}$ – конечное множество, то семейство множеств $\{A_i\}_{i\in I}$ состоит из $n$ множеств $A_1,...,A_n$. Если же $I=\boldsymbol{N}$, то семейство множеств $\{A_i\}_{i\in I}$ есть бесконечная последовательность множеств $A_1, A_2,...,A_n,....$

**Определение.** *Объединением семейства множеств* $\{A_i\}_{i\in I}$ называется множество $\bigcup\limits_{i\in I}A_i$, которое состоит из тех и только тех элементов, которые принадлежат хотя бы одному из множеств $A_i$. В этом случае семейство множеств $\{A_i\}_{i\in I}$ называется также *покрытием*

множества $A=\bigcup_{i\in I}A_i$. Покрытие называется *разбиением,* если его элементы попарно не пересекаются между собой, т.е. $A_i\cap A_j=\varnothing$ при всех различных $i, j\in I$. В этом случае говорят также, что множество $A$ *разбивается на классы* $A_i$ $(i\in I)$.

**Определение.** *Пересечением семейства множеств* $\{A_i\}_{i\in I}$ называется множество $\bigcap_{i\in I}A_i$, которое состоит из тех и только тех элементов, которые принадлежат всем множествам $A_i$ для любых $i\in I$.

В частности, если $I=\{1,..n\}$, то $\bigcup_{i\in I}A_i=A_1\cup...\cup A_n$ – объединение $n$ множеств $A_1,...,A_n$ и $\bigcap_{i\in I}A_i=A_1\cap...\cap A_n$ – пересечение $n$ множеств $A_1,...,A_n$.

**Примеры.**

1. Если каждому натуральному числу $n\in \boldsymbol{N}$ поставить в соответствие отрезок $A_n=[0;1-1/n]$, то объединение бесконечной последовательности множеств $A_1, A_2,...,A_n,...$ будет равно числовому промежутку $[0;1)$.

2. Если каждому натуральному числу $n\in \boldsymbol{N}$ поставить в соответствие числовой промежуток $A_n=[0;1/n)$, то пересечение бесконечной последовательности множеств $A_1, A_2,...,A_n,...$ будет равно одноэлементному множеству $\{0\}$.

3. Если каждому целому числу $n\in \boldsymbol{Z}$ поставить в соответствие числовой промежуток $A_n=[n;n+1]$, то семейство множеств $\{A_n\}_{n\in \boldsymbol{Z}}$ образует покрытие множества вещественных чисел $\boldsymbol{R}$, так как $\bigcup_{i\in \boldsymbol{Z}}A_i=\boldsymbol{R}$. Если же каждому целому числу $n\in \boldsymbol{Z}$ поставить в соответствие числовой промежуток $B_n=[n;n+1)$, то семейство множеств $\{B_n\}_{n\in \boldsymbol{Z}}$ образует разбиение множества вещественных чисел $\boldsymbol{R}$, так как $\bigcup_{i\in \boldsymbol{Z}}B_i=\boldsymbol{R}$ и $B_i\cap B_j=\varnothing$ при всех различных $i, j\in \boldsymbol{Z}$.

4. Множества $\boldsymbol{N_2}$ и $\boldsymbol{N_1}$ соответственно четных и нечетных натуральных чисел образуют двухэлементное разбиение множества натуральных чисел $\boldsymbol{N}$. Другими словами, множество $\boldsymbol{N}$ разбивается на два класса – $\boldsymbol{N_2}$ и $\boldsymbol{N_1}$.

5. Множество вещественных чисел $\boldsymbol{R}$ разбивается на бесконечное множество классов чисел, имеющих одинаковые дробные части.

6. Множество студентов вуза разбивается на классы студентов, обучающихся в одной группе.

## 1.2. Бинарные отношения и отображения

Как уже отмечалось выше, множество $A$, состоящее из элементов $a$ и $b$, обозначается $A=\{a,b\}$. Так как $\{a,b\}=\{b,a\}$, то множество $\{a,b\}$ называется *неупорядоченной парой элементов* $a$ и $b$. С другой стороны, для элементов $a$ и $b$ существует множество $(a,b)$, которое называется *упорядоченной парой элементов* $a,b$ и удовлетворяет свойству $(a,b)=(c,d)$ в том и только том случае, если $a=c$ и $b=d$.

В общем случае для любого натурального числа $n$ и любых элементов $a_1,...,a_n$ существует множество $(a_1,...,a_n)$, которое называется *упорядоченным набором* $n$ *элементов* $a_1,...,a_n$ и удовлетворяет свойству $(a_1,...,a_n)=(b_1,...,b_n)$ в том и только том случае, если $a_1=b_1,\ldots,a_n=b_n$.

**Определение.** *Декартовым* (или *прямым*) *произведением* $n$ множеств $A_1,...,A_n$ называется множество $A_1\times...\times A_n$, которое состоит из всех таких упорядоченных наборов $n$ элементов $(a_1,...,a_n)$, что $a_1\in A_1,\ldots,a_n\in A_n$. Если все множества $A_1,...,A_n$ равны одному и тому же множеству $A$, то прямое произведение $A\times...\times A$ $n$ множителей $A$ называется $n$-ой *декартовой степенью* множества $A$ и обозначается символом $A^n$.

В частности, декартово произведение двух множеств $A$ и $B$ есть множество $A\times B$, которое состоит из всех таких упорядоченных пар $(a,b)$, что $a\in A$ и $b\in B$. Если $A=B$, то декартово произведение $A\times B$ называется *декартовым квадратом* множества $A$ и обозначается символом $A^2$.

**Определение.** Подмножества декартова произведения $A_1\times...\times A_n$ множеств $A_1,...,A_n$ называются *n-арными отношениями* между элементами множеств $A_1,...,A_n$ и обозначаются строчными греческими буквами (возможно с индексами): $\rho,\sigma,...,\rho_1,\rho_2,...$ .

В частности, при $n=1$ подмножества декартова произведения $A_1\times...\times A_n=A_1$ называются *унарными отношениями* между элементами множества $A_1$ и при $n=2$ подмножества декартова произведения $A_1\times...\times A_n=A_1\times A_2$ называются *бинарными отношениями* между элементами множеств $A_1,A_2$.

Для бинарного отношения $\rho\subset A\times B$ *область определения* обозначается символом $D_\rho$ и определяется по формуле:

$$D_\rho=\{a:(a,b)\in\rho \text{ для некоторого } b\in B\}.$$

Для бинарного отношения $\rho \subset A \times B$ *множество значений* обозначается символом $E_\rho$ и определяется по формуле:

$$E_\rho = \{b : (a,b) \in \rho \text{ для некоторого } a \in A\}.$$

Для любого подмножества $X \subset A$ множество

$$\rho(X) = \{b \in B : (x,b) \in \rho \text{ для некоторого } x \in X\}$$

называется *образом* множества $X$ относительно отношения $\rho$. Образ одноэлементного множества $X = \{a\}$ относительно отношения $\rho$ обозначается символом $\rho(a)$ и называется также *срезом* отношения $\rho$ через элемент $a$.

**Определение.** Бинарное отношение $\rho \subset A \times B$ называется:

– *всюду определенным,* если его область определения $D_\rho = A$;

– *однозначным* (или *частичной функцией, частичным отображением* множества $A$), если для каждого элемента $a \in D_\rho$ условие $(a,b) \in \rho$ выполняется точно для одного элемента $b \in B$, который называется *значением функции* $\rho$ для элемента $a$ и обозначаеется символом $\rho(a)$;

– *взаимно однозначным,* если оно однозначно и для каждого элемента $b \in E_\rho$ условие $(a,b) \in \rho$ выполняется точно для одного элемента $a \in A$, который называется *прообразом элемента* $b$ для функции $\rho$ и обозначается символом $\rho^{-1}(b)$.

**Определение.** Всюду определенное и однозначное бинарное отношение $\varphi \subset A \times B$ обозначается символом $\varphi : A \to B$ и называется *отображением* множества $A$ в множество $B$, или (*всюду определенной*) *функцией* на множестве $A$ со значениями в множестве $B$.

**Определение.** Отображение $\varphi : A \to B$ называется:

– *отображением* множества $A$ на множество $B$ (или *сюръекцией*), если его множество значений $E_\varphi = B$;

– *взаимно однозначным отображением* множества $A$ в множество $B$ (или *инъекцией*), если оно является взаимно однозначным бинарным отношением;

– *взаимно однозначным отображением* множества $A$ на множество $B$ (или *биекцией*), если оно является взаимно однозначным отображением $A$ на $B$;

– *преобразованием* множества $A$, если $A = B$;

– *перестановкой* множества $A$, если оно является взаимно однозначным отображением множества $A$ на себя.

**Примеры.**

1. Пусть $A$ – множество студентов вуза и $B$ – множество студенческих групп этого вуза. Рассмотрим бинарное отношение $\rho \subset A \times B$ принадлежности студентов группе, т.е. для элементов $a \in A$, $b \in B$ условие $(a,b) \in \rho$ означает, что студент $a$ обучается в группе $b$. Тогда $D_\rho$ есть множество всех таких студентов $a \in A$, которые обучаются по крайней мере в одной группе, и $E_\rho$ есть множество всех таких групп $b \in B$, в которых обучается хотя бы один студент. Ясно, что в этом случае отношение $\rho$ является всюду определенным и однозначным, так как каждый студент $a \in A$ обучается точно в одной из групп вуза, и $E_\rho = B$, так как в каждой группе $b \in B$ обучается хотя бы один студент. Таким образом, $\rho$ – отображение множества $A$ на множество $B$.

2. Пусть $A$ – множество учеников школы и $B$ – множество кружков центра дополнительного образования. Рассмотрим бинарное отношение $\rho \subset A \times B$ посещаемости учениками кружков, т.е. для элементов $a \in A$, $b \in B$ условие $(a,b) \in \rho$ означает, что ученик $a$ посещает кружок $b$. Тогда $D_\rho$ есть множество всех таких учеников $a \in A$, которые посещают, по крайней мере, один кружок, и $E_\rho$ есть множество всех таких кружков $b \in B$, которые посещает хотя бы один ученик. В общем случае данное отношение $\rho$ не является всюду определенным, так как некоторые ученики $a \in A$ могут не посещать ни один из кружков, и не является однозначным, так как некоторые ученики могут посещать несколько кружков.

3. Пусть $A$ – множество студентов вуза, обучающихся на 1-м курсе по специальности «Математика», и $B$ – множество дисциплин учебного плана по специальности «Математика». Рассмотрим бинарное отношение $\rho \subset A \times B$ сдачи студентами экзаменов в зимнюю сессию, т.е. для элементов $a \in A$, $b \in B$ условие $(a,b) \in \rho$ означает, что студент $a$ сдал в зимнюю сессию экзамен по специальности $b$. Тогда $D_\rho$ есть множество всех таких студентов $a \in A$, которые сдали по крайней мере один экзамен в зимнюю сессию, и $E_\rho$ есть множество всех таких дисциплин $b \in B$, экзамен по которым предусмотрен в зимнюю сессию на 1-м курсе учебным планом специальности «Математика» (предполагается, что все экзамены сдаются по крайней мере

одним студентом $a \in A$). В общем случае данное отношение $\rho$ не является всюду определенным, так как некоторые студенты $a \in A$ могут не сдать ни одного экзамена, и не является однозначным, так как учебным планом в сессию может быть предусмотрено несколько экзаменов, которые сданы успевающими студентами.

***Основные действия над бинарными отношениями.***

1. *Теоретико-множественные операции*: для бинарных отношений, как для множеств, определены действия сравнения, объединения, пересечения и вычитания.

2. *Обращение бинарных отношений*: обратным для бинарного отношения $\rho \subset A \times B$ называется бинарное отношение $\rho^{-1} \subset B \times A$, которое определяется по формуле: $\rho^{-1} = \{(b,a) : (a,b) \in \rho\}$.

3. *Композиция бинарных отношений*: композицией бинарных отношений $\rho \subset A \times B$ и $\sigma \subset B \times C$ называется бинарное отношение $\rho\sigma \subset A \times C$, которое определяется по формуле:

$$\rho\sigma = \{(a,c) : (a,b) \in \rho \text{ и } (b,c) \in \sigma \text{ для некоторого } b \in B\}.$$

В частности, для отображений $\varphi : A \to B$, $\psi : B \to C$ композиция $\varphi\psi$ является отображением множества $A$ в множество $C$, которое каждому элементу $a \in A$ ставит в соответствие единственный элемент $(\varphi\psi)(a) = \psi(\varphi(a))$ множества $C$. Иногда для обозначения композиции отображений используется правосторонняя запись $\psi \circ \varphi$, при которой для любого $a \in A$ выполняется равенство: $(\psi \circ \varphi)(a) = \psi(\varphi(a))$.

Композиция $\varphi\psi$ называется также *сложной функцией*, полученной подстановкой функции $\varphi$ в функцию $\psi$.

Легко видеть, что для любых бинарных отношений $\rho \subset A \times B$, $\sigma \subset B \times C$ и $\gamma \subset C \times D$ выполняется свойство $(\rho\sigma)\gamma = \rho(\sigma\gamma)$, которое называется *ассоциативностью композиции*.

В случае $A=B$ подмножества декартова квадрата $A \times A$ называются также *бинарными отношениями* на множестве $A$. Пример бинарного отношения на множестве $A$ дает *тождественное отношение* на этом множестве, которое обозначается символом $\Delta_A$ и состоит из всех таких упорядоченных пар $(a,b)$, что $a \in A$ и $a = b$. Очевидно, что для любого бинарного отношения $\rho$ на множестве $A$ выполняются равенства $\rho\Delta_A = \Delta_A\rho = \rho$.

**Определение.** Бинарное отношение $\rho \subset A \times A$ называется:

– *рефлексивным*, если $\Delta_A \subset \rho$, т.е. $(a,a) \in \rho$ для любого $a \in A$;

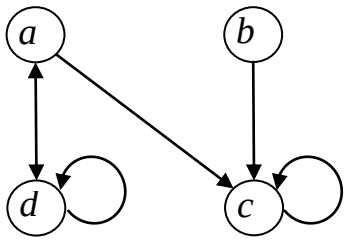
– *симметричным*, если $\rho^{-1} \subset \rho$, т.е. из $(a,b) \in \rho$ следует $(b,a) \in \rho$;

– *антисимметричным*, если $\rho \cap \rho^{-1} \subset \Delta_A$, т.е. из $(a,b) \in \rho$ и $(b,a) \in \rho$ следует $a=b$;

– *транзитивным*, если $\rho\rho \subset \rho$, т.е. из $(a,b) \in \rho$ и $(b,c) \in \rho$ следует $(a,c) \in \rho$.

Заданные на конечном множестве бинарные отношения наглядно изображают специальными рисунками – графами. *Графом* бинарного отношения $\rho$ на множестве $A=\{a_1,...,a_n\}$ называется плоская фигура, которая состоит из $n$ выделенных точек, изображающих элементы $a_1,...,a_n$ и называющихся *вершинами* графа, и у которой вершины $a_i, a_j$, удовлетворяющие условию $(a_i,a_j) \in \rho$, соединяются стрелкой, направленной от $a_i$ к $a_j$ и называемой *дугой* графа. При этом вершины $a_i$ и $a_j$ называются соответственно *началом* и *концом* такой дуги. Дуга, у которой начало и конец совпадают, называется *петлей*. В случае, если $(a_i,a_j) \in \rho$ и $(a_j,a_i) \in \rho$, две противоположно направленные стрелки, соединяющие вершины $a_i, a_j$, изображаются одной стрелкой с двумя противоположными направлениями.

**Пример.** Граф заданного на множестве $A=\{a,b,c,d\}$ бинарного отношения $\rho=\{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ имеет следующий вид:




Ясно, что у графа рефлексивного бинарного отношения каждая вершина имеет петлю, у графа симметричного бинарного отношения вместе с каждой стрелкой от $a_i$ к $a_j$ имеется обратная стрелка от $a_j$ к $a_i$, у графа антисимметричного бинарного отношения любые две вершины $a_i$, $a_j$ могут соединяться только одной стрелкой, у графа транзитивного бинарного отношения вместе с каждой парой стрелок от $a_i$ к $a_j$ и от $a_j$ к $a_k$ имеется стрелка от $a_i$ к $a_k$.

С целью упрощения вычисления результатов действий над бинарными отношениями используется представление бинарных отношений специальными таблицами, называемыми матрицами. *Матрицей* бинарного отношения $\rho$ между элементами множеств $A=\{a_1,...,a_m\}$ и $B=\{b_1,...,b_n\}$ называется прямоугольная таблица $M(\rho)$, состоящая из $m$ строк, помеченных элементами множества $A$, и $n$ столбцов, помеченных элементами множества $B$, в которой на пересечении $i$-ой строки и $j$-го столбца стоит элемент $[M(\rho)]_{ij}$ из множества $\{0,1\}$, определяемый по правилу:

$$[M(\rho)]_{ij}=\begin{cases}1, & \text{если } (a_i,b_j)\in\rho,\\ 0, & \text{в противном случае.}\end{cases}$$

Таким образом, матрица $M(\rho)$ бинарного отношения $\rho$ имеет вид:

$$M(\rho)=\begin{array}{c} \\ a_1\\ \vdots\\ a_m\end{array}\begin{array}{c}\begin{array}{ccc} b_1 & \dots & b_n\end{array}\\ \begin{pmatrix}[M(\rho)]_{11} & \dots & [M(\rho)]_{1n}\\ \dots & \dots & \dots\\ [M(\rho)]_{m1} & \dots & [M(\rho)]_{mn}\end{pmatrix}\end{array}.$$

**Пример.** Матрица заданного на множестве $A=\{a,b,c,d\}$ бинарного отношения $\rho=\{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ имеет следующий вид:

$$M(\rho)=\begin{array}{c} \\ a\\ b\\ c\\ d\end{array}\begin{array}{c}\begin{array}{cccc} a & b & c & d\end{array}\\ \begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0\\ 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\end{pmatrix}\end{array}.$$

Для простоты записи матрицы бинарного отношения $M(\rho)$ обычно явно не указывается разметка ее строк и столбцов.

Легко видеть, что для бинарных отношений $\rho,\sigma\subset A\times B$ выполняются следующие свойства:

1) $\rho\subset\sigma$ в том и только том случае, если $[M(\rho)]_{ij}\le[M(\sigma)]_{ij}$ для всех $1\le i\le m, 1\le j\le n$;

2) элементы матрицы $M(\rho\cap\sigma)$ вычисляются по формуле:

$$[M(\rho\cap\sigma)]_{ij}=[M(\rho)]_{ij}\cdot[M(\sigma)]_{ij};$$

3) элементы матрицы $M(\rho\cup\sigma)$ вычисляются по формуле:

$$[M(\rho\cup\sigma)]_{ij}=\max\{[M(\rho)]_{ij},[M(\sigma)]_{ij}\}.$$

Кроме того, если $\rho \subset A \times B$ и $\sigma \subset B \times C$ для некоторого множества $C = \{c_1,...,c_p\}$, то элементы матрицы $M(\rho\sigma)$ вычисляются по формуле:

$$[M(\rho\sigma)]_{ij} = \max_{1 \le k \le n} \{[M(\rho)]_{ik} \cdot [M(\sigma)]_{kj}\}.$$

**Примеры.**

1. Пусть $A$ – множество студентов, сдающих экзамены по алгебре и геометрии. Рассмотрим бинарное отношение $\rho \subset A \times A$ сравнения успеваемости студентов по алгебре, т.е. для элементов $a,b \in A$ условие $(a,b) \in \rho$ означает, что по алгебре успеваемость студента $a$ ниже, чем успеваемость студента $b$. Ясно, что такое отношение транзитивно. Аналогичными свойствами обладает бинарное отношение $\sigma \subset A \times A$ сравнения успеваемости студентов по геометрии, т.е. для элементов $a,b \in A$ условие $(a,b) \in \sigma$ означает, что по геометрии успеваемость студента $a$ ниже, чем успеваемость студента $b$. Рассмотрим отношения $\rho \cap \sigma$ и $\rho \cup \sigma$. По определению для элементов $a,b \in A$ условие $(a,b) \in \rho \cap \sigma$ означает, что успеваемость студента $a$ ниже, чем успеваемость студента $b$ как по алгебре, так и по геометрии, и условие $(a,b) \in \rho \cup \sigma$ означает, что успеваемость студента $a$ ниже, чем успеваемость студента $b$ либо по алгебре, либо по геометрии. Легко видеть, что отношение $\rho \cap \sigma$ всегда будет транзитивным, но отношение $\rho \cup \sigma$ транзитивным может не быть, так как возможно наличие таких элементов $a,b,c \in A$, что $(a,b) \in \rho$, $(b,c) \in \sigma$ и $(a,c) \notin \rho \cup \sigma$. Например, это выполняется в случае, если студент $a$ сдал алгебру на «4» и геометрию на «5», студент $b$ сдал алгебру на «5» и геометрию на «3», студент $c$ сдал алгебру на «3» и геометрию на «4». Графы таких отношений $\rho,\sigma$ для множества $A = \{a,b,c\}$ изображены на рис.1.10, 1.11.

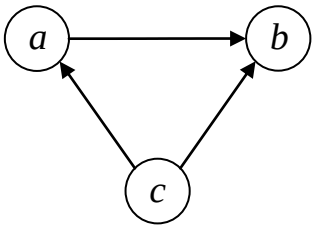



Рис. 1.10.
Граф отношения $\rho$

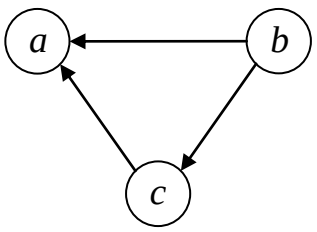



Рис.1. 11.
Граф отношения $\sigma$

Графы отношений $\rho \cap \sigma$ и $\rho \cup \sigma$ изображены на рис.1.12,1.13.

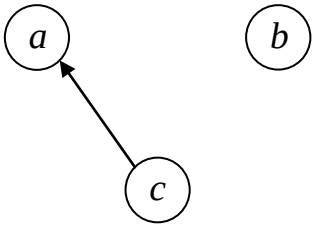



Рис.1.12.
Граф отношения $\rho \cap \sigma$

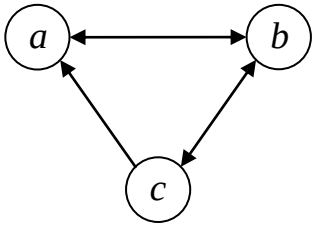



Рис.1.13.
Граф отношения $\rho \cup \sigma$

Очевидно, что данные бинарные отношения представляются матрицами:

$$M(\rho) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \; M(\sigma) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$M(\rho \cap \sigma) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \; M(\rho \cup \sigma) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

2. Пусть четыре города $A,B,C,D$ обслуживаются двумя авиакомпаниями «Ро» и «Сигма». При этом авиакомпания «Ро» выполняет прямые рейсы: из $A$ в $B$, из $B$ в $C$ и $D$, из $C$ в $B$, и авиакомпания «Сигма» выполняет прямые рейсы: из $A$ в $B$, из $B$ в $C$, из $D$ в $C$. Тогда отношения $\rho$ и $\sigma$ связи городов из множества $X = \{A,B,C,D\}$ прямыми рейсами соответственно авиакомпаний «Ро» и «Сигма» имеют вид:

$$\rho = \{(A,B),(B,C),(B,D),(C,B)\} \text{ и } \sigma = \{(A,B),(B,C),(D,C)\}.$$

Графы таких отношений $\rho,\sigma$ изображены на рис.1.14,1.15.

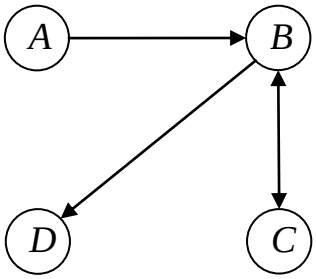



Рис.1.14.
Граф отношения $\rho$

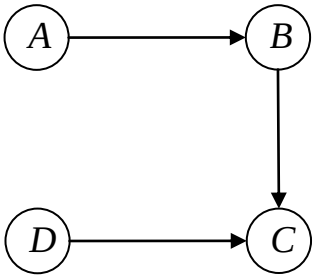



Рис.1.15.
Граф отношения $\sigma$

Матрицы таких отношений $\rho,\sigma$ имеют вид:

$$M(\rho)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\0&1&0&0\\0&0&0&0\end{pmatrix},\ M(\sigma)=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&0\\0&0&1&0\end{pmatrix}.$$

В данном примере $\rho^{-1}$ является отношением связи множества городов $X=\{A,B,C,D\}$ обратными рейсами авиакомпания «Ро» и $\rho\sigma$ является отношением связи этих городов стыковочными рейсами авиакомпаний «Ро» и «Сигма». Графы таких отношений $\rho^{-1},\rho\sigma$ изображены на рис.1.16,1.17.

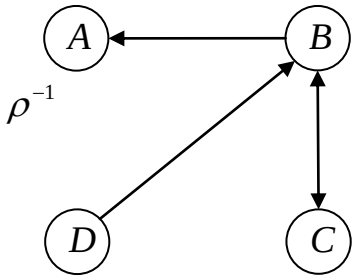



Рис.1.16.
Граф отношения $\rho^{-1}$

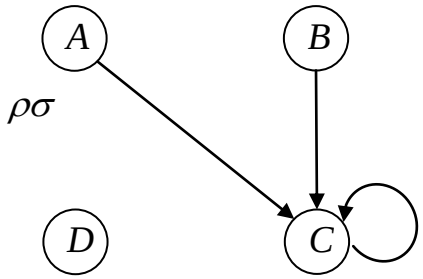



Рис.1.17.
Граф отношения $\rho\sigma$

Матрицы таких отношений $\rho^{-1},\rho\sigma$ имеют вид:

$$M(\rho^{-1})=\begin{pmatrix}0&0&0&0\\1&0&1&0\\0&1&0&0\\0&1&0&0\end{pmatrix},\ M(\rho\sigma)=\begin{pmatrix}0&0&1&0\\0&0&1&0\\0&0&1&0\\0&0&0&0\end{pmatrix}.$$

## 1.3. Отношение эквивалентности и фактор-множество

**Определение.** Бинарное отношение $\varepsilon$ на множестве $A$ называется *отношением эквивалентности* (или просто *эквивалентностью*), если оно рефлексивно, симметрично и транзитивно.

Для обозначения эквивалентности $\varepsilon$ используется инфиксная запись с помощью символа $\equiv$, т.е. вместо $(a,b)\in\varepsilon$ пишут $a\equiv b(\varepsilon)$ или просто $a\equiv b$ (читается «$a$ эквивалентно $b$ относительно эквивалентности $\varepsilon$» или просто «$a$ эквивалентно $b$»).

Срезы $\varepsilon(a)$ отношения эквивалентности $\varepsilon$ через элементы $a \in A$ называются *классами эквивалентности* по отношению $\varepsilon$ и сокращенно обозначаются символом $[a]$. Множество всех таких классов эквивалентности $\{[a]: a \in A\}$ называется *фактор-множеством* множества $A$ по эквивалентности $\varepsilon$ и обозначается символом $A/\varepsilon$.

Отношения эквивалентности характеризуются свойством: для любых элементов $a,b \in A$ классы эквивалентности $[a],[b]$ либо не пересекаются, либо совпадают, т.е. условие $[a] \cap [b] \neq \varnothing$ влечет $[a] = [b]$. Таким образом, множество всех классов эквивалентности $A/\varepsilon = \{[a]: a \in A\}$ образует семейство непересекающихся подмножеств множества $A$, объединение которого дает все множество $A$ и которое называется *разбиением множества* $A$ .

***Теорема.*** Непустое семейство $\{A_i : i \in I\}$ подмножеств множества $A$ в том и только том случае является разбиением множества $A$, если это семейство является фактор-множеством некоторого отношения эквивалентности $\varepsilon$ на множестве $A$.

**Определение.** Подмножество $T \subset A$ называется *полной системой представителей классов* эквивалентности $\varepsilon$ на множестве $A$, если выполняются следующие два условия:

1)каждый элемент множества $A$ эквивалентен некоторому элементу множества $T$ , т.е. $\varepsilon(T) = A$;

2)различные элементы множества $T$ неэквивалентны между собой, т.е. для любых $t_1, t_2 \in T$ из условия $t_1 \equiv t_2(\varepsilon)$ следует $t_1 = t_2$.

В этом случае классы эквивалентности $[t] \in A/\varepsilon$, содержащие элементы $t \in T$, могут быть отождествлены со своими представителями $t$ и фактор-множество $A/\varepsilon$ может быть отождествлено с множеством $T$.

**Примеры.**

1. Пусть $A$ – множество шаров в коробке, состоящее из 7 красных, 5 синих и 8 зеленых шаров. Определим на множестве $A$ отношение $\varepsilon$ по формуле: для любых шаров $a,b \in A$ условие $a \equiv b(\varepsilon)$ означает, что шары $a,b$ одного цвета. Легко видеть, что отношение $\varepsilon$ рефлексивно, симметрично и транзитивно, т.е. является эквивалентностью на множестве $A$. Ясно, что любой красный шар $a_к \in A$ определяет класс эквивалентности $[a_к]$, состоящий из 7 красных шаров, любой синий шар $a_с \in A$ определяет класс эквивалентности $[a_с]$, состоящий из 5 синих шаров и любой зеле-

ный шар $a_з \in A$ определяет класс эквивалентности $[a_з]$, состоящий из 8 зеленых шаров. Значит, фактор-множество $A/\varepsilon$ состоит из трех элементов $[a_к],[a_с],[a_з]$ и может быть отождествлено с *полной системой представителей классов* эквивалентности $\varepsilon$ на множестве $A$, состоящей из трех разноцветных шаров $\{a_к, a_с, a_з\}$, или просто с множеством трех цветов $\{красный, синий, зеленый\}$.

2. Пусть $A = \boldsymbol{Z}$ – множество целых чисел. Определим на множестве $\boldsymbol{Z}$ отношение $\varepsilon$ по формуле: для любых $a,b \in \boldsymbol{Z}$ условие $a \equiv b(\varepsilon)$ означает, что числа $a,b$ имеют одинаковые остатки при делении на число 3, т.е. разность $a–b$ кратна числу 3. Легко видеть, что отношение $\varepsilon$ рефлексивно, симметрично и транзитивно, т.е. является эквивалентностью на множестве $\boldsymbol{Z}$. Ясно, что число 0 определяет класс эквивалентности $[0] = \{0, \pm 3, \pm 6, \ldots\}$, число 1 – класс эквивалентности $[1] = \{1, 1 \pm 3, 1 \pm 6, \ldots\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, число 2 – класс эквивалентности $[2] = \{2, 2 \pm 3, 2 \pm 6, \ldots\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$. Так как этими множествами исчерпываются все классы данной эквивалентности $\varepsilon$, то фактор-множество $\boldsymbol{Z}/\varepsilon$ состоит из трех элементов $[0],[1],[2]$ и может быть отождествлено с трехэлементным множеством $\{0,1,2\}$.

**Определение.** *Ядром отображения* $\varphi: A \to B$ называется бинарное отношение $\ker\varphi$ на множестве $A$, которое определяется по формуле:

$$\ker\varphi = \{(a,b) \in A^2 : \varphi(a) = \varphi(b)\}.$$

Легко видеть, что отношение $\ker\varphi$ рефлексивно, симметрично и транзитивно, т.е. является эквивалентностью на множестве $A$. Ясно, что каждый элемент $a \in A$ определяет класс эквивалентности

$$[a] = \{b \in A : \varphi(a) = \varphi(b)\} = \varphi^{-1}(\varphi(a)),$$

который является прообразом элемента $\varphi(a)$ для функции $\varphi$. Значит, фактор-множество $A/\ker\varphi$ состоит из элементов $\varphi^{-1}(b)$ для всех $b \in E_\varphi$ и может быть отождествлено с множеством $E_\varphi$.

**Определение.** Пусть $\varepsilon$ – отношение эквивалентности на множестве $A$. *Каноническим отображением* эквивалентности $\varepsilon$ называется отображение $\mathrm{nat}\,\varepsilon$ (от англ. *natural* – канонический) множества $A$ на фактор-множество $A/\varepsilon$, которое каждому элементу $a \in A$ ставит в соответствие содержащий его класс эквивалентности $[a]$.

Легко видеть, что выполняется равенство: $\ker \mathrm{nat}\,\varepsilon = \varepsilon$.

## 1.4. Отношение порядка и упорядоченное множество

**Определение**. Бинарное отношение $\omega$ на множестве $A$ называется *отношением порядка* (или просто *порядком*), если оно рефлексивно, транзитивно и антисимметрично. Для обозначения порядка $\omega$ используется инфиксная запись с помощью символа $\le$: вместо $(a,b)\in\omega$ принято писать $a\le b(\omega)$ или просто $a\le b$ (читается «$a$ меньше или равно $b$ относительно порядка $\omega$»).

Множество $A$ с заданным на нем отношением порядка $\le$ называется *упорядоченным множеством* и обозначается $A=(A,\le)$ или просто $(A,\le)$.

**Определение**. Подмножество $X$ упорядоченного множества $(A,\le)$ называется *ограниченным сверху,* если найдется такой элемент $a\in A$, что $x\le a$ для всех $x\in X$. В этом случае элемент $a$ называется *верхней гранью* множества $X$. Если для множества $X$ существует наименьшая верхняя грань, то она обозначается символом $\sup X$ (читается «супремум множества $X$») и называется *точной верхней гранью* множества $X$. В случае, когда $\sup X\in X$, значение $\sup X$ является *наибольшим элементом* множества и обозначается $\max X$.

**Определение**. Подмножество $X$ упорядоченного множества $(A,\le)$ называется *ограниченным снизу,* если найдется такой элемент $a\in A$, что $a\le x$ для всех $x\in X$. В этом случае элемент $a$ называется *нижней гранью* множества $X$. Если для множества $X$ существует наибольшая нижняя грань, то она обозначается символом $\inf X$ (читается «инфимум множества $X$») и называется *точной нижней гранью* множества $X$. В случае, когда $\inf X\in X$, значение $\inf X$ является *наименьшим элементом* множества и обозначается $\min X$.

Если само упорядоченное множество $(A,\le)$ ограничено сверху (соответственно, снизу), то его верхняя (соответственно, нижняя) грань является *наибольшим* (соответственно, *наименьшим*) *элементом* множества $A$ и обозначается символом 1 (соответственно, 0).

**Определение**. Порядок $\le$ на множестве $A$ называется:

– *линейным*, если для любых $a,b\in A$ выполняется $a\le b$ или $b\le a$;

– *полным*, если каждое непустое подмножество множества $A$ имеет наименьший элемент.

Множество, на котором задан линейный порядок, называется *линейно упорядоченным множеством* или *цепью.* Множество, на котором задан полный порядок, называется *вполне упорядоченным множеством.*

## 1.5. Мощность множества

Мощность является количественной характеристикой множества, которая обобщает на произвольные множества понятие числа элементов конечного множества.

Любое конечное множество $A=\{a_1,...,a_n\}$ количественно характеризуется числом его элементов, которые последовательно нумеруются натуральными числами $1, 2, \dots, n$. Такая нумерация устанавливает взаимно однозначное соответствие между элементами множества $A$ и начальным отрезком натурального ряда $[1; n] = \{1,2, \dots, n\}$. При этом конечные множества $A,B$ в том и только том случае имеют одинаковую количественную характеристику $n$, если элементы этих множеств нумеруются элементами одного и того же отрезка $[1; n]$, что очевидно равносильно существованию взаимно однозначного отображения множества $A$ на множество $B$.

Такой подход к количественной характеристике конечных множеств естественно обобщается на произвольные множества $A,B$, которые имеют одинаковую количественную характеристику в том и только том случае, если существует взаимно однозначное отображение $A$ на $B$.

**Определение**. Множества $A,B$ называют *количественно эквивалентными* или *равномощными* и записывают $A \sim B$, если существует взаимно однозначное отображение множества $A$ на множество $B$.

**Примеры.**

1. Любое конечное $n$-элементное множество $A$ равномощно начальному отрезку натурального ряда $[1; n] = \{1,2, \dots, n\}$..
2. Множество натуральных чисел $\boldsymbol{N}$ равномощно как множеству четных чисел $\boldsymbol{N_2}$, так и множеству нечетных чисел $\boldsymbol{N_1}$.
3. Интервал $\left(-\frac{\pi}{2};\frac{\pi}{2}\right)$ равномощен множеству вещественных чисел $\boldsymbol{R}$, так как функция $y=\operatorname{tg} x$ взаимно однозначно отображает данный интервал на множество $\boldsymbol{R}$.

4. Любые интервалы $(a;b),(c;d)$ числовой прямой $\boldsymbol{R}$ равномощны между собой, так как линейная функция $y=\frac{d-c}{b-a}(x-a)+c$ взаимно однозначно отображает $(a;b)$ на $(c;d)$.

***Свойства равномощных множеств:***

1. Для любого множества $A$ выполняется условие $A\sim A$.
2. Для любых множеств $A,B$ условие $A\sim B$ влечет $B\sim A$.
3. Для любых множеств $A,B,C$ условия $A\sim B, B\sim C$ влекут $A\sim C$.

Например, из предыдущих примеров 3,4 и свойства 3) следует, что все интервалы числовой прямой $\boldsymbol{R}$ равномощны множеству $\boldsymbol{R}$.

Как уже отмечалось выше, конечное множество $A$ количественно характеризуется тем, что его элементы можно перечислить, располагая их в конечную последовательность $a_1,...,a_n$. Поэтому самое простое бесконечное множество $A$ будет количественно характеризоваться тем, что его элементы можно последовательно перечислить, располагая их в бесконечную последовательность $a_1,...,a_n,...$ . Такие множества количественно эквивалентны множеству натуральных чисел $\boldsymbol{N}$ и называются счетными.

**Определение**. Бесконечное множество $A$ называется *счетным,* если оно равномощно множеству натуральных чисел $\boldsymbol{N}$**,** и *несчетным* в противном случае.

***Свойства счетных множеств:***

1. Множества, отличающиеся от счетных множеств на конечное число элементов, являются счетными.
2. Объединение конечного или счетного семейства счетных множеств является счетным множеством.
3. Декартово произведение конечного семейства счетных множеств является счетным множеством.
4. Любое бесконечное множество содержит счетное подмножество.
5. Всякое подмножество счетного множества конечно или счетно.

Из этих свойств и построения множества рациональных чисел $\boldsymbol{Q}$ следует, что это множество счетное.

Важный пример несчетного множества дает следующий результат.

**Теорема Кантора.** Отрезок $[0;1]$ числовой прямой $\boldsymbol{R}$ является несчетным множеством.

Из этой теоремы, свойств счетных множеств и предыдущих примеров следует, что все промежутки числовой прямой $\boldsymbol{R}$ равномощны множеству $\boldsymbol{R}$.

Таким образом, любое конечное множество взаимно однозначно отображается на некоторое подмножество множества натуральных чисел $\boldsymbol{N}$, и любое бесконечное множество содержит счетное подмножество. Это означает, что, с одной стороны, количественная характеристика счетных множеств превосходит любое конечное число и, с другой стороны, среди бесконечных множеств счетные множества имеют самую маленькую количественную характеристику. Более точно количественное сравнение множеств определяется с помощью понятия мощности, которое обобщает понятие числа элементов конечных множеств.

**Определение.** *Мощностью* множества $A$ называется математический объект $|A|$, который соответствует всем равномощным $A$ множествам $B$, так что выполняется следующее фундаментальное свойство: $|A|=|B|$ в том и только том случае, если $A \sim B$.

Согласно определению мощностью конечного $n$-элементного множества $A$ можно считать число элементов этого множества, т.е. $|A|=n$. Для бесконечных множеств строгое определение мощности дается значительно сложнее и мы не будем здесь на нем останавливаться.

Сравнение мощностей определяется следующим образом.

**Определение.** Говорят, что мощность множества $A$ не превосходит мощности множества $B$ и записывают $|A| \le |B|$, если множество $A$ равномощно некоторому подмножеству множества $B$. Если при этом множества $A,B$ не являются равномощными, то говорят, что мощность множества $A$ меньше мощности множества $B$ и записывают $|A| < |B|$.

> **Например**, для любого натурального числа $n$ и любого бесконечного множества $A$ выполняется $n < |\boldsymbol{N}| \le |A|$ и, с другой стороны, $|\boldsymbol{N}| < |\boldsymbol{R}|$.

**Определение.** Мощность $|\boldsymbol{R}|$ называется *мощностью континуума*. Множества, равномощные множеству $\boldsymbol{R}$, называются *континуальными.*

Из приведенных выше результатов следует, что множество всех иррациональных чисел, а также все промежутки числовой прямой $\boldsymbol{R}$ являются континуальными множествами.

Нетрудно убедиться, что отношение сравнения мощностей рефлексивно и транзитивно, т.е. для любых множеств $A,B,C$ выполняется $|A| \le |A|$ и из условий $|A| \le |B|$, $|B| \le |C|$ следует $|A| \le |C|$. Антисимметричность этого отношения показывает следующий результат.

**Теорема Кантора – Бернштейна.** Для любых множеств $A,B$ из условий $|A| \le |B|$, $|B| \le |A|$ следует $|A| = |B|$.

Существование бесконечно возрастающей последовательности бесконечных мощностей вытекает из следующей теоремы.

**Теорема Кантора.** Для любого множества $A$ множество $\mathcal{P}(A)$ всех подмножеств множества $A$ удовлетворяет условию $|A| < |\mathcal{P}(A)|$.

### *Контрольные вопросы для среза знаний*

1) Основные действия над множествами и их свойства.
2) Виды бинарных отношений и отображений.
3) Основные действия над отношениями и их свойства.
4) Отношение эквивалентности и фактор-множество.
5) Отношение порядка и упорядоченные множества.
6) Равномощные множества и их свойства.
7) Счетные множества и их свойства.
8) Множества мощности континуума.
9) Понятие мощности и сравнение мощностей.

ГЛАВА 2

# АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

## 2.1. Определение алгебраической операции, алгебраической системы и алгебры

Пусть $A$ – непустое множество и $n$ – неотрицательное целое число.

**Определение.** Отображение $f : A^n \to A$ называется *алгебраической $n$-арной операцией* или просто *алгебраической операцией* на множестве $A$. При этом $n$ называется *порядком* или *арностью* алгебраической операции $f$.

В случае $n = 0$ по определению $A^0=\{\varnothing\}$ и, значит, 0-арная операция $f$ просто выделяет в множестве $A$ некоторый элемент $f(\varnothing)\in A$. В случае $n = 1$ операция $f$ называется также *унарной* и в случае $n = 2$ – *бинарной*. Для унарных и бинарных операций, как правило, используется специальная символическая запись.

> **Пример.** На множестве целых чисел $\boldsymbol{Z}$ 0-арная операция $f_0(\varnothing)=1$ выделяет элемент 1, унарная операция $f_1$ взятия противоположного по знаку числа обозначается знаком «минус» – и бинарная операция $f_2$ сложения целых чисел обозначается знаком «плюс» + , т.е. для любого числа $\boldsymbol{x}\in\boldsymbol{Z}$ записывается $f_1(x) = -x$ и для любых чисел $\boldsymbol{x, y}\in\boldsymbol{Z}$ записывается $\boldsymbol{f_2(x, y) = x + y}$.

Далее для бинарной операции $f$ по возможности будем использовать *мультипликативную запись* с помощью символа $\cdot$ , т.е. вместо $f(x,y)$ писать $x\cdot y$, или просто $xy$. При необходимости для бинарной операции $f$ используется также *аддитивная запись* с помощью символа + , т.е. вместо $f(x,y)$ записывается $x+y$.

В случае конечного $m$-элементного множества $A =\{a_1,a_2,\ldots,a_m\}$ $n$-арная операция $f = f(x_1,\ldots,x_n)$ на $A$ задается прямоугольной таблицей размерности $m^n \times (n+1)$, в первых $n$ столбцах которой размещаются всевозможные упорядоченные наборы значений переменных

$x_1,...,x_n$ в множестве $A$ и в последнем $(n+1)$-ом столбце – соответствующие значения функции $f(x_1,...,x_n)$ в множестве $A$. Общее число таких функций определяется числом различных последних $m^n$-мерных столбцов таблицы и равно $m^{m^n}$.

**Определение.** Бинарная операция $\cdot$ на множестве $A$ называется:

– *ассоциативной*, если $x\cdot(y\cdot z) = (x\cdot y)\cdot z$ для любых $x,y,z \in A$ ;

– *коммутативной*, если $x\cdot y = y\cdot x$ для любых $x,y \in A$ .

**Определение.** *Алгебраической системой* называется непустое множество $A$ с фиксированным набором $\boldsymbol{n_i}$-арных отношений $\boldsymbol{P_i}$ $(\boldsymbol{i = \overline{1,k}})$ и $\boldsymbol{n_j}$-арных операций $\boldsymbol{f_j}$ $(\boldsymbol{j = \overline{1,r}})$. При этом множество $A$ называется *базисным множеством* алгебраической системы и набор $\Omega = \{\boldsymbol{P_1}, \dots, \boldsymbol{P_k}; \boldsymbol{f_1}, \dots, \boldsymbol{f_r}\}$ символов отношений и операций соответствующей арности называется *алгебраическим типом* (или *сигнатурой*) алгебраической системы.

Такая алгебраическая система сокращенно обозначается $(\boldsymbol{A}; \boldsymbol{P_1}, \dots, \boldsymbol{P_k}; \boldsymbol{f_1}, \dots, \boldsymbol{f_r})$, или $(A;\Omega)$, или просто буквой $A$ и называется *алгебраической системой типа* $\Omega$, или сокращенно – *алгебраической* $\Omega$-*системой*.

Если сигнатура $\Omega$ не содержит символов отношений, то алгебраическая система $(\boldsymbol{A}; \boldsymbol{f_1}, \dots, \boldsymbol{f_r})$ является множеством $A$ с фиксированным набором $\boldsymbol{n_j}$-арных операций $\boldsymbol{f_j}$ $(\boldsymbol{j = \overline{1,r}})$ и называется *алгеброй типа* $\Omega$, или сокращенно – $\Omega$-*алгеброй*.

**Примеры.**

1. Непустое множество $A$ с фиксированным $n$-арным отношением $\rho \subset A^n$ является алгебраической системой типа $\Omega = \{\rho\}$, который состоит из единственного символа $n$-арного отношения $\rho$. Такие алгебраические $\Omega$-системы называются *релятивами* (или в случае $n = 2$ – *ориентированными графами*).

2. Непустое множество $A$ с набором $n_i$-арных отношений $\rho_i \subset A^{n_i}$ $(i = \overline{1,k})$ является алгебраической системой типа $\Omega = \{\rho_1, \dots, \rho_k\}$, который состоит из $k$ символов $n_i$-арных отношений $\rho_1, \dots, \rho_k$. Такие алгебраические $\Omega$-системы называются *полирелятивами* или *реляционными базами данных*.

3. Множество целых чисел $\boldsymbol{Z}$ с операцией сложения + является алгеброй $\boldsymbol{Z^+} = (\boldsymbol{Z}; +)$ типа $\Omega=\{+\}$**,** где + – символ бинарной операции сложения**.**

4. Множество целых чисел $\boldsymbol{Z}$ с операциями сложения + и умножения · является алгеброй $\boldsymbol{Z} = (\boldsymbol{Z}; +, \cdot)$ типа Ω={+,·}**,** где + – символ бинарной операции сложения и · – символ бинарной операции умножения**.**

5. Множество вещественных чисел $\boldsymbol{R}$ с отношением порядка ≤ и операциями сложения + и умножения · является алгебраической системой $\boldsymbol{R} = (\boldsymbol{R}; \leq; +, \cdot)$ типа Ω={≤;+,·}**,** где ≤ – символ бинарного отношения сравнения вещественных чисел по величине, + – символ бинарной операции сложения и · – символ бинарной операции умножения вещественных чисел**.**

## 2.2. Действия над алгебрами

При рассмотрении Ω-алгебр естественно выделяются их подмножества, эквивалентности и отображения, которые согласованы с операциями таких алгебр и которые называются соответственно подалгебрами, конгруэнтностями и гомоморфизмами алгебр.

**Определение.** Подмножество $X$ Ω-алгебры $A$ называется *подалгеброй*, если оно устойчиво относительно действия всех операций данной алгебры, т.е. для любой $n$-арной операции $f$ алгебры $A$ и любых элементов $x_1,...,x_n \in X$ значение $f(x_1,...,x_n) \in X$. В этом случае множество $X$ с ограничениями на нем операций исходной алгебры $A$ образует Ω-алгебру.

**Примеры.**

1. Множество натуральных чисел $\boldsymbol{N}$ является подалгеброй алгебры $\boldsymbol{Z}^+ = (\boldsymbol{Z}; +)$ с операцией сложения +.

2. Множество целых чисел $\boldsymbol{Z}$ является подалгеброй алгебры рациональных чисел $\boldsymbol{Q} = (\boldsymbol{Q}; +, \cdot)$ с операциями сложения + и умножения · .

***Теорема 1.*** Для любого непустого подмножества $X$ Ω-алгебры $A$ найдется наименьшая подалгебра алгебры $A$, которая содержит множество $X$. Такая подалгебра обозначается символом $\langle X \rangle$ и называется подалгеброй алгебры $A$, *порожденной подмножеством* $X \subset A$. В случае $\langle X \rangle = A$ подмножество $X$ называется *порождающим множеством алгебры* $A$.

**Пример.** Подмножество $X$={1} алгебры $\boldsymbol{Z}^+ = (\boldsymbol{Z}; +)$ порождает подалгебру $\boldsymbol{N}$ и, значит, одноэлементное множество $X$={1} является порождающим множеством алгебры $\boldsymbol{N} = (\boldsymbol{N}; +)$.

**Определение**. *Конгруэнцией* Ω-алгебры $A$ называется отношение эквивалентности $\varepsilon$ на множестве $A$, которое для любой $n$-арной операции $f$ алгебры $A$ и любых элементов $x_1,...,x_n, y_1,...,y_n \in A$ удовлетворяет условию:

$$(x_1, y_1),...,(x_n, y_n) \in \varepsilon \Rightarrow (f(x_1,...,x_n), f(y_1,...,y_n) \in \varepsilon.$$

Если вместо условия $(x, y) \in \varepsilon$ используется запись $x \equiv y(\varepsilon)$ или просто $x \equiv y$, то последнее определение конгруэнтности записывается в виде:

$$x_1 \equiv y_1, \ldots, x_n \equiv y_n \Rightarrow f(x_1,...,x_n) \equiv f(y_1,...,y_n).$$

Как уже отмечалось в разделе 1.3, класс отношения эквивалентности $\varepsilon$, определяемый элементом $x$, обозначается символом $[x] = \{y \in A : x \equiv y\}$. Множество всех классов эквивалентности $\varepsilon$ образует фактор-множество $A/\varepsilon = \{[x] : x \in A\}$, на котором следующим образом естественно определяются операции алгебраического типа Ω: для любого символа $n$-арной операции $f \in \Omega$ и любых элементов $[x_1],...,[x_n] \in A/\varepsilon$ значение $f([x_1],...,[x_n]) = [f(x_1,...,x_n)]$. В результате $A/\varepsilon$ является Ω-алгеброй, которая называется *фактор-алгеброй* Ω-алгебры $A$ по конгруэнции $\varepsilon$.

**Пример.** Пусть $A = \boldsymbol{Z}^+$ – алгебра целых чисел с операцией сложения и $m$ – фиксированное натуральное число. Рассмотрим на множестве $\boldsymbol{Z}$ бинарное отношение $\varepsilon$, которое определяется по формуле:

$$(x, y) \in \varepsilon \Leftrightarrow x - y = k \cdot m \text{ для некоторого } k \in \boldsymbol{Z}.$$

Тогда отношение $\varepsilon$ является эквивалентностью на множестве $\boldsymbol{Z}$, так как для любых $x, y \in \boldsymbol{Z}$ выполняются свойства:

1) $(x, x) \in \varepsilon$ в силу $x - x = 0 \cdot m = 0$ – рефлексивность отношения $\varepsilon$;

2) $(x, y) \in \varepsilon \Rightarrow (y, x) \in \varepsilon$ в силу $x - y = k \cdot m \Rightarrow y - x = (-k) \cdot m$ – симметричность отношения $\varepsilon$;

3) $(x, y), (y, z) \in \varepsilon \Rightarrow (x, z) \in \varepsilon$ в силу $x - y = k \cdot m,\ y - z = l \cdot m \Rightarrow$
$\Rightarrow x - z = (x - y) + (y - z) = k \cdot m + l \cdot m = (k + l) \cdot m$ – транзитивность отношения $\varepsilon$.

Такое отношение эквивалентности $\varepsilon$ обозначается символом $\bmod m$ и называется *отношением сравнимости целых чисел по модулю m*. Если $(x, y) \in \varepsilon$, то записывают $x \equiv y (\bmod m)$, или просто $x \equiv y$ и числа $x, y$ называют *сравнимыми по модулю m*.

Отношение $\varepsilon = \mathrm{mod}\, m$ является конгруэнцией алгебры целых чисел $\boldsymbol{Z}^+$, так как для любых $x_1, y_1, x_2, y_2 \in \boldsymbol{Z}$ выполняется свойство:

$$x_1 \equiv y_1,\ x_2 \equiv y_2 \Rightarrow x_1 + x_2 \equiv y_1 + y_2$$

в силу того, что условие $x_1 - y_1 = k_1 \cdot m,\ x_2 - y_2 = k_2 \cdot m$ влечет равенства $(x_1 + x_2) - (y_1 + y_2) = k_1 \cdot m + k_2 \cdot m = (k_1 + k_2) \cdot m$.

Класс отношения эквивалентности $\varepsilon$, содержащий элемент $a \in \boldsymbol{Z}$, определяется по формуле:

$$[a] = \{x \in Z : a \equiv x\} = \{x \in Z : a - x = k \cdot m \text{ для некоторого } k \in \boldsymbol{Z}\} =$$
$$= \{x \in Z : x = a + k \cdot m \text{ для некоторого } k \in \boldsymbol{Z}\} = a + mZ$$

и называется *классом вычетов элемента a по модулю m.*

Очевидно, что отношение $\varepsilon$ имеет всего $m$ классов эквивалентности:

$$[0] = \{0, 0 \pm m, 0 \pm 2m, \ldots\} = 0 + mZ = mZ,$$
$$[1] = \{1, 1 \pm m, 1 \pm 2m, \ldots\} = 1 + mZ,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[m-1] = \{m-1, (m-1) \pm m, (m-1) \pm 2m, \ldots\} = (m-1) + mZ,$$

так как класс эквивалентности

$$[m] = \{m, m \pm m, m \pm 2m, \ldots\} = m + mZ = mZ = [0].$$

Значит, фактор-множество $Z/\varepsilon$ состоит из $m$ классов эквивалентности $[0],[1],\ldots,[m-1]$, которые с помощью взаимно однозначного отображения $[n] \mapsto n$ $(n \in \{0,1,\ldots,m-1\})$ могут быть отождествлены с их представителями $0,1,\ldots,m-1$. Таким образом, фактор-множество $Z/\varepsilon$ может быть отождествлено с множеством $Z_m = \{0,1,\ldots,m-1\}$, которое называется *полной системой вычетов по модулю m.*

Операция сложения на фактор-множестве $Z/\varepsilon$ для элементов $n_1, n_2 \in \{0,1,\ldots,m-1\}$ определяется по формуле:

$$[n_1] + [n_2] = [n_1 + n_2] = (n_1 + n_2) + Zm.$$

Следовательно, при отождествлении классов вычетов $[n]$ с их представителями $n \in \{0,1,\ldots,m-1\}$ операция сложения + классов вычетов $[n_1],[n_2]$ (для значений $n_1, n_2 \in \{0,1,\ldots,m-1\}$) отождествляется с операцией сложения по модулю $m$ представителей этих классов $n_1, n_2$, т.е. вычисляется обычная сумма $n_1 + n_2$ элементов $n_1, n_2$ и затем берется остаток от деления этой суммы на число $m$.

Обозначается такая фактор-алгебра символом $Z_m^+ = (\{0,1,\ldots,m\},+)$ и называется *аддитивной группой классов вычетов по модулю m.*

В частности для $m = 3$ фактор-алгебра $Z_3^+$ является трехэлементным множеством $Z_3 = \{0,1,2\}$ с операцией сложения по модулю 3, которая определяется следующей таблицей:

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Аналогично можно показать, что отношение $\varepsilon = \bmod m$ является конгруэнтностью алгебры $\boldsymbol{Z}^{\times}$ целых чисел с операцией умножения и что фактор-алгебра $Z/\varepsilon$ является алгеброй $Z_m^{\times} = (\{0,1,\ldots,m-1\},\cdot)$ с операцией умножения чисел $n_1, n_2 \in \{0,1,\ldots,m-1\}$ по модулю $m$, т.е. в этом случае вычисляется обычное произведение $n_1 \cdot n_2$ элементов $n_1, n_2$ и затем берется остаток от деления этого произведения на число $m$. Такая алгебра $Z_m^{\times}$ называется *мультипликативная полугруппа классов вычетов по модулю m.*

В частности для $m = 3$ алгебра $Z_3^{\times}$ является трехэлементным множеством $Z_3 = \{0,1,2\}$ с операцией умножения по модулю 3, которая определяется следующей таблицей:

| · | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

**Определение.** Отображение $\varphi: A \to B$ Ω-алгебры $A$ в Ω-алгебру $B$ называется *гомоморфизмом,* если для любого символа $n$-арной операции $f \in \Omega$ и любых элементов $x_1,\ldots,x_n \in A$ выполняется равенство:

$$\varphi(f_A(x_1,\ldots,x_n)) = f_B(\varphi(x_1),\ldots,\varphi(x_n)),$$

где $f_A$ и $f_B$ – соответствующие символу $f \in \Omega$ $n$-арные операции Ω-алгебр $A$ и $B$.

Гомоморфизм $\varphi$ алгебры $A$ в алгебру $B$ называется:

– *мономорфизмом A* в *B*, если $\varphi$ – взаимно-однозначный гомоморфизм $A$ в $B$;

– *эпиморфизмом A* на *B (*или *гоморфизмом A на B,),* если $\varphi$ – такой гомоморфизм *A* в *B*, что $\varphi(A) = B$;

– *изоморфизмом A* на *B*, если $\varphi$ – взаимно-однозначный гомоморфизм *A* на *B;* при этом записывают $A \overset{\varphi}{\cong} B$, или просто $A \cong B$, и говорят, что алгебры *A,B изоморфны.*

Так как изоморфные алгебры различаются только обозначением элементов, то с алгебраической точки зрения такие алгебры не различаются.

**Примеры.**

1. Пусть $A = \boldsymbol{N}^+$ – алгебра натуральных чисел с операцией сложения и $B = \boldsymbol{Z}^+$ – алгебра целых чисел с операцией сложения. Для каждого $n \in \boldsymbol{N}$ положим $\varphi(n) = n \in \boldsymbol{Z}$. В результате получаем взаимно-однозначное отображение $\varphi: \boldsymbol{N} \to \boldsymbol{Z}$, которое удовлетворяет условию: $\varphi(n+m) = n+m = \varphi(n) + \varphi(m)$. Это означает, что $\varphi$ – мономорфизм алгебры *A* в алгебру *B.*

2. Пусть $A = \boldsymbol{Z}^{\times}$ – алгебра целых чисел с операцией умножения и $B = (\{-1,0,1\},\cdot)$ – трехэлементная алгебра с обычным умножением. Для каждого целого числа $x \in \boldsymbol{Z}$ положим

$$\varphi(x) = \operatorname{sgn}(x) = \begin{cases} 1, & \textit{если} \quad x > 0, \\ 0, & \textit{если} \quad x = 0, \\ -1, & \textit{если} \quad x < 0. \end{cases}$$

Очевидно, что для любых $x, y \in \boldsymbol{Z}$ выполняется равенство: $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ и, кроме того, $\varphi(A) = \{-1,0,1\}$. Это означает, что $\varphi$ – эпиморфизм алгебры *A* на алгебру *B.*

3. Пусть $A = \boldsymbol{R}_+$ – алгебра положительных вещественных чисел с операцией умножения и $B = \boldsymbol{R}$ – алгебра всех вещественных чисел с операцией сложения. Тогда для каждого числа $x \in \boldsymbol{R}_+$ в множестве вещественных чисел $\boldsymbol{R}$ определено значение $\varphi(x) = \lg x$**.** По известному свойству логарифма $\varphi$ – взаимно-однозначное отображение множества $\boldsymbol{R}_+$ на множество $\boldsymbol{R}$**,** для которого при любых $x, y \in$ $x, y \in \boldsymbol{R}_+$ выполняется равенство: $\varphi(x \cdot y) = \lg(x \cdot y) = \lg x + \lg y = \varphi(x) + \varphi(y)$. Это означает, что $\varphi$ – изоморфизм алгебры *A* на алгебру *B.*

***Теорема 2.*** Для любого гомоморфизма $\varphi: A \to B$ Ω-алгебры *A* в Ω-алгебру *B* ядро $\ker\varphi$ является конгруэнцией Ω-алгебры *A.* При этом

фактор-алгебра $A/\ker\varphi \cong \langle E_\varphi \rangle$, где $\langle E_\varphi \rangle$ – подалгебра Ω-алгебры *B*, порожденная множеством $E_\varphi$ значений отображения $\varphi$.

С другой стороны, из того, что ядро $\ker\varphi$ отображения $\varphi: A \to B$ Ω-алгебры *A* в Ω-алгебру *B* является конгруэнцией Ω-алгебры *A* в общем случае не следует, что $\varphi$ – гомоморфизм *A* в *B*. Например, если Ω-алгебры *A* и *B* имеют одинаковые базисные множества, но разные алгебраические структуры, то тождественное отображение $\Delta_A: A \to B$ не будет гомоморфизмом *A* в *B*, но ядро такого отображения $\ker\Delta_A = \Delta_A$ – конгруэнция Ω-алгебры *A*.

***Теорема 3***. Пусть $\varepsilon$ – конгруэнция Ω-алгебры *A* и $\text{nat}\,\varepsilon: A \to A/\varepsilon$ – каноническое отображение эквивалентности $\varepsilon$, которое каждому элементу $x \in A$ ставит в соответствие класс эквивалентности $[x]$. Тогда отображение $\text{nat}\,\varepsilon$ является гомоморфизмом Ω-алгебры *A* на фактор-алгебру $A/\varepsilon$. При этом отображение $\text{nat}\,\varepsilon$ называется *каноническим гомоморфизмом* конгруэнции $\varepsilon$.

Таким образом, каждому гомоморфизму $\varphi$ Ω-алгебры *A* соответствует конгруэнция $\varepsilon = \ker\varphi$ этой Ω-алгебры, для которой найдется такой изоморфизм $\psi: A/\ker \to E_\varphi$, что $\varphi = \psi \circ \text{nat}\,\varepsilon$. Это означает, что гомоморфизм $\varphi$ отличается от канонического гомоморфизма $\text{nat}\,\varepsilon$ только обозначением элементов алгебры $E_\varphi$. С другой стороны, каждой конгруэнции $\varepsilon$ Ω-алгебры *A* соответствует канонический гомоморфизм $\text{nat}\,\varepsilon: A \to A/\varepsilon$, ядро которого $\ker \text{nat}\,\varepsilon = \varepsilon$.

Как показано выше, подалгебры, гомоморфизмы и фактор-алгебры дают универсальную технику конструирования новых Ω-алгебр из уже известных Ω-алгебр. Еще один универсальный метод конструирования новых Ω-алгебр дает следующий результат.

***Теорема 4***. Пусть *I* – непустое множество и для каждого элемента $i \in I$ определена Ω-алгебра $A_i$, т.е. задано семейство Ω-алгебр $\{A_i\}_{i \in I}$. Тогда на множестве отображений

$$A = \{\varphi: I \to \bigcup_{i \in I} A_i: \ \varphi(i) \in A_i \text{ для всех } i \in I\}$$

для каждого символа *n*-арной операции $f \in \Omega$ покомпонентно определяется *n*-арная операция $f_A$ по правилу: для любых элементов $\varphi_1,\ldots,\varphi_n \in A$ значение $f_A(\varphi_1,\ldots,\varphi_n)$ есть отображение $\varphi: I \to \bigcup_{i \in I} A_i$, которое при всех $i \in I$ удовлетворяет условию: $\varphi(i) = f_{A_i}(\varphi_1(i),\ldots,\varphi_n(i))$.

Такая Ω-алгебра $A$ называется *декартовым* (или *прямым*) *произведением семейства* Ω-алгебр $\{A_i\}_{i\in I}$ и обозначается $\prod_{i\in I} A_i$.

В частности, если все Ω-алгебры $A_i$ равны одной и той же Ω-алгебре $A$, то декартово произведение $\prod_{i\in I} A_i$ называется $I$-ой *декартовой степенью* Ω-алгебры $A$ и обозначается символом $A^I$. Если $I$ – конечное $n$-элементное множество, то $A^I$ называется также $n$-ой *декартовой степенью* Ω-алгебры $A$ и обозначается символом $A^n$.

**Пример.** Пусть для каждого значения $i = 1,..,n$ Ω-алгебра $A_i$ равна алгебре вещественных чисел $\boldsymbol{R} = (\boldsymbol{R}; +)$ с операцией сложения +. Тогда $n$-я декартова степень $A^n$ есть алгебра $\boldsymbol{R^n} = (\boldsymbol{R^n}; +)$ $n$-мерных векторов $(x_1, \dots, x_n) \in \boldsymbol{R^n}$ с операцией их покомпонентного сложения: $(x_1,...,x_n)+(y_1,...,y_n) = (x_1+y_1,\dots,x_n+y_n)$.

## 2.3. Классификация алгебр

**Определение.** Алгебра $S = (S, \cdot)$ с одной ассоциативной бинарной операцией называется *полугруппой*. Полугруппа $S$ называется *коммутативной*, если умножение в этой полугруппе коммутативно.

**Примеры.**

1. Алгебра целых чисел $\boldsymbol{Z}^+ = (\boldsymbol{Z}\ ,\ +\ )$ с операцией сложения + является коммутативной полугруппой, так как $x + (y + z) = (x + y) + z, x + y = y + x$ для любых $x,y,z \in \boldsymbol{Z}$.

2. Множество всех преобразований непустого множества $X$ с операцией композиции является полугруппой. Такая полугруппа называется *симметрической полугруппой преобразований* множества $X$ и обозначается символом $\mathfrak{T}(X)$. Подполугруппы этой полугруппы называются *полугруппами преобразований* множества $X$.

3. Пусть $A$ – произвольное множество, называемое *алфавитом*. Элементы $a \in A$ называются *буквами*. *Словом* над алфавитом $A$ называется конечная последовательность букв $a_1 \dots a_n$ алфавита $A$. Слово без букв называется *пустым словом* и обозначается символом $\Lambda$. Для слова $w = a_1 \dots a_n$ число $n$ букв в определяющей его последовательности называется *длиной* этого слова и обозначается символом $l(w)$.

Обозначим символом $A^+$ множество всех непустых слов над алфавитом $A$ и символом $A^*$ – множество слов $A^* = A^+ \cup \{\Lambda\}$. На

этих множествах слов определена операция умножения, которая называется операцией *конкатенации* слов и определяется по правилу: любым словам $w_1 = a_1 \ldots a_n$ и $w_2 = b_1 \ldots b_m$ операция конкатенации ставит в соответствие слово $w_1 \cdot w_2 = a_1 \ldots a_n b_1 \ldots b_n$. В результате множество слов $A^+$ с операцией конкатенации образует полугруппу, которая называется *полугруппой слов над алфавитом A.*

В случае конечного *n*-элементного множества $S = \{s_1, s_2, \ldots, s_n\}$ операция умножения на $S$ задается *таблицей Кэли* размерности $n \times n$, строки и столбцы которой помечены элементами множества $S$ и в которой на пересечении $i$-ой строки и $j$-го столбца стоит произведение $s_i \cdot s_j$ элементов $s_i, s_j$.

| · | $s_1$ | $s_2$ | … | $s_n$ |
|---|---|---|---|---|
| $s_1$ | $s_1 \cdot s_1$ | $s_1 \cdot s_2$ | … | $s_1 \cdot s_n$ |
| $s_2$ | $s_2 \cdot s_1$ | $s_2 \cdot s_2$ | … | $s_2 \cdot s_n$ |
| … | … | … | … | … |
| $s_n$ | $s_n \cdot s_1$ | $s_n \cdot s_2$ | … | $s_n \cdot s_n$ |

Ассоциативность такой операции определяется по *тесту Лайта*: для доказательства тождества ассоциативности последовательно фиксируем элементы $a \in S$ и проверяем выполнимость равенства $(x \cdot a) \cdot z = x \cdot (a \cdot z)$ для любых $x, z \in S$ путем сравнения следующих двух таблиц, составленных для произведений соответственно левой и правой частей этого равенства.

Таблица произведений $(x \cdot a) \cdot z$ левой части равенства:

| $x \cdot a$ \ $z$ | $s_1$ | $s_2$ | … | $s_n$ |
|---|---|---|---|---|
| $s_1 \cdot a$ | $(s_1 \cdot a) \cdot s_1$ | $(s_1 \cdot a) \cdot s_2$ | … | $(s_1 \cdot a) \cdot s_n$ |
| $s_2 \cdot a$ | $(s_2 \cdot a) \cdot s_1$ | $(s_2 \cdot a) \cdot s_2$ | … | $(s_2 \cdot a) \cdot s_n$ |
| … | … | … | … | … |
| $s_n \cdot a$ | $(s_n \cdot a) \cdot s_1$ | $(s_n \cdot a) \cdot s_2$ | … | $(s_n \cdot a) \cdot s_n$ |

строка исходной таблицы с меткой $s_1 \cdot a$

строка исходной таблицы с меткой $s_2 \cdot a$

строка исходной таблицы с меткой $s_n \cdot a$

столбец исходной таблицы с меткой $a$

Таблица произведений $x\cdot(a\cdot z)$ правой части равенства:

| $x$ \ $a\cdot z$ | $a\cdot s_1$ | $a\cdot s_2$ | … | $a\cdot s_n$ |
|---|---|---|---|---|
| $s_1$ | $s_1\cdot(a\cdot s_1)$ | $s_1\cdot(a\cdot s_2)$ | … | $s_1\,(a\cdot s_n)$ |
| $s_2$ | $s_2\cdot(a\cdot s_1)$ | $s_2\cdot(a\cdot s_2)$ | … | $s_2\cdot(a\cdot s_n)$ |
| … | … | … | … | … |
| $s_n$ | $s_n\cdot(a\cdot s_1)$ | $s_n\cdot(a\cdot s_2)$ | … | $s_n\cdot(a\cdot s_n)$ |

← строка исходной таблицы с меткой $a$

↑ столбец исходной таблицы с меткой $a\cdot s_1$,
↑ столбец исходной таблицы с меткой $a\cdot s_2$,
↑ столбец исходной таблицы с меткой $a\cdot s_n$.

**Пример**. Как известно из примера в разделе 2.2, на конечном множестве $\mathbf{Z}_3^{\times}=\{0,1,2\}$ определена операция умножения по модулю 3 со следующей таблицей Кэли размерности 3 ×3:

| · | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Для доказательства ассоциативности этой операции по тесту Лайта последовательно фиксируем элементы $a$ = 0,1,2 и проверяем выполнимость равенства $(x\cdot a)\cdot z = x\cdot(a\cdot z)$ для любых $x,z\in\mathbf{Z}_3^{\times}$ путем сравнения соответствующих двух таблиц. В частности, для $a$ = 2 таблица произведений $(x\cdot 2)\cdot z$ левой части равенства имеет вид:

| $x\cdot 2$ \ $z$ | 0 | 1 | 2 |
|---|---|---|---|
| $0\cdot 2=0$ | 0 | 0 | 0 |
| $1\cdot 2=2$ | 0 | 2 | 1 |
| $2\cdot 2=1$ | 0 | 1 | 2 |

и таблица произведений $x\cdot(2\cdot z)$ правой части равенства имеет вид:

| $x$ \ $2\cdot z$ | $2\cdot 0=0$ | $2\cdot 1=2$ | $2\cdot 2=1$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 1 |
| 2 | 0 | 1 | 2 |

Так как эти две таблицы совпадают, то равенство $(x\cdot 2)\cdot z = x\cdot(2\cdot z)$ выполняется при любых $x,z \in \mathbf{Z}_3^{\times}$. Аналогично для элементов $a = 0,1$ доказывается, что при любых $x,z \in \mathbf{Z}_3^{\times}$ выполняется равенство $(x\cdot a)\cdot z = x\cdot(a\cdot z)$. Значит, данная операция ассоциативна и $\mathbf{Z}_3^{\times}$ является полугруппой.

**Определение**. Элемент $s$ полугруппы $S$ называется:

– *нулевым*, если $s\cdot x = x\cdot s = s$ для любого $x \in S$ (при мультипликативной записи операции полугруппы такой элемент обозначается символом 0 и называется *нулем*);

– *нейтральным* (*единичным*), если $s\cdot x = x\cdot s = x$ для любого $x \in S$ (при мультипликативной записи операции полугруппы такой элемент обозначается символом 1 и называется *единицей*);

– *обратимым*, если для некоторого $x \in S$ выполняется свойство: $x\cdot s = s\cdot x = 1$ (такой элемент $x$ называется *обратным* для элемента $s$ и обозначается символом $s^{-1}$);

– *идемпотентом*, если $s\cdot s = s$, т.е. $s^2 = s$.

**Примеры.**

1. В симметрической полугруппе $\mathfrak{T}(X)$ преобразований множества $X$ тождественное преобразование $\Delta_X$ является нейтральным элементом и элемент $\varphi \in \mathfrak{T}(X)$ обратим в том и только том случае, если $\varphi$ – перестановка множества $X$.

2. Множество $A^*$ всех слов над алфавитом $A$ с операцией конкатенации образует полугруппу с единичным элементом $\Lambda$, которая называется *моноидом слов над алфавитом A*.

***Лемма (необходимое условие ассоциативности)***. Любая конечная полугруппа имеет идемпотент.

***Теорема Кэли о представлении полугрупп преобразованиями.*** Каждая полугруппа изоморфна полугруппе преобразований некоторого множества.

***Теорема о представлении полугрупп словами.*** Любая полугруппа $S$ является фактор-полугруппой некоторой полугруппы слов $A^+$, т.е. $S \cong A^+/\varepsilon$ для некоторой конгруэнции $\varepsilon$ полугруппы $A^+$.

**Определение**. *Группой* называется полугруппа $G = (G, \cdot)$ с нейтральным элементом $e$, в которой каждый элемент обратим, т.е. для любого элемента $a \in G$ существует обратный элемент $a^{-1} \in G$, удовлетворяющий условию: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Другими словами группа – это алгебра $G = (G, \cdot, ^{-1}, e)$ с ассоциативной бинарной операцией умножения $\cdot$, унарной операцией обращения $^{-1}$ и 0-арной операцией фиксирования нейтрального элемента $e$, которая удовлетворяем следующим аксиомам группы:

1) $(xy)z = x(yz)$ – ассоциативность умножения;
2) $xe = ex = x$ – нейтральность элемента $e$;
3) $xx^{-1} = x^{-1}x = e$ – обратимость умножения;
4) $(x^{-1})^{-1} = x$ – идемпотентность обращения;
5) $(xy)^{-1} = y^{-1}x^{-1}$ – инвертирование умножения обращением.

При мультипликативной записи бинарной операции группы нейтральный элемент $e$ обозначается символом 1 и называется единицей группы, а значение $x^{-1}$ называется обратным для $x$ элементом группы.

При аддитивной записи бинарной операции группы нейтральный элемент $e$ обозначается символом 0 и называется нулем группы, а значение $x^{-1}$ называется противоположным для $x$ элементом группы и обозначается символом $-x$.

**Примеры.**

1. Алгебра целых чисел $\boldsymbol{Z} = (\boldsymbol{Z}, +, -, 0)$ является группой, так как очевидно выполняются свойства 1) – 5). Такая группа называется *аддитивной группой целых чисел* и обозначается символом $\boldsymbol{Z}^+$.

2. Алгебра ненулевых рациональных чисел $\boldsymbol{Q}^* = (\boldsymbol{Q}^*, \cdot, ^{-1}, 0)$ является группой, так как очевидно выполняются свойства 1) – 5). Такая группа называется *мультипликативной группой рациональных чисел*.

3. Для любого натурального числа $m \in \boldsymbol{N}$ определенная в разделе 2.2 фактор-алгебра $\boldsymbol{Z}_m^+ = (\{1,\ldots,m-1\}, +, 0)$ является группой с операцией сложения по модулю $m$, так как для любого $0 \le k \le m-1$ выполняется $k+(m-k) = 0$, т.е. элемент $m - k$ является обратным для $k$. Напомним, что такая группа называется *аддитивной группой классов вычетов по модулю* $m$.

4. Определенная в разделе 2.2 мультипликативная полугруппа $\boldsymbol{Z}_m^\times = (\{1,\ldots,m-1\}, \cdot, 1)$ ненулевых классов вычетов по модулю $m$ тогда и только тогда является группой, когда $m$ – простое число. Такая группа называется *мультипликативной группой классов вычетов по модулю* $m$.

**Определение**. *Кольцом* называется алгебра $K=(K,+,\cdot)$ с двумя бинарными операциями сложения + и умножения $\cdot$, которые удовлетворяют следующим условиям:

1) $(K,+)$ – коммутативная группа с нейтральным элементом 0, который называется *нулем* кольца;

2) $(K,\cdot)$ – коммутативная полугруппа с нейтральным элементом 1, который отличен от 0 и называется *единицей* кольца;

3) $(x+y)\cdot z=x\cdot z+y\cdot z$ – дистрибутивность умножения относительно сложения.

Ясно, что для любого элемента $x$ кольца $K$ существует обратный относительно операции сложения + элемент $-x$, удовлетворяющий свойству $x+(-x)=0$.

**Определение**. Элемент $x$ кольца $K$ называется *обратимым*, если для него в кольце $K$ существует *обратный* относительно операции умножения $\cdot$ *элемент* $x^{-1}$, удовлетворяющий свойству $x\cdot x^{-1}=1$.

Легко видеть, что множество всех обратимых элементов кольца $K$ с операцией умножения $\cdot$ образует группу, которая называется *мультипликативной группой кольца*.

**Определение.** *Полем* называется кольцо $K$, в котором каждый ненулевой элемент $x$ обратим относительно операции умножения $\cdot$, т.е. для некоторого элемента $x^{-1}\in K$ выполняется равенство $x\cdot x^{-1}=1$.

Другими словами, поле – это кольцо $K$ с мультипликативной группой $K^*=K\setminus\{0\}$, которая называется *мультипликативной группой поля*.

**Примеры.**

1. Алгебра целых чисел $\boldsymbol{Z}=(\boldsymbol{Z},+,\cdot)$ является кольцом, которое называется *кольцом целых чисел.* Однако это кольцо не является полем, так как его мультипликативная группа имеет вид $\{1,-1\}$.

2. Алгебра рациональных чисел $\boldsymbol{Q}=(\boldsymbol{Q},+,\cdot)$ является полем, которое называется *полем рациональных чисел.*

3. Для любого натурального числа $m$ алгебра $(\{0,1,\ldots,m-1\},+,\cdot)$ с операциями сложения и умножения по модулю $m$ является кольцом, которое называется *кольцом классов вычетов по модулю* $m$ и обозначается символом $\boldsymbol{Z}_m$.

4. Для любого простого натурального числа $p$ алгебра $(\{0,1,\ldots,p-1\},+,\cdot)$ с операциями сложения и умножения по модулю $p$ является полем, которое называется *полем классов вычетов по модулю* $p$ и обозначается символом $\boldsymbol{Z}_p$.

**Определение.** Кольцо $K$ называется *кольцом без делителей нуля*, если для любых его элементов $x, y \in K$ из условия $x \cdot y = 0$ следует, что $x = 0$ или $y = 0$.

***Теорема Веддербарна***. Любое конечное кольцо без делителей нуля является полем.

Рассмотрим произвольное кольцо $K$.

**Определение.** Пусть $a,b$ – элементы кольца $K$. Если для некоторого $c \in K$ выполняется равенство $b = ac$, то элемент $a$ называется *делителем* $b$, а элемент $b$ – *кратным* $a$. В этом случае пишут $a|b$ и говорят, что $a$ делит $b$, или равносильно, пишут $b \vdots a$ и говорят, что $b$ *делится* на $a$.

***Свойства отношения делимости элементов***:

1) $a|a$ – рефлективность отношения делимости |;

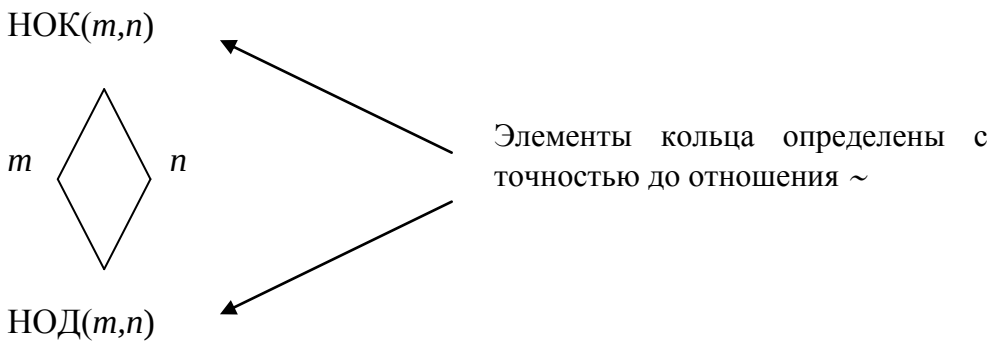
2) $a|b$ и $b|c \Rightarrow a|c$ – транзитивность отношения делимости | ;

3) $1|{-1}$ и $-1|1$, но $1 \neq -1$ – отношение делимости | не является антисимметричным.

**Определение.** Элементы $a,b$ кольца $K$ называют *ассоциированными* и пишут $a \sim b$, если $a|b$ и $b|a$.

Очевидно, что отношение $\sim$ является отношением эквивалентности на множестве $K$ и что при отождествлении ассоциированных элементов отношение делимости | упорядочивает кольцо $K$.

**Пример**. Пусть $K = \boldsymbol{Z}$ – кольцо целых чисел. Тогда для элементов $a, b \in \boldsymbol{Z}$ условие $a \sim b$ означает, что $a = \pm b$ или $a = b = 0$. Следовательно, для любых элементов $m, n \in \boldsymbol{Z}$ с точностью до знака определена точная нижняя грань относительно отношения делимости | , которая называется *наибольшим общим делителем* чисел $m,n$ и обозначается символом НОД($m,n$). Кроме того, для любых элементов $m, n \in \boldsymbol{Z}$ определена также точная верхняя грань относительно отношения делимости | , которая называется *наименьшим общим кратным* чисел $m,n$ и обозначается символом НОК($m,n$).




**Например**, НОД(6,8) = {2, –2} и НОД(–6,8) = {–2,2}.

**Определение**. Элемент *a* кольца *K* называется:

1) *обратимым*, если $a|1$,т.е. $ax = 1$ для некоторого $x \in K$;

2) *простым* (или *неприводимым*), если этот элемент отличен от нуля, не делит 1 и имеет только тривиальные делители – обратимые элементы кольца *K* и ассоциированные с *a* элементы.

> **Пример:** Пусть $K = \boldsymbol{Z}$ – кольцо целых чисел. Тогда элемент $m \in \boldsymbol{Z}$ в том и только том случае обратим, если $m = \pm 1$. Значит, число $m \in \boldsymbol{Z}$ в том и только том случае будет простым, если $m \neq 0, \pm 1$ и имеет только тривиальные делители – числа $\pm 1, \pm m$.

**Определение**. Подмножество $X$ кольца $K$ называется *идеалом*, если $X$ не пусто и удовлетворяет условию: $x, y \in X, z \in K \implies x - y, x \cdot z \in X$. При этом идеал $X$ называется *главным*, если $X = K \cdot a \cdot K$ для некоторого $a \in K$.

**Определение.** Кольцо *K* без делителей нуля называется:

1) *факториальным* (сокращенно ФК), если любой его ненулевой элемент $a \in K$ представим в виде $a = \varepsilon p_1 \dots p_n$, где $\varepsilon|1$ и $p_1, \dots, p_n$ – простые элементы кольца *K*;

2) *кольцом главных идеалов* (сокращенно КГИ), если любой его идеал является главным (т.е. порождается одним элементом),

3) *евклидовым кольцом* (сокращенно ЕК), если существует отображение $h$ множества $K^* = K \setminus \{0\}$ в множество $\boldsymbol{N}_0 = \boldsymbol{N} \cup \{0\}$, которое удовлетворяет условиям:

i) $h(ab) \geq h(a)$ для любых ненулевых элементов $a, b \in K$;

ii) для любых $a, b \in K, b \neq 0$ найдутся элементы $q, r \in K$, обладающие евклидовым свойством:

$$a = bq + r \text{ и либо } h(r) < h(b), \text{ либо } r = 0.$$

Известно, что определенные выше свойства взаимосвязаны следующим образом: ЕК $\Rightarrow$ КГИ $\Rightarrow$ ФК.

> **Пример.** Кольцо целых чисел $\boldsymbol{Z}$ является ФК,КГИ и ЕК, так как функция $h(m) = |m|$ удовлетворяет приведенным выше условиям i) и ii).

1) Алгебраическая операция и сигнатура.
2) Алгебры и алгебраическая система.
3) Подалгебры и порождающее множество алгебры.
4) Конгруэнции алгебры и фактор-алгебры.
5) Гомоморфизм алгебр и классификация гомоморфизмов.
6) Полугруппы и проверка ассоциативности бинарной операции по тесту Лайта.
7) Классификация элементов полугруппы.
8) Представление полугрупп преобразованиями.
9) Представление полугрупп словами.
10) Определение группы и примеры групп.
11) Определение кольца и примеры колец.
12) Определение области целостности и теорема Веддербарна.
13) Определение поля и примеры полей.
14) Отношение делимости элементов кольца.
15) Факториальное кольцо, кольцо главных идеалов и евклидово кольцо.
16) Взаимосвязь между свойствами колец.

ГЛАВА 3

# ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика – это раздел математики, в котором изучаются методы построения комбинаций элементов конечных множеств в соответствии со специальными правилами. Такие комбинации принято называть комбинаторными конфигурациями. Простейшими примерами комбинаторных конфигураций являются перестановки элементов конечного множества и его конечные подмножества с наперед заданным числом элементов. При изучении комбинаторных конфигураций принципиально важными проблемами являются задачи существования таких конфигураций, нахождения методов их построения и определения правил подсчета числа таких конфигураций.

## 3.1. Основные правила комбинаторики

Простейшими правилами подсчета числа комбинаторных конфигураций являются следующие правила суммы, произведения и степени.

*Правило суммы*: если элемент $x_1$ можно выбрать $n_1$ способами и элемент $x_2$ можно выбрать $n_2$ способами, причем все эти способы выбора попарно различны, то выбор одного из элементов $x_1, x_2$ можно осуществить $n_1 + n_2$ способами.

В общем случае, если элемент $x_1$ можно выбрать $n_1$ способами, элемент $x_2$ можно выбрать $n_2$ способами и т.д., наконец, $x_m$ можно выбрать $n_m$ способами, причем все эти способы выбора попарно различны, то выбор одного из элементов $x_1, x_2, \dots, x_m$ можно осуществить $n_1 + n_2 + \cdots + n_m$ способами.

В теоретико-множественной трактовке правило суммы означает, что для любых конечных взаимно непересекающихся множеств $A_1, A_2, \dots, A_m$ выполняется равенство: $|A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|$.

*Правило произведения*: если элемент $x_1$ можно выбрать $n_1$ способами и элемент $x_2$ можно выбрать $n_2$ способами, то упорядоченный набор $(x_1, x_2)$ можно выбрать $n_1 \cdot n_2$ способами.

В общем случае, если элемент $x_1$ можно выбрать $n_1$ способами и элемент $x_2$ можно выбрать $n_2$ способами и т.д., наконец, элемент $x_m$ можно выбрать $n_m$ способами, то упорядоченный набор $(x_1, x_2, \dots, x_m)$ можно выбрать $n_1.n_2 \cdot \dots \cdot n_m$ способами.

В теоретико-множественной трактовке правило произведения означает, что для любых конечных множеств $A_1, A_2, \dots, A_m$ выполняется равенство: $|A_1 \times A_2 \times \dots \times A_m| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_m|$.

*Правило степени*: если каждый из элементов $x_1, x_2, \dots, x_m$ можно выбрать n способами, то упорядоченный набор $(x_1, x_2, \dots, x_m)$ можно выбрать $n^m$ способами.

В теоретико-множественной трактовке правило степени означает, что для любых конечных множеств A, B множество $A^B$ всех отображений *B* в *A* имеет $|A|^{|B|}$ элементов, т.е. выполняется равенство: $|A^B| = |A|^{|B|}$.

**Задача 1**. Рассматривается алфавит $A = \{0,1\}$. Конечная последовательность $a_1 \dots a_n$ символов алфавита *A* называется словом длины *n*. Определить число слов: а) длины 3; б) длины не больше 4.

*Решение.* Обозначим $N_k$ – число слов длины $k$ и $N_{\le k}$ – число слов длины не больше *k*.

Слово $a_1 a_2 a_3$ длины 3 определяется комбинаторной конфигурацией $(a_1, a_2, a_3)$. Так как каждый из элементов можно выбрать двумя способами, то по правилу произведения: $N_3 = 2 \cdot 2 \cdot 2 = 2^3$.

По правилу суммы: $N_{\le 4} = N_1 + N_2 + N_3 + N_4 = 2 + 2^2 + 2^3 + 2^4 = 30$.

**Задача 2**. Какой длины слова из символов 0,1 достаточны для кодировки 33 букв русского алфавита?

*Решение.* Так как $N_{\le 4} = 30 < 33$, то словами длины не больше 4 невозможно закодировать 33 буквы русского алфавита. С другой стороны, $N_{\le 5} = N_{\le 4} + N_5 = 30 + 2^5 = 62 > 33$. Значит, для кодировки букв русского алфавита достаточны слова длины не больше 5.

**Задача 3.** В замке на общей оси 5 дисков, каждый из которых разделен на 7 секторов. Сколько наборов имеет такой замок?

*Решение.* Наборы замка моделируются комбинаторными конфигурациями вида $(x_1, x_2, x_3, x_4, x_5)$, где $x_1, x_2, x_3, x_4, x_5$ – установленные на 5 дисках некоторые значения из 7 секторов. Значит, по правилу степени число таких наборов равно $7^5$.

## 3.2. Основные комбинаторные конфигурации

Рассмотрим *n*-элементное множество $M = \{a_1, \dots, a_n\}$.

**Определение.** Упорядоченный набор $(x_1, \dots, x_m)$ *m* различных элементов $x_1, \dots, x_m$ множества *M* называется *размещением из n элементов по m*. Другими словами, размещения из *n* элементов по *m* – это комбинации из *m* различных элементов *n*-элементного множества *M*, которые различаются либо составом элементов, либо порядком их расположения в комбинации.

Число всех таких размещений обозначается $A_n^m$ или $(n)_m$ (читается: «число размещений из *n* по *m*»). Из определения по правилу произведения получаем формулу:

$$A_n^m = n \cdot (n-1) \cdot \dots \cdot (n-m+1),$$

для значений $1 \le m \le n$. В остальных случаях считаем: $A_n^0 = A_0^0 = 1$ и $A_n^m = 0$ при $m > n$.

В частности, при $m = n$ получим размещение из *n* по *n* элементов $(x_1, \dots, x_n)$ – упорядоченный набор всех *n* различных элементов множества *M*. Такие наборы называются *перестановками n-элементного множества M*. Другими словами, перестановки *n* элементов – это комбинации из всех элементов *n*-элементного множества *M*, которые различаются порядком расположения элементов.

Число всех таких перестановок обозначается $P_n$ (читается «число перестановок *n* элементов»).

Из определения получаем формулу вычисления числа перестановок:

$P_n = A_n^n = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$ (читается: «*n* факториал»).

В случае $n = 0$ считаем: $P_0 = 0! = 1$.

**Определение.** Подмножество $\{x_1, \dots, x_m\}$ множества *M*, состоящее из *m* различных элементов $x_1, \dots, x_m$, называется *сочетанием из n элементов по m*. Другими словами, сочетания из *n* элементов по *m* – это комбинации из *m* различных элементов *n*-элементного множества *M*, которые различаются составом элементов.

Число всех таких сочетаний обозначается $C_n^m$ (читается: «число сочетаний из *n* по *m*»).

Поскольку в случае $1 \le m \le n$ каждое сочетание из *n* элементов по *m* можно упорядочить *m*! способами и получить из такого сочетания *m*! размещений из *n* элементов по *m*, то выполняется равенство $A_n^m = C_n^m \cdot m!$ Отсюда получаем формулу вычисления числа сочетаний:

$$C_n^m = \frac{A_n^m}{m!} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-m+1)}{m!}.$$

В остальных случаях считаем: $C_n^0 = C_0^0 = 1$ и $C_n^m = 0$ при $m > n$.

После умножения числителя и знаменателя последней дроби на выражение $(n-m)!$ получаем компактную формулу вычисления числа сочетаний:

$$C_n^m = \frac{n!}{m!\,(n-m)!}$$

для значений $1 \le m \le n$.

***Свойства числа сочетаний.***

1) $C_n^m = C_n^{n-m}$;

2) $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$;

3) $(1+x)^n = \sum_{m=0}^{n} C_n^m x^m$ – эта формула называется *биномом Ньютона* (в силу чего комбинаторные числа $C_n^m$ называются также *биномиальными коэффициентами*),

4) $C_n^0 + C_n^1 + \cdots + C_n^n = 2^n$.

Первые два свойства легко доказываются с помощью последней формулы вычисления числа сочетаний. Третье свойство доказывается индукцией по переменной *n* (см. раздел 3.3). Последнее свойство получается из бинома Ньютона подстановкой значения $x = 1$.

Заметим, что второе свойство дает рекуррентное соотношение для последовательного вычисления биномиальных коэффициентов $C_n^m$ с помощью таблицы, которая называется *треугольником Паскаля*.

**Определение.** Упорядоченный набор $(x_1, \ldots, x_m)$ элементов $x_1, \ldots, x_m$ множества *M* называется *размещением с повторением из n элементов по m.* В отличие от обычных размещений из *n* элементов по *m*, в этом случае элементы $x_1, \ldots, x_m$ не обязательно различные.

Число всех таких размещений с повторением обозначается $\overline{A}_n^m$ (читается: «число размещений с повторением из *n* по *m*»).

Так как на каждом из *m* мест в размещении с повторением $(x_1, \ldots, x_m)$ может стоять любой из *n* элементов множества *M*, то по правилу произведения получаем формулу:

$$\overline{A}_n^m = n^m.$$

В частности, при $m = n$ получим размещения с повторением из *n* элементов по *n*, которые называются также *перестановками с повторениями из n элементов.* Если рассматриваются перестановки с повторением из *n* элементов, в которых имеется *k* различных элементов,

каждый из которых встречается соответственно $n_1, \dots, n_k$ раз, то число всех таких перестановок обозначается $P_n(n_1, \dots, n_k)$ и вычисляется по формуле:

$$P_n(n_1, \dots, n_k) = \frac{n!}{n_1! \dots n_k!}.$$

**Определение.** Неупорядоченный набор $\{x_1, \dots, x_m\}$ элементов $x_1, \dots, x_m$ множества *M* называется *сочетанием с повторением из n элементов по m.* В отличие от обычных сочетаний из *n* элементов по *m*, в этом случае элементы $x_1, \dots, x_m$ не обязательно различные.

Число всех таких сочетаний с повторением обозначается $\bar{C}_n^m$ (читается: «число сочетаний с повторением из *n* по *m*»).

Формула вычисления числа сочетаний с повторением имеет вид:

$$\bar{C}_n^m = C_{n+m-1}^m = \frac{(n+m-1)!}{m!\,(n-1)!}.$$

**Задача 1.** Группе из пяти сотрудников выделено три путевки. Сколько существует способов распределения путевок, если: а) все путевки различны (т.е. трех категорий); б) все путевки одинаковы (т.е. одной категории)?

***Решение.*** В случае а) элементарные исходы моделируются комбинаторными конфигурациями вида $(x_1, x_2, x_3)$, где $x_1$ – сотрудник, получивший путевку 1-й категории, $x_2$ – сотрудник, получивший путевку 2-й категории, и $x_3$ – сотрудник, получивший путевку 3-й категории. Так как эта конфигурация является размещением из 5 элементов по 3, то общее число способов распределения путевок равно значению $A_5^3 = 5 \cdot 4 \cdot 3 = 60$.

В случае б) элементарные исходы моделируются комбинаторными конфигурациями вида $\{x_1, x_2, x_3\}$, где $x_1, x_2, x_3$ – сотрудники, получившие путевки одной категории. Так как эта конфигурация является сочетанием из 5 элементов по 3, то общее число способов распределения путевок равно значению $C_5^3 = \frac{5 \cdot 4 \cdot 3}{3!} = 10$.

**Задача 2.** Во взводе 3 сержанта и 30 солдат. Сколько существует способов выделения одного сержанта и трех солдат для патрулирования?

***Решение.*** Назначения патрулей моделируются комбинаторными конфигурациями вида $(x_1, \{y_1, y_2, y_3\})$, где $x_1$ – один сержант,

выделенный в патруль, и $y_1, y_2, y_3$ – три солдата, выделенных в патруль. Элемент $x_1$ можно выбрать 3 способами, а конфигурация $\{y_1, y_2, y_3\}$ является сочетанием из 30 элементов по 3, которую можно выбрать $C_{30}^3$ способами. Тогда по правилу произведения общее число патрулей равно $3 \cdot C_{30}^3 = 3 \cdot \frac{30 \cdot 29 \cdot 28}{3!} = 12180$. Следовательно, всего существует 12180 способов выделения одного сержанта и трех солдат для патрулирования.

## 3.3. Методы вычисления комбинаторных конфигураций

***Принцип включения и исключения.***

Обобщением правила суммы на произвольные два множества *A,B* является очевидное равенство: $|A \cup B| = |A| + |B| - |A \cap B|$.

В общем случае, для произвольных множеств $A_1, \ldots, A_n$ значение $|A_1 \cup \ldots \cup A_n| = |\cup_{i=1}^n A_i|$ вычисляется по следующему правилу, которое называется *принципом включения и исключения*:

$$\left|\bigcup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| +$$

$$+\sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|.$$

**Пример.** Найдем количество трехзначных чисел, в записи которых есть хотя бы одна цифра 5.

Для каждого $1 \le i \le 3$ обозначим $A_i$ множество всех трехзначных чисел, в записи которых цифра 5 стоит на *i*-м месте. Тогда искомое количество трехзначных чисел вычисляется по принципу включения и исключения следующим образом:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| = 10^2 + 9 \cdot 10 + 9 \cdot 10 - 10 - 10 - 9 + 1 = 252.$$

Пусть элементы множества *A* могут обладать *n* свойствами $\alpha_1, \ldots, \alpha_n$ и $N_{i_1,\ldots,i_k}$ – число элементов множества *A*, обладающих свойствами $\alpha_{i_1}, \ldots, \alpha_{i_k}$. Тогда число $N(r)$ элементов множества *A*, обладающих ровно *r* свойствами $(0 \le r \le n)$, вычисляется по формуле:

$$N(r) = \sum_{k=0}^{n-r} (-1)^k C_{r+k}^r S_{r+k},$$

где $S_0 = |A|;\ S_k = \sum_{1 \le i_1 < \cdots < i_k \le n} N_{i_1,\ldots,i_k}, k = \overline{1,n}.$

В частности, число $N(0)$ элементов множества $A$, не обладающих ни одним из $n$ свойств, вычисляется по формуле:

$$N(0) = S_0 - S_1 + S_2 - \cdots + (-1)^n S_n.$$

**Пример.** Если $|X| = n$ и $|Y| = m$, то число $F_{n,m}$ всех отображений множества $X$ на множество $Y$, вычисляется по формуле:

$$F_{n,m} = \sum_{k=0}^{m-1} (-1)^k C_m^k (m-k)^n ,$$

так как любое отображение $f: X \to Y$ может обладать $m$ свойствами $\alpha_i$ – множество значений $f(X)$ не содержит элемент $y_i \in Y$ $(i = \overline{1,m})$ и число отображений $f: X \to Y$, обладающих свойствами $\alpha_{i_1}, \ldots, \alpha_{i_k}$, вычисляется по формуле

$$N_{i_1,\ldots,i_k} = \left|\left(Y \backslash \{y_{i_1}, \ldots, y_{i_k}\}\right)^X\right| = (m-k)^n.$$

Тогда $S_k = C_m^k (m-k)^n$ и $F_{n,m} = N(0)$ вычисляется по приведенной выше формуле.

***Производящие функции.***

**Определение.** Производящей функцией последовательности $a_0, a_1, \ldots, a_n, \ldots$ называется формальный степенной ряд $\sum_{k=0}^{\infty} a_k x^k$ .

Если такой ряд имеет сумму $f(x)$, то по формуле Тейлора коэффициенты исходного степенного ряда вычисляются по формуле:

$$a_n = \frac{f^{(n)}(0)}{n!},$$

где $n = 0,1, \ldots$

**Примеры.**

1. Так как $\sum_{k=0}^{\infty} x^k = (1-x)^{-1}$, то $f(x) = (1-x)^{-1}$ – производящая функция последовательности $1,1,\ldots$
2. Так как $\sum_{k=0}^{\infty} C_n^k x^k = \sum_{k=0}^{n} C_n^k x^k = (1+x)^n$, то $f(x) = (1+x)^n$ – производящая функция последовательности $C_n^0, C_n^1, \ldots, C_n^n$ .

***Математическая индукция.***

Одним из главных свойств системы натуральных чисел является следующий принцип.

**Принцип математической индукции.** Если $P = P(n)$ – такое свойство натуральных чисел $n$, что $n$=1 обладает этим свойством $P$ и вместе с любым натуральным числом $n$ этим свойством $P$ обладает следующее за ним число $n$+1, то данным свойством $P$ обладает каждое натуральное число.

**Пример.** Докажем формулу бинома Ньютона индукцией по переменной $n$. В этом случае для произвольного значения $x \in \mathbf{R}$ свойство $P = P(n)$ натуральных чисел $n$ выражается равенством $(1+x)^n = \sum_{m=0}^{n} C_n^m x^m$.

При $n = 1$ это свойство имеет вид очевидного равенства: $(1+x)^1 = \sum_{m=0}^{1} C_1^m x^m = C_1^0 x^0 + C_1^1 x^1 = 1 + x$. Предположим теперь, что свойство $P$ выполняется для натурального числа $n$, и докажем, что этим свойством $P$ обладает следующее за ним число $n+1$, т.е. выполняется равенство:

$$(1+x)^{n+1} = \sum_{m=0}^{n+1} C_{n+1}^m x^m.$$

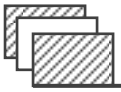
Тогда по нашему предположению с учетом второго свойства числа сочетаний получаем равенства:

$$(1+x)^{n+1} = (1+x)^n(1+x) = \left(\sum_{m=0}^{n} C_n^m x^m\right)(1+x) =$$

$$= \sum_{m=0}^{n} C_n^m x^m + \sum_{m=0}^{n} C_n^m x^{m+1} =$$

$$= C_n^0 x^0 + \sum_{m=1}^{n} C_n^m x^m + \sum_{m=1}^{n} C_n^{m-1} x^m + C_n^n x^{n+1} =$$

$$= C_{n+1}^0 x^0 + \sum_{m=1}^{n} (C_n^m + C_n^{m-1}) x^m + C_{n+1}^{n+1} x^{n+1} = \sum_{m=0}^{n+1} C_{n+1}^m x^m.$$



## *Контрольные вопросы для среза знаний*

1) Правило суммы и его теоретико-множественное истолкование.
2) Правило произведения и его теоретико-множественное истолкование.
3) Правило степени и его теоретико-множественное истолкование.
4) Определение основных комбинаторных конфигураций и формулы вычисления их количества.
5) Свойства числа сочетаний и их приложения.
6) Треугольник Паскаля.
7) Доказательство формулы бинома Ньютона.
8) Формулировка и обоснование принципа включения и исключения.
9) Определение, примеры и приложения производящей функции.
10) Принцип математической индукции.

ГЛАВА 4

# АЛГЕБРА ЛОГИКИ

## 4.1. Определение алгебры логики

**Определение.** Порядок $\leq$ на множестве $A$ называется *решеточным,* если для любых $a,b \in A$ множество $\{a,b\}$ имеет точную верхнюю грань $\sup\{a,b\}$ и точную нижнюю грань $\inf\{a,b\}$, которые принято обозначать символами $a \vee b$ и $a \wedge b$ соответственно. В этом случае на множестве $A$ определены две бинарные операции $\vee$ и $\wedge$, которые называются соответственно *дизъюнкция* и *конъюнкция*, и алгебра $(A,\vee,\wedge)$ называется *решеткой*.

**Определение**. Решетка $(A,\vee,\wedge)$ с наибольшим 1 и наименьшим 0 элементами называется *булевой алгеброй*, если в ней для любого элемента $a \in A$ существует такой элемент $a' \in A$, называемый *дополнением элемента* $a$, что $a \vee a' = 1$ и $a \wedge a' = 0$.

Таким образом, булева алгебра является алгеброй $(A,\vee,\wedge,',1,0)$ типа $\Omega = \{\vee,\wedge,',1,0\}$, где $\vee,\wedge$ – символы бинарных операций конъюнкции и дизъюнкции, $'$ – символ унарной операции дополнения и 1,0 – символы 0-арных операций фиксирования выделенных элементов 1,0. Легко видеть, что операции булевой алгебры удовлетворяют следующим свойствам:

1) $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ – ассоциативность дизъюнкции и конъюнкции;

2) $a \vee b = b \vee a$, $a \wedge b = b \wedge a$ – коммутативность дизъюнкции и конъюнкции;

3) $a \vee a = a$, $a \wedge a = a$ – идемпотентность дизъюнкции и конъюнкции;

4) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ – дистрибутивность соответственно конъюнкции относительно дизъюнкции и дизъюнкции относительно конъюнкции;

5) $(a')' = a$ – идемпотентность дополнения;

6) $(a \vee b)' = a' \wedge b'$, $(a \wedge b)' = a' \vee b'$ – законы де Моргана;

7) $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$ – законы поглощения;

8) $a \vee a' = 1$, $a \wedge a' = 0$ – характеристическое свойство дополнения;

9) $a \vee 1 = 1$, $a \wedge 1 = a$ – характеристическое свойство наибольшего элемента 1;

10) $a \vee 0 = a$, $a \wedge 0 = 0$ – характеристическое свойство наименьшего элемента 0.

Важный пример булевой алгебры дает двухэлементное множество $\boldsymbol{B} = \{0,1\}$ с обычным порядком $0 < 1$ и следующими операциями дизъюнкции $\vee$, конъюнкции $\wedge$ и дополнения $'$:

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $a$ | $a'$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

**Определение.** Алгебра $\boldsymbol{B} = (\{0,1\}, \vee, \wedge, ')$ называется *алгеброй Буля* или *алгеброй логики,* так как она впервые была введена в XIX веке английским математиком Дж. Булем с целью применения в логике математических методов.

**Примеры.**

1. Для любого натурального числа $n$ булевой алгеброй является $n$-я декартова степень $\boldsymbol{B}^n = (\{0,1\}^n; \vee, \wedge, ')$ алгебры Буля $\boldsymbol{B}$ с покомпонентно определенными для ее элементов $a = (a_1,...,a_n)$, $b = (b_1,...,b_n)$ операциями дизъюнкции $a \vee b = (a_1 \vee b_1,...,a_n \vee b_n)$, конъюнкции $a \wedge b = (a_1 \wedge b_1,...,a_n \wedge b_n)$ и отрицания $a' = (a_1',...,a_n')$.

2. Булевой алгеброй является алгебра $\mathcal{P}(X)=(\mathcal{P}(X),\cup,\cap,',X,\varnothing)$ всех подмножеств непустого множества $X$ с теоретико-множественными операциями объединения $\cup$, пересечения $\cap$, дополнения $'$ и фиксирования выделенных элементов $X,\varnothing$.

Заметим, что операция дизъюнкция $x \vee y$ иногда называется *объединением* или *суммой* переменных $x, y$ и обозначается соответственно через $x \cup y$ или $x + y$, а операция конъюнкция $x \wedge y$ иногда называется *пересечением* или *произведением* переменных $x, y$ и обозначается соответственно через $x \cap y$ или $x \cdot y$.

## 4.2. Булевы многочлены и булевы функции

Для описания алгебраических свойств булевых алгебр используются формулы, которые называются *булевыми многочленами* и которые образованы из булевых переменных $x,y,\ldots$(принимающих значения 0,1) и символов булевых операций $+, \cdot, '$ по следующим правилам:

1) все булевы переменные $x,y,\ldots$ и символы 0,1 – булевы многочлены;

2) если $p$ и $q$ – булевы многочлены, то таковыми являются выражения: $(p)+(q), (p)\cdot(q), (p)'$.

При этом скобки в многочленах используются для указания порядка выполнения операций над переменными и по возможности опускаются с учетом следующего приоритета выполнения булевых операций: $'$ , $\cdot$ , $+$. Например, булев многочлен $\Big(\big((x)'\cdot(y)'\big)\Big)+\Big(\big((x)'\big)'\Big)$ можно записать в виде $x'y'+x''$.

Если булев многочлен $p$ образован с помощью переменных $x_1,\ldots,x_n$, то он называется булевым многочленом от $n$ переменных и обозначается символом $p(x_1,\ldots,x_n)$. Множество всех булевых многочленов от $n$ переменных обозначим через $P_n$.

Если в булев многочлен $p(x_1,\ldots,x_n)$ вместо переменных $x_1,\ldots,x_n$ подставить произвольные значения $a_1,\ldots,a_n$ из множества $\boldsymbol{B}$ и для полученного выражения $p(a_1,\ldots,a_n)$ произвести все вычисления в булевой алгебре $\boldsymbol{B}$ по правилу построения исходного булева многочлена, то в результате получится некоторый элемент $\bar{p}(a_1,\ldots,a_n)$ алгебры $\boldsymbol{B}$. Таким образом, каждый булев многочлен $p(x_1,\ldots,x_n)$ определяет отображение $\bar{p}\colon \boldsymbol{B}^n \to \boldsymbol{B}$, которое каждому упорядоченному набору $(a_1,\ldots,a_n)\in \boldsymbol{B}^n$ $n$ элементов $a_1,\ldots,a_n$ множества $\{0,1\}$ ставит в соответствие элемент $\bar{p}(a_1,\ldots,a_n)$ этого же множества $\{0,1\}$. Такое отображение $\bar{p}$ называется *булевой полиномиальной функцией*, определяемой булевым многочленом $p$.

**Пример.** Булев многочлен $p = x'y' + x''$ определяет булеву полиномиальную функцию $\bar{p}$ со значениями:

$$\bar{p}(0,0) = 0'0' + 0'' = 1+0 = 1,\quad \bar{p}(0,1) = 0'1' + 0'' = 0+0 = 0,$$

$$\bar{p}(1,0) = 1'0' + 1'' = 0+1 = 1,\quad \bar{p}(1,1) = 1'1' + 1'' = 0+1 = 1.$$

**Определение.** Булевы многочлены $p, q \in P_n$ называются *эквивалентными*, если они определяют одну и ту же булеву полиномиальную функцию, т.е. выполняется равенство $\overline{p} = \overline{q}$. Символически это записывается формулой $p \sim q$ или просто $p = q$.

Легко видеть, что бинарное отношение ~ является эквивалентностью на множестве $P_n$, которое разбивает это множество на классы эквивалентности $[p] = \{q \in P_n : p \sim q\}$, порождаемые элементами $p \in P_n$ и образующие фактор-множество $P_n / \sim = \{[p] : p \in P_n\}$.

**Определение.** Полные системы представителей фактор-множества $P_n / \sim$ называются *системами нормальных форм* булевых многочленов.

Покажем, что булевыми полиномиальными функциями исчерпываются все отображения вида $f : \boldsymbol{B}^n \to \boldsymbol{B}$, которые называются также *булевыми функциями* от *n* переменных.

Для булевой переменной *x* и значения $\alpha \in \{0,1\}$ введем обозначение:

$$x^{\alpha} = \begin{cases} x, & \text{если } \alpha = 1, \\ x', & \text{если } \alpha = 0, \end{cases}$$

которое называется *литерой.*

**Определение.** Литера, или конъюнкция (соответственно, дизъюнкция) литер, называется *конъюнктом* (соответственно, *дизъюнктом*). Конъюнкт (дизъюнкт) называется *совершенным*, если он содержит все булевы переменные рассматриваемой формулы.

**Определение.** Дизъюнкт, или конъюнкция (совершенных) дизъюнктов, называется (*совершенной*) *конъюнктивной нормальной формой.* Для названия таких форм используются сокращения КНФ и СКНФ соответственно.

**Определение.** Конъюнкт, или дизъюнкция (совершенных) конъюнктов, называется (*совершенной*) *дизъюнктивной нормальной формой*. Для названия таких форм используются сокращения ДНФ и СДНФ соответственно.

Очевидно, что $x^{\alpha} = 1$ в том и только том случае, если $x = \alpha$. Поэтому из свойств булевых операций легко выводятся следующие результаты.

***Теорема***. Любая булева функция $f : \boldsymbol{B}^n \to \boldsymbol{B}$ является булевой полиномиальной функцией следующих булевых многочленов:

$$p_f = \sum_{(\alpha_1,\dots,\alpha_n)\in \boldsymbol{B}^n} f(\alpha_1,\dots,\alpha_n)\cdot x_1^{\alpha_1}\dots x_n^{\alpha_n} \text{ и}$$

$$q_f = \prod_{(\alpha_1,\dots,\alpha_n)\in \boldsymbol{B}^n} (f(\alpha_1,\dots,\alpha_n) + x_1^{\alpha_1'} + \dots + x_n^{\alpha_n'}).$$

***Следствие.*** Если булева функция $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ не равна тождественно нулю, то она является булевой полиномиальной функцией следующей совершенной дизъюнктивной нормальной формы:

$$p_f = \sum_{\substack{(\alpha_1,\dots,\alpha_n)\in \boldsymbol{B}^n,\\ f(\alpha_1,\dots,\alpha_n)=1}} x_1^{\alpha_1}\dots x_n^{\alpha_n},$$

которая называется *совершенной дизъюнктивной нормальной формой* (сокращенно – СДНФ) *функции* $f$.

С другой стороны, если булева функция $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ не равна тождественно единице, то она является булевой полиномиальной функцией следующей совершенной конъюнктивной нормальной формы

$$q_f = \prod_{\substack{(\alpha_1,\dots,\alpha_n)\in \boldsymbol{B}^n,\\ f(\alpha_1,\dots,\alpha_n)=0}} (x_1^{\alpha_1'} + \dots + x_n^{\alpha_n'}),$$

которая называется *совершенной конъюнктивной нормальной формой* (сокращенно – СКНФ) *функции* $f$.

В силу свойств булевых операций СДНФ (соответственно, СКНФ) функции $f$ определяется однозначно с точностью до порядка составляющих эту форму конъюнктов (соответственно, дизъюнктов) и порядка литер в этих конъюнктах (соответственно, дизъюнктах).

*Алгоритм нахождения СДНФ и СКНФ функции* $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$:

1. Составить таблицу значений функции $f$ и добавить к ней два дополнительных столбца с заголовками «Совершенные конъюнкты» и «Совершенные дизъюнкты».

2. Если при значениях $x_1 = k_1,\dots,x_n = k_n$ значение функции $f$ равно 1, то в соответствующей строке таблицы в столбце «Совершенные конъюнкты» записать конъюнкт $x_1^{k_1}\dots x_n^{k_n}$ и в столбце «Совершенные дизъюнкты» сделать прочерк (при этом $x^1 = x$ и $x^0 = x'$).

3. Если при значениях $x_1 = m_1,\dots,x_n = m_n$ значение функции $f$ равно 0, то в соответствующей строке таблицы в столбце «Совершенные

дизъюнкты» записать дизъюнкт $x_1^{m_1'}+\ldots+x_n^{m_n'}$ и в столбце «Совершенные конъюнкты» поставить прочерк.

| $x_1$ | … | $x_n$ | ... | $f(x_1,\ldots,x_n)$ | Совершенные конъюнкты | Совершенные дизъюнкты |
|---|---|---|---|---|---|---|
| … | … | … | ... | … | … | … |
| $k_1$ | … | $k_n$ | ... | 1 | $x_1^{k_1}\ldots x_n^{k_n}$ | – |
| … | … | … | ... | … | … | … |
| $m_1$ | … | $m_n$ | ... | 0 | – | $x_1^{m_1'}+\ldots+x_n^{m_n'}$ |
| … | … | … | ... | … | … | … |

4. Дизъюнкция полученных совершенных конъюнктов $x_1^{k_1}\ldots x_n^{k_n}+\ldots$ является СДНФ функции $f$, конъюнкция полученных совершенных дизъюнктов $(x_1^{m_1'}+\ldots+x_n^{m_n'})\cdot\ldots$ является СКНФ функции $f$.

## 4.3. Системы булевых функций

Операция отрицания $'$ является одной из четырех булевых функций от одной переменной, которые перечисляются в следующей таблице:

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

Очевидно, что функция $f_1(x)\equiv 0$ – константа, тождественно равная нулю, и функция $f_4(x)\equiv 1$ – константа, тождественно равная единице. Функция $f_2(x)=x$ – тождественная функция и функция $f_3(x)=x'$ – операция отрицания.

Булевы операции дизъюнкции и конъюнкции являются примерами двух из шестнадцати булевых функций от двух переменных, которые перечисляются в следующей таблице:

| $x$ | $y$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ | $f_{11}$ | $f_{12}$ | $f_{13}$ | $f_{14}$ | $f_{15}$ | $f_{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| | | 0 | · | $\to'$ | $x$ | $\leftarrow'$ | $y$ | $\oplus$ | + | $\downarrow$ | $\leftrightarrow$ | $y'$ | $\leftarrow$ | $x'$ | $\to$ | $\mid$ | 1 |

Очевидно, что функция $f_1(x,y)\equiv 0$ – константа, тождественно равная нулю, и функция $f_{16}(x,y)\equiv 1$ – константа, тождественно равная единице.

Функция $f_2(x,y)=x\cdot y$ – операция конъюнкции и функция $f_{15}(x,y)=f_2(x,y)'$ – отрицание операции конъюнкции, которая называется *штрихом Шеффера* и обозначается $x\,|\,y$.

Функция $f_8(x,y)=x+y$ – операция дизъюнкции и функция $f_9(x,y)=f_8(x,y)'$ – отрицание операции дизъюнкции, которая называется *стрелкой Пирса* и обозначается $x\downarrow y$.

Функция $f_4(x,y)=x$ – операция проектирования на первый аргумент и функция $f_{13}(x,y)=f_4(x,y)'$ – отрицание этой операции проектирования. Функция $f_6(x,y)=y$ – операция проектирования на второй аргумент и функция $f_{11}(x,y)=f_6(x,y)'$ – отрицание этой операции проектирования.

Функция $f_{10}(x,y)$ называется *эквивалентностью* и обозначается $x\leftrightarrow y$. Функция $f_7(x,y)=f_{10}(x,y)'$ – отрицание эквивалентности, она называется *суммой Жегалкина* и обозначается $x\oplus y$.

Функция $f_{14}(x,y)$ называется *импликацией* и обозначается $x\to y$. Отрицанием импликации является функция $f_3(x,y)=f_{14}(x,y)'$, которая обозначается $x\to' y$.

Функция $f_{12}(x,y)$ называется *обратной импликацией* и обозначается $x\leftarrow y$. Отрицанием обратной импликации является функция $f_5(x,y)=f_{12}(x,y)'$, которая обозначается $x\leftarrow' y$.

Из описанных выше простейших булевых функций можно конструировать более сложные булевы функции с помощью следующей операции.

**Определение.** *Суперпозицией* булевых функций $g(y_1,\ldots,y_m)$ и $h_1(x_1,\ldots,x_n),\ \ldots,h_m(x_1,\ldots,x_n)$ называется булева функция $f(x_1,\ldots,x_n)$, значения которой определяются по формуле:

$$f(x_1,\ldots,x_n)=g\big(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n)\big).$$

**Примеры.**

1. Суперпозицией булевых функций $g(y_1,y_2,y_3)=y_1+y_2+y_3$ и $h_1(x_1,x_2)=x_1x_2$, $h_2(x_1,x_2)=x_1\to x_2$, $h_3(x_1,x_2)=x_1\leftrightarrow x_2$ является булева функция $f(x_1,x_2)=(x_1x_2)+(x_1\to x_2)+(x_1\leftrightarrow x_2)$.

2. Булева функция $f(x_1, x_2) = (x_1 x_2) \leftrightarrow (x_1 + x_2)$ является суперпозицией булевых функций $g(y_1, y_2) = y_1 \leftrightarrow y_2$ и $h_1(x_1, x_2) = x_1 x_2$, $h_2(x_1, x_2) = x_1 + x_2$.

При построении суперпозиции булевых функций необходимо использовать скобки для указания порядка выполнения операций над переменными. Для упрощения записи таких выражений скобки будут по возможности опускаться с учетом следующего приоритета выполнения булевых операций: $'$, $\cdot$ и затем все остальные операции. Например, функцию $\left(\left((x)' \cdot (y)'\right)\right) \to \left(\left((x)'\right)' \mid y\right)$ можно записать в виде $x'y' \to (x'' \mid y)$.

***Лемма.*** Булевы функции от двух переменных взаимосвязаны следующими свойствами:

1) $(x+y)' = x'y'$, $(xy)' = x' + y'$ – законы де Моргана;

2) $x + xy = x$, $x(x+y) = x$ – законы поглощения;

3) $x + x' = 1$, $xx' = 0$ – характеристическое свойство отрицания;

4) $x + 1 = 1$, $x \cdot 1 = x$ – характеристическое свойство элемента 1;

5) $x + 0 = x$, $x \cdot 0 = 0$ – характеристическое свойство элемента 0;

6) $x + y = (x'y')'$, $xy = (x' + y')'$ – взаимосвязь конъюнкции и дизъюнкции;

7) $x \to y = x' + y$, $x \to y = (xy')'$ – взаимосвязь импликации с дизъюнкцией, конъюнкцией и отрицанием;

8) $x \leftrightarrow y = (x \to y)(y \to x)$, $x \leftrightarrow y = (x' + y)(x + y') = xy + x'y'$ – взаимосвязь эквивалентности с импликацией, дизъюнкцией, конъюнкцией и отрицанием;

9) $x \mid y = (xy)'$, $xy = (x \mid y)' = (x \mid y) \mid (x \mid y)$, $x + y = x' \mid y' = (x \mid x) \mid (y \mid y)$, $x' = x \mid x$ – взаимосвязь штриха Шеффера с дизъюнкцией, конъюнкцией и отрицанием;

10) $x \downarrow y = (x + y)'$, $x' = x \downarrow x$, $x + y = (x \downarrow y)' = (x \downarrow y) \downarrow (x \downarrow y)$, $xy = x' \downarrow y' = (x \downarrow x) \downarrow (y \downarrow y)$ – взаимосвязь стрелки Пирса с дизъюнкцией, конъюнкцией и отрицанием;

11) $x \oplus y = y \oplus x$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$, $x(y \oplus z) = xy \oplus xz$, $x \oplus x = 0$, $x \oplus 0 = x$, $x \oplus 1 = x'$, $x \oplus x' = 1$ – характеристическое свойство суммы Жегалкина;

12) $x \oplus y = xy' + x'y$, $x \to y = xy \oplus x \oplus 1$, $x \leftrightarrow y = x \oplus y \oplus 1$, $x + y = (x \oplus 1)(y \oplus 1) \oplus 1 = x \oplus y \oplus xy$ – взаимосвязь суммы Жегалкина с дизъюнкцией, конъюнкцией, отрицанием, импликацией и эквивалентностью.

В частности, из данной леммы следует, что любая булева функция может быть представлена в виде суперпозиции трех булевых функций – дизъюнкции, конъюнкции и отрицания. Обладающие таким свойством системы булевых функций описываются в следующем определении.

**Определение.** Система булевых функций $F = \{f_1,...,f_k\}$ называется *полной*, если любая булева функция может быть представлена в виде суперпозиции функций из этой системы *F*.

Например, в силу п.п. 6) – 8) леммы системы функций $\{+,\cdot,'\}$, $\{+,'\}$ $\{\cdot,'\}$ являются полными системами булевых функций. Система функций $\{\oplus,\cdot,0,1\}$ является полной системой булевых функций в силу следующего результата.

***Теорема Жегалкина.*** Любая булева функция $f$ от $n$ переменных представима полиномом Жегалкина, т.е. в виде

$$f(x_1,...,x_n) = \bigoplus_{(i_1,...i_k)} x_{i_1}...x_{i_k} \oplus c,$$

где $c \in \{0,1\}$ и суммирование ведется по некоторому множеству несовпадающих наборов элементов $(i_1, \dots, i_k)$, удовлетворяющих условию $1 < i_1 < \cdots < i_k \leq n$. Причем такое представление булевой функции $f$ единственно с точностью до порядка слагаемых.

Приведем критерий полноты классов булевых функций, полученный американским математиком Э. Постом.

**Определение.** Булева функция $f$ называется *линейной*, если ее представление полиномом Жегалкина не содержит конъюнкции различных переменных, т.е. имеет вид $f(x_1,...,x_n) = c_0 \oplus c_1x_1 \oplus ... \oplus c_nx_n$ для некоторых значений $c_0, c_1,..., c_n \in \{0,1\}$.

> **Пример.** Функция $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus 1$ является линейной и функция $f(x_1, x_2) = x_1 + x_2$ не является линейной, так как в силу п. 11) леммы выполняется равенство: $x_1 + x_2 = x_1 \oplus x_2 \oplus x_1x_2$.

Множество всех линейных булевых функций обозначим $\mathcal{L}$.

**Определение**. Булева функция $f(x_1,...,x_n)$ называется *самодвойственной*, если выполняется равенство: $f(x_1,...,x_n) = \left(f(x_1',...,x_n')\right)'$.

> **Пример.** Функция $f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ является самодвойственной и функция $f(x_1, x_2) = x_1 + x_2$ не является самодвойственной.

Множество всех самодвойственных булевых функций обозначим $\mathcal{S}$.

**Определение.** Булева функция $f(x_1,...,x_n)$ называется *монотонной*, если для любых $x_1,...,x_n, y_1,...,y_n \in \{0,1\}$ из условий $x_1 \le y_1,...,x_n \le y_n$ следует неравенство: $f(x_1,...,x_n) \le f(y_1,...,y_n)$.

Множество всех монотонных булевых функций обозначим $\mathcal{M}$.

Обозначим символом $\mathcal{P}_0$ класс всех булевых функций $f(x_1,...,x_n)$, удовлетворяющих условию $f(0,...,0)=0$, и символом $\mathcal{P}_1$ – класс всех булевых функций $f(x_1,...,x_n)$, удовлетворяющих условию $f(1,...,1)=1$.

**Определение.** Классы булевых функций $\mathcal{L},\mathcal{S},\mathcal{M},\mathcal{P}_0,\mathcal{P}_1$ называются *классами Поста.*

***Теорема Поста.*** Система булевых функций в том и только том случае является полной, если она не содержится ни в одном из классов Поста.

*Алгоритм доказательства полноты системы булевых функций* $F=\{f_1,...,f_k\}$:

1. Составляем таблицу, столбцы которой помечены классами Поста $\mathcal{L},\mathcal{S},\mathcal{M},\mathcal{P}_0,\mathcal{P}_1$ и строки – функциями рассматриваемой системы $f_1,...,f_n$.

2. Для каждой из функций $f_1,...,f_n$ проверяем принадлежность ее к классам Поста и результаты проверки фиксируем словами «Да» или «Нет» в соответствующей клетке таблицы.

3. По теореме Поста данная система является полной в том и только том случае, если в каждом столбце таблицы имеется слово «Нет».

**Пример.** Рассмотрим систему $F=\{|\}$, состоящую из одной булевой функции | – штрих Шеффера. Составляем таблицу, столбцы которой помечены классами Поста $\mathcal{L},\mathcal{S},\mathcal{M},\mathcal{P}_0,\mathcal{P}_1$ и одна строка – функцией |.

| Функция | Классы Поста | | | | |
|---|---|---|---|---|---|
| | $\mathcal{L}$ | $\mathcal{S}$ | $\mathcal{M}$ | $\mathcal{P}_0$ | $\mathcal{P}_1$ |
| \| | Нет | Нет | Нет | Нет | Нет |

Так как $0|0=1$ и $1|1=0$, то функция | не принадлежит классам $\mathcal{P}_0,\mathcal{P}_1$. В силу свойств $1|0 \ne (0|1)'$, $0|0 > 1|1$ функция | не принадлежит классам $\mathcal{S},\mathcal{M}$. Из равенств $x|y=(xy)'=1 \oplus xy$ следует, что функция | не принадлежит классу $\mathcal{L}$. Таким образом, во всех клетках строки таблицы, помеченной функцией |, записываем

слово «Нет». Следовательно, по теореме Поста система функций $F = \{ | \}$ является полной. Это означает, что любая булева функция представима в виде суперпозиции функции штрих Шеффера.

## 4.4. Минимизация булевых многочленов

Для булевой функции *f* булевы многочлены СДНФ и СКНФ в общем случае не являются минимальными по числу вхождений в них булевых переменных.

Рассмотрим вопрос минимизации ДНФ $p$. Конъюнкт $q$ называется *импликантом* формы $p$, если $pq = q$. Импликанты, минимальные по множеству вхождений в них булевых переменных, называются *простыми импликантами*. Дизъюнкция всех простых импликант формы $p$ называется *сокращенной ДНФ*.

***Лемма.*** Любая ДНФ $p$ эквивалентна некоторой сокращенной ДНФ.

Практически сокращенную ДНФ формы $p$ можно получить *методом Квайна* с помощью последовательного применения следующих двух видов операций:

1) *операция склеивания,* которая для конъюнктов $q$ и булевых переменных $x$ определяется по формуле:

$$qx + qx' = qx + qx' + q;$$

2) *операция поглощения,* которая для конъюнктов $q$, булевых переменных $x$ и значений $\alpha \in \{0,1\}$ определяется по формуле:

$$qx^{\alpha} + q = q.$$

**Пример.** Найдем сокращенную ДНФ для булева многочлена

$$p = x'yz' + x'yz + xy'z + xyz' + xyz.$$

В результате применения операции склеивания к различным парам конъюнктов многочлена $p$ получим ДНФ:

$$x'yz' + x'yz + xy'z + xyz' + xyz + x'y + yz' + yz + xz + xy + y.$$

В результате применения операции поглощения к различным парам конъюнктов последней ДНФ получим булев многочлен $xz + y$, который является сокращенной ДНФ булева многочлена $p$.

Заметим, что на каждом этапе вычислений при выполнении операции склеивания можно не переписывать члены, участвующие в склеивании, а выписывать только полученные результаты склеивания и конъюнкты, не участвующие ни в каком склеивании.

В общем случае сокращенная ДНФ формы $p$ не является минимальной формой, так как она может содержать *лишние* импликанты, удаление которых не изменяет булеву функцию $\overline{p}$. В результате удаления таких лишних импликант получаются *тупиковые ДНФ*. Тупиковые ДНФ с наименьшим числом вхождений в них булевых переменных называются *минимальными ДНФ* (сокращенно – МДНФ).

***Теорема.*** Любая ДНФ $p$ эквивалентна некоторой минимальной ДНФ.

Практически минимальную ДНФ формы $p$ можно получить из ее сокращенной ДНФ с помощью следующей *матрицы Квайна*:

– столбцы матрицы помечаются конъюнктами $p_1,...,p_m$ формы $p$ ;

– строки матрицы помечаются импликантами $q_1,...,q_k$ сокращенной ДНФ формы $p$ ;

– на пересечении строки $q_i$ и столбца $p_j$ ставится символ $*$, если импликант $q_i$ является делителем конъюнкта $p_j$, т.е. $p_j = q_i q$ для некоторого конъюнкта $q$.

Тупиковые ДНФ будут дизъюнкциями тех минимальных наборов импликант, в строках которых имеются звездочки для всех столбцов матрицы Квайна. Тупиковые ДНФ с наименьшим числом вхождений булевых переменных являются искомыми минимальными ДНФ формы $p$ .

**Примеры.**

1. Найдем минимальную ДНФ для булева многочлена

$$p = x'yz' + x'yz + xy'z + xyz' + xyz\,.$$

В предыдущем примере показано, что булев многочлен $xz + y$ является сокращенной ДНФ исходного многочлена $p$ . Значит, матрица Квайна имеет вид:

| | $x'yz'$ | $x'yz$ | $xy'z$ | $xyz'$ | $xyz$ |
|---|---|---|---|---|---|
| $xz$ | | | * | | * |
| $y$ | * | * | | * | * |

По матрице видно, что минимальный набор импликант, в строках которых имеются звездочки для всех столбцов матрицы Квайна, состоит из конъюнктов $xz$ и $y$. Значит, многочлен $p$ имеет одну тупиковую ДНФ $xz + y$, которая является искомой минимальной ДНФ формы $p$.

2. Найдем минимальную ДНФ для булева многочлена

$$p = x'y'z' + x'y'z + xy'z + xyz.$$

В результате применения операции склеивания к различным парам конъюнктов многочлена $p$ получим ДНФ:

$$x'y'z' + x'y'z + xy'z + xyz + x'y' + y'z + xz.$$

В результате применения операции поглощения к различным парам конъюнктов последней ДНФ получим булев многочлен $x'y' + y'z + xz$, который является сокращенной ДНФ булева многочлена $p$.

Матрица Квайна в этом случае имеет следующий вид:

| | $x'y'z'$ | $x'y'z$ | $xy'z$ | $xyz$ |
|---|---|---|---|---|
| $x'y'$ | * | * | | |
| $y'z$ | | * | * | |
| $xz$ | | | * | * |

По матрице видно, что минимальный набор импликант, в строках которых имеются звездочки для всех столбцов матрицы Квайна, состоит из конъюнктов $x'y'$ и $xz$. Значит, многочлен $p$ имеет одну тупиковую ДНФ $x'y' + xz$, которая является искомой минимальной ДНФ формы $p$.

Ясно, что описанные выше методы нахождения минимальных ДНФ двойственным образом можно преобразовать в методы нахождения минимальных КНФ.

***Следствие.*** Любая булева функция**,** не равная тождественно нулю, представима минимальной ДНФ, и любая булева функция**,** не равная тождественно единице, представима минимальной КНФ.

1) Алгебра логики и основные свойства ее операций.
2) Булевы многочлены и их взаимосвязь с булевыми функциями.
3) Системы нормальных форм булевых многочленов.
4) Построение дизъюнктивной нормальной формы и совершенной дизъюнктивной нормальной формы булева многочлена.
5) Построение конъюнктивной нормальной формы и совершенной конъюнктивной нормальной формы булева многочлена.
6) Булевы функции от двух переменных.
7) Взаимосвязь между булевыми функциями от двух переменных.
8) Равносильные преобразования булевых функций.
9) Полные системы булевых функций.
10) Классы Поста булевых функций.
11) Исследование булевой функции на линейность.
12) Исследование булевой функции на монотонность.
13) Исследование булевой функции на самодвойственность.
14) Критерий Поста полноты системы булевых функций.
15) Алгоритм доказательства полноты системы булевых функций.
16) Построение сокращенных дизъюнктивных нормальных форм булевой функции.
17) Построение тупиковых дизъюнктивных нормальных форм булевой функции.
18) Построение минимальной дизъюнктивной нормальной формы булевой функции.

ГЛАВА 5

# ТЕОРИЯ ГРАФОВ

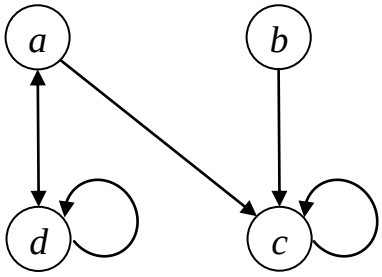
## 5.1. Основные определения

Наглядно-геометрически графы определяются как диаграммы, представляющие собой множество точек плоскости, некоторые из которых соединены непрерывными линиями. Такие точки называются вершинами графа и обозначаются буквами $x_1, x_2, ..., x_n$, а соединяющие их линии – ребрами графа и обозначаются буквами $a_1, a_2, ... , a_m$ . Графы могут быть ориентированными, неориентированными и смешанными.

**Определение.** *Графом* называется алгебраическая система $G = (V, \rho)$, состоящая из непустого множества $V$ и некоторого бинарного отношения $\rho \subset V \times V$ между элементами этого множества $V$. Элементы множества $V$ называются *вершинами* графа и элементы бинарного отношения $\rho$ – *дугами* графа. Для дуги $(a, b) \in \rho$ вершины $a$ называется *началом* и вершина $b$ – *концом* этой дуги. При этом говорят, что такая дуга $(a, b)$ связывает вершины $a$ и $b$, исходит из вершины $a$ и заходит в вершину $b$. В этом случае говорят, что вершина $a$ является предшественником вершины $b$, вершина $b$ – последователем вершины $a$, вершины $a$,$b$ называются *смежными* и *инцидентными* дуге $(a, b)$. Дуга $(a, a) \in \rho$, у которой начало и конец совпадают, называется *петлей* для вершины $a$.

Граф $G = (V, \rho)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ наглядно-геометрически изображается специальным рисунком, который состоит из $n$ выделенных точек, изображающих вершины графа $a_1,...,a_n$, и на котором дуги $(a_i, a_j) \in \rho$ изображаются стрелками – ориентированными кривыми линиями, направленными от $a_i$ к $a_j$. В случае, если $(a_i, a_j) \in \rho$ и $(a_j, a_i) \in \rho$, две противоположно направленные стрелки, соединяющие вершины $a_i, a_j$, изображаются одной стрелкой с двумя противоположными направлениями. Такое изображение графа $G$ называется его геометрической реализацией.

**Пример.** Граф $G = (V, \rho)$ с множеством вершин $V = \{a, b, c, d\}$ и бинарным отношением $\rho = \{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ изображается следующим рисунком:

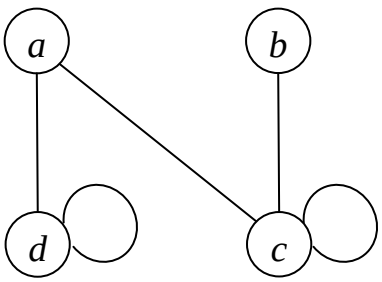



При задании графа $G = (V, \rho)$ принципиальную роль играют элементы бинарного отношения $\rho \subset V \times V$, которые определяют наличие ориентированной связи между вершинами графа. Поэтому такие графы называются также *ориентированными графами*, или кратко – *орграфами*. В случае, когда направленность связи между вершинами графа не важна, приходим к понятию неориентированного графа.

**Определение.** *Неориентированным графом* называется алгебраическая система $G = (V, E)$, состоящая из непустого множества $V$, элементы которого называются *вершинами* графа, и некоторого множества $E$ неупорядоченных пар $\{a, b\}$ элементов $a$,$b$ множества $V$, которые называются *ребрами* графа, соединяющими вершины $a$,$b$. В этом случае вершины $a$,$b$ называются *смежными* и *инцидентными* ребру $\{a, b\}$. Ребро $\{a, a\} \in E$ называется *петлей* для вершины $a$.

Неориентированный граф $G = (V, E)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ наглядно геометрически изображается специальным рисунком, который состоит из $n$ выделенных точек, изображающих вершины графа $a_1,...,a_n$, и на котором ребра $\{a_i, a_j\} \in E$ изображаются непрерывными линиями, соединяющими вершины $a_i, a_j$. Такое изображение графа $G$ называется его геометрической реализацией.

**Пример.** На рисунке изображен неориентированный граф $G = (V, E)$ с множеством вершин $V = \{a, b, c, d\}$ и множеством ребер $E = \{\{a,c\},\{a,d\},\{b,c\},\{c,c\},\{d,d\}\}$:



**Определение.** Неориентированный граф без петель называется *обыкновенным графом*.

Помимо ориентированных и неориентированных графов, отражающих характер связи между вершинами графа, в прикладных задачах приходится рассматривать мультиграфы и взвешенные графы, которые отражают характер нескольких связей между вершинами графа и количественную характеристику таких связей.

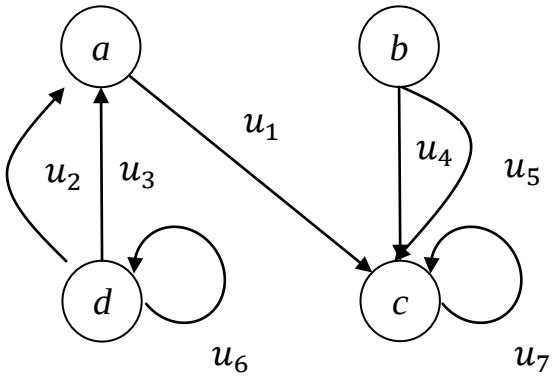
**Определение.** *Мультиграфом* называется алгебраическая система $G = (V, U, \alpha)$, состоящая из непустого множества $V$, элементы которого называются *вершинами* мультиграфа, множества $U$, элементы которого называются *дугами* мультиграфа и некоторого тернарного отношения $\alpha \subset V \times U \times V$, которое называется *инцидентором* мультиграфа. В случае $(a, u, b) \in \alpha$ говорят, что вершины $a$ и $b$ соединяются дугой $u$, которая исходит из вершины $a$ и заходит в вершину $b$. В этом случае вершины $a$,$b$ называются смежными и инцидентными дуге $u$.

Мультиграф $G = (V, U, \alpha)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ наглядно-геометрически изображается специальным рисунком, который состоит из $n$ выделенных точек, изображающих вершины графа $a_1,...,a_n$, и на котором в случае $(a_i, u, a_j) \in \alpha$ дуга $u$ изображается стрелкой, направленной от $a_i$ к $a_j$.

**Пример.** Мультиграф $G = (V, U, \alpha)$ с множеством вершин $V = \{a, b, c, d\}$, множеством дуг $U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7\}$ и инцидентором

$\alpha = \{(a, u_1, c), (d, u_2, a), (d, u_3, a), (b, u_4, c), (b, u_5, c), (d, u_6, d), (c, u_7, c)\}$

изображается следующим рисунком:

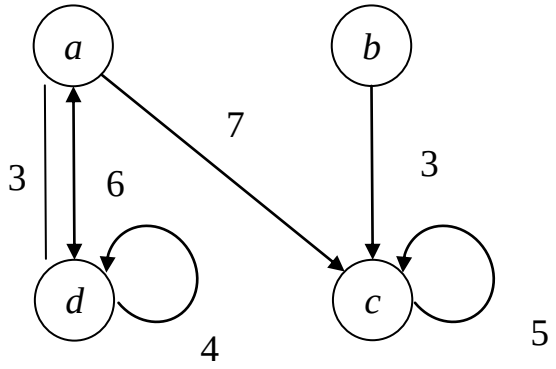



**Определение.** *Взвешенным графом* называется алгебраическая система $G = (V, \rho, c)$, состоящая из непустого множества $V$, элементы которого называются *вершинами* графа, бинарного отношения

$\rho \subset V \times V$, элементы которого называются *дугами* графа, и некоторого отображения $\nu\colon \rho \to \boldsymbol{R}$, которое каждой дуге $(a,b) \in \rho$ ставит в соответствие число $\nu(a,b)$, называемое *весом* этой дуги $(a,b)$.

Взвешенный граф $G = (V, \rho, \nu)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ наглядно геометрически изображается специальным рисунком, который состоит из $n$ выделенных точек, изображающих вершины графа $a_1,...,a_n$, и на котором дуги $(a_i, a_j) \in \rho$ изображаются стрелками с метками $\nu(a_i, a_j)$,, направленными от $a_i$ к $a_j$.

**Пример.** Пусть взвешенный граф $G = (V, \rho, \nu)$ имеет множество вершин $V = \{a, b, c, d\}$, бинарное отношение $\rho = \{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ и отображение $\nu\colon \rho \to \boldsymbol{R}$, определяемое по правилу: $\nu(a,c) = 7, \nu(a,d) = 3, \nu(b,c) = 3,$ $\nu(d,a) = 6, \nu(c,c) = 5, \nu(d,d) = 4$. Тогда граф $G$ изображается следующим рисунком:




***Способы задания графов.***

1. *Теоретико-множественное задание графа* $G = (V, \rho)$ осуществляется с помощью описания множества вершин $V$ и свойства элементов множества дуг графа.

**Пример.** Граф с множеством вершин $V = \{2,3,4,6\}$ и свойством элементов множества дуг $P(a,b) =$ "$a$ делит $b$" имеет множество дуг:

$\rho = \{(a,b) \in V \times V : "a \text{ делит } b"\} = \{(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(6,6)\}.$

2. *Геометрическое задание графа* $G = (V, \rho)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ осуществляется при помощи геометрической реализации этого графа.

3. *Матричное задание графа* $G = (V, \rho)$ с конечным множеством вершин $V = \{a_1,...,a_n\}$ и конечным множеством дуг $\rho = \{u_1,...,u_m\}$ осу-

ществляется либо с помощью матрицы смежности, либо с помощью матрицы инцидентности.

**Определение.** *Матрицей смежности* графа $G$ называется квадратная матрица $M(G)$ порядка $n$, строки и столбцы которой помечены элементами множества вершин $V$, и в которой на пересечении $i$-ой строки и $j$-го столбца стоит элемент $M(G)_{ij}$ множества $\{0,1\}$, определяемый по правилу:

$$M(G)_{ij} = \begin{cases} 1, & \text{если } (a_i, a_j) \in \rho, \\ 0, & \text{в противном случае.} \end{cases}$$

Таким образом, матрица смежности $M(G)$ графа $G$ имеет вид:

$$M(G) = \begin{array}{c} \\ a_1 \\ \vdots \\ a_n \end{array} \begin{array}{c} \begin{array}{ccc} a_1 & \dots & a_n \end{array} \\ \begin{pmatrix} M(G)_{11} & \dots & M(G)_{1n} \\ \dots & \dots & \dots \\ M(G)_{n1} & \dots & M(G)_{nn} \end{pmatrix} \end{array}$$

**Пример.** Граф $G = (V, \rho)$ с множеством вершин $V = \{a, b, c, d\}$ и бинарным отношением $\rho = \{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ имеет следующую матрицу смежности:

$$M(G) = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Для простоты записи матрицы смежности $M(G)$ разметка ее строк и столбцов обычно явно не указывается.

**Определение.** *Матрицей инцидентности* графа $G$ называется прямоугольная матрица $A(G)$ размерности $n \times m$, строки и столбцы которой помечены соответственно элементами множества вершин $V = \{a_1,...,a_n\}$ и элементами множества дуг $\rho = \{u_1,...,u_m\}$ и в которой на пересечении $i$-ой строки и $j$-го столбца стоит элемент $A(G)_{ij}$ множества $\{0,1,-1\}$, определяемый по правилу:

$$A(G)_{ij} = \begin{cases} 1, & \text{если } a_i - \text{начало дуги } u_j, \\ -1, & \text{если } a_i - \text{конец дуги } u_j, \text{ не являющейся петлей}, \\ 0, & \text{если вершина } a_i \text{ не инцидентна дуге } u_j. \end{cases}$$

Таким образом, матрица инцидентности $A(G)$ графа $G$ имеет вид:

$$A(G)=\begin{array}{c} \\ a_1 \\ \vdots \\ a_n \end{array}\begin{array}{c} \begin{array}{ccc} u_1 & \dots & u_m \end{array} \\ \begin{pmatrix} A(G)_{11} & \dots & A(G)_{1m} \\ \dots & \dots & \dots \\ A(G)_{n1} & \dots & A(G)_{nm} \end{pmatrix} \end{array}.$$

**Пример.** Граф $G=(V,\rho)$ с множеством вершин $V=\{a,b,c,d\}$ и бинарным отношением

$$\rho=\{u_1=(a,c),u_2=(a,d),u_3=(b,c),u_4=(c,c),u_5=(d,a),u_6=(d,d)\}$$

имеет следующую матрицу инцидентности:

$$A(G)=\begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{cccccc} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}.$$

Для простоты записи матрицы инцидентности $A(G)$ разметка ее строк и столбцов обычно явно не указывается.

4. *Списочное задание графа* $G=(V,\rho)$ с конечным множеством вершин $V$ осуществляется с помощью *структуры смежности*, представляющей собой список вершин, в котором для каждой вершины $a$ указывается список ее последователей, т.е. таких вершин $b$, что $(a,b)\in\rho$.

**Пример.** Для графа $G=(V,\rho)$ с множеством вершин $V=\{a,b,c,d\}$ и бинарным отношением $\rho=\{(a,c),(a,d)(b,c),(c,c),(d,a),(d,d)\}$ структура смежности имеет вид: $(a\colon c,d),(b\colon c),(c\colon c),(d\colon a,d)$.

Аналогичные способы задания определяются для неориентированных графов, мультиграфов и взвешенных графов.

## 5.2. Обыкновенные графы

Напомним, что обыкновенным графом называется неориентированный граф без петель, т.е. алгебраическая система $G=(V,E)$, состоящая из непустого множества $V$, элементы которого называются *вершинами* графа, и некоторого множества $E$ неупорядоченных пар $\{a,b\}$ попарно различных элементов $a$,$b$ множества $V$, которые называются *ребрами* графа, соединяющими вершины $a$,$b$. В этом случае вершины $a$,$b$ называются *смежными* и *инцидентными* ребру $\{a,b\}$. *Ребра* с общей вершиной называются *смежными*.

Для конечного графа $G = (V, E)$ число вершин обозначается символом $|V|$ и число ребер – символом $|E|$. Число ребер, инцидентных вершине $a \in V$, обозначается символом $d(a)$ и называется *степенью вершины a*. Вершина графа $a$ называется *изолированной*, если ее степень $d(a) = 0$, и *концевой*, если $d(a) = 1$.

Для конечного графа $G = (V, E)$ с множеством вершин $V = \{a_1,...,a_n\}$ вектор $(d(a_1),...,d(a_n))$ называется *распределением степеней вершин* этого графа.

***Лемма о рукопожатиях.*** Для любого графа $G = (V, E)$ сумма степеней всех его вершин равна удвоенному числу его ребер, т.е. выполняется равенство $\sum_{a \in V} d(a) = 2 \cdot |E|$.

*Классификация графов.* Граф $G = (V, E)$ называется:

- *пустым*, если у него нет ребер, т.е. выполняется равенство $E = \emptyset$; пустые графы с $n$ вершинами обозначаются символом $N_n$;
- *полным*, если любая пара его попарно различных вершин соединена ребром, т.е. выполняется равенство $E = \{\{a, b\}: a, b \in V \text{ и } a \neq b\}$; полные графы с $n$ вершинами обозначаются символом $K_n$;
- *двудольным*, если его множество вершин так разбивается на две доли – непустые подмножества $X$ и $Y$, что любое ребро этого графа соединяет вершины из $X$ и $Y$;
- *полным двудольным*, если он двудольный и любая вершина из доли $X$ соединяется ребром с каждой вершиной из доли $Y$; полные двудольные графы, у которых доли $X$ и $Y$ состоят соответственно из $n$ и $m$ вершин, обозначаются символом $K_{n,m}$; при этом граф $K_{1,n}$ называется также звездой с $n$ лучами.

***Действия над графами.***

**Определение.** Граф $G' = (V', E')$ называется *подграфом* графа $G = (V, E)$, если все вершины графа $G'$ являются вершинами графа $G$ и все ребра $G'$ – ребрами $G$, т.е. выполняются условия: $V' \subset V$ и $E' \subset E$. Если при этом выполняется равенство $V' = V$, то граф $G'$ называется *остовным подграфом* графа $G$.

Любое подмножество $X \subset V$ множества вершин графа $G = (V, E)$ определяет подграф $G'$ этого графа $G$ с множеством вершин $X$ и множеством ребер $E'$, состоящим из всех ребер графа $G$, которые соединяют вершины из $X$. Такой подграф $G' = (X, E')$ обозначается символом $\langle X \rangle$ и называется *подграфом* графа $G$, *порожденным множеством вершин* $X$.

*Операцией добавления вершины* $a$ к графу $G = (V, E)$ образуется граф $G + a = (V \cup \{a\}, E)$.

*Операцией добавления ребра* $e = \{a, b\}$ к графу $G = (V, E)$ образуется граф $G + e = (V \cup \{a, b\}, E \cup \{e\})$.

*Операцией удаления вершины* $a$ из графа $G = (V, E)$ образуется граф $G - a = (V \setminus \{a\}, E \setminus \{e \in E : a \in e\})$, который получается из графа $G$ удалением вершины $a$ и всех инцидентных ей ребер.

*Операцией удаления ребра* $e$ образуется граф $G - e = (V, E \setminus \{e\})$, который получается из графа $G$ удалением ребра $e$.

**Определение.** *Дополнением графа* $G = (V, E)$ называется граф $\bar{G} = (V, \bar{E})$ с тем же множеством вершин, в котором различные вершины смежны тогда и только тогда, когда они не смежны в графе $G$.

**Определение.** *Объединением графов* $G' = (V', E')$ и $G = (V, E)$ называется граф $G \cup G' = (V \cup V', E \cup E')$, который получается объединением множеств вершин $V, V'$ и множеств ребер $E, E'$ графов $G, G'$. В случае, когда множества вершин графов $G, G'$ не пересекаются, т.е. $V \cap V' = \emptyset$, объединение графов $G \cup G'$ называется также *суммой* этих *графов* $G, G'$ и обозначается $G + G'$.

**Определение.** *Пересечением графов* $G' = (V', E')$ и $G = (V, E)$ называется граф $G \cap G' = (V \cap V', E \cap E')$, который получается пересечением множеств вершин $V, V'$ и множеств ребер $E, E'$ графов $G, G'$.

**Определение.** *Соединением графов* $G' = (V', E')$ и $G = (V, E)$ называется граф $G \,\overline{\cup}\, G' = \left(V \cup V', E \cup E' \cup \left\{\{a, b\} : a \in V, b \in V', a \neq b\right\}\right)$, который получается объединением множеств вершин $V, V'$ и множеств ребер $E, E'$ графов $G, G'$ с добавлением ребер, соединяющих все вершины графа $G$ со всеми отличными от них вершинами графа $G'$.

**Определение.** *Произведением графов* $G' = (V', E')$ и $G = (V, E)$ называется граф

$$G \times G' = \left(V \times V', \left\{\{(a, a'), (b, b')\} : \{a, b\} \in E, \{a', b'\} \in E'\right\}\right),$$

у которого вершины $(a, a'), (b, b') \in V \times V'$ смежны в том и только том случае, если вершины $a, b$ смежны в графе $G$ и вершины $a', b'$ смежны в графе $G'$.

**Определение.** *Композицией графов* $G' = (V', E')$ и $G = (V, E)$ называется граф

$$G[G'] = \left(V \times V', \left\{\{(a, a'), (b, b')\} : \{a, b\} \in E \text{ или } (a = b \text{ и } \{a', b'\} \in E')\right\}\right),$$

у которого вершины $(a, a'), (b, b') \in V \times V'$ смежны в том и только том случае, если вершины $a, b$ смежны в графе $G$ или эти вершины

совпадают и вершины $a', b'$ смежны в графе $G'$. Наглядно-геометрически композиция графов $G[G']$ получается заменой каждой вершины $a$ графа $G$ на изоморфную копию ${G'}_a$ графа $G'$ и, в случае смежности вершин $a,b$ в графе $G$, добавлением ребер, соединяющим все вершины из ${G'}_a$ с каждой вершиной из ${G'}_b$.

**Определение.** Графы $G = (V, E)$ и $G' = (V', E')$ называются *изоморфными*, если существует биекция $\varphi: V \to V'$, которая сохраняет ребра этих графов, т.е. любые вершины $a, b \in V$ в том и только том случае соединены ребром $\{a, b\} \in E$ в графе $G$, если их образы – вершины $\varphi(a), \varphi(b)$ – соединены ребром $\{\varphi(a), \varphi(b)\}$ в графе $G'$. В этом случае биекция $\varphi$ называется *изоморфизмом* графа $G$ на граф $G'$ и факт изоморфности графов $G, G'$ обозначается символом $G \cong G'$.

С наглядно-геометрической точки зрения графы $G, G'$ изоморфны в том и только том случае, если на геометрической реализации графа $G$ можно так переобозначить вершины, что получится геометрическая реализация графа $G'$. С алгебраической точки зрения изоморфность графов $G, G'$ равносильна тому, что их матрицы смежности получаются друг из друга одновременными перестановками строк и столбцов.

*Инвариантом графа* $G$ называется математический объект (например, число, вектор, фиксированный граф и др.), который сохраняется при действии изоморфизмов. Важным примером инварианта конечного графа является распределение степеней его вершин $(d(a_1),...,d(a_n))$, записанное в порядке их возрастания: $d(a_1) \le ... \le d(a_n)$.

## 5.3. Связность графа

**Определение.** *Маршрутом* графа $G = (V, E)$ называется последовательность его смежных ребер вида $\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{m-1}, v_m\}$. Такой маршрут обозначается

$$v_0 \to v_1 \to v_2 \to \cdots \to v_{m-1} \to v_m$$

и называется маршрутом из вершины $v_0$ в вершину $v_m$, или кратко $(v_0, v_m)$-маршрутом. При этом $v_0$ называется *началом маршрута*, $v_m$ – *концом маршрута* и говорят, что $(v_0, v_m)$-маршрут соединяет вершины $v_0, v_m$. Число $m$ ребер маршрута называется *длиной маршрута*.

Вершины графа $G$ называются *связными*, если в этом графе они соединяются некоторым маршрутом, и несвязными в противном случае.

*Классификация маршрутов.*

Маршрут называется:

– *цепью*, если все его ребра различны;

– *простой цепью*, если различны все его вершины, за исключением, быть может, его начала и конца;

– *замкнутой цепью*, если он является цепью, у которой начало и конец совпадают;

– *циклом*, если он является замкнутой простой цепью, содержащей по крайней мере одно ребро.

*Отношение связности* $\equiv$ на множестве вершин графа $G = (V, E)$ определяется по правилу: $v_0 \equiv v_m$ в том и только том случае, если вершины $v_0, v_m$ равные или связные. Легко видеть, что это отношение является эквивалентностью на множестве вершин графа, которое разбивает это множество на классы эквивалентности, называющиеся *компонентами связности графа. Число компонент связности* графа $G$ обозначается символом $C(G)$.

**Определение.** Граф называется *связным*, если он имеет одну компоненту связности, т.е. любые две различные вершины такого графа соединяются цепью. В противном случае граф называется *несвязным*.

***Теорема.*** Граф в том и только том случае является связным, если его нельзя представить в виде объединения двух непересекающихся графов.

***Лемма 1.*** Для любого графа $G$ с матрицей смежности $A$ справедливы следующие утверждения:

1) матрица $B = A^k$ является матрицей маршрутов длины $k$ графа $G$, т.е. в матрице $B$ элемент $b_{ij} = 1$ в том и только том случае, если в графе $G$ есть $(v_i, v_j)$-маршрут длины $k$;

2) если $E$ – единичная матрица порядка $n$, то матрица

$$C = E + A + A^2 + \cdots + A^{n-1}$$

является матрицей отношения связности графа $G$, т.е. в матрице $C$ элемент $c_{ij} = 1$ в том и только том случае, если вершины $v_i, v_j$ равные или связные.

***Лемма 2.*** Если граф $G$ имеет $n$ вершин, $m$ ребер и $k$ компонент связности, то выполняется неравенство: $m \geq n - k$. В частности, для любого связного графа с $n$ вершинами и $m$ ребрами справедливо неравенство: $m \geq n - 1$.

**Определение.** Ребро $e$ графа $G$ называется *мостом*, если удаление этого ребра из графа $G$ увеличивает число компонент связности, т.е. граф $G - e$ имеет больше компонент связности, чем граф $G$.

**Определение.** Вершина $v$ графа $G$ называется *точкой сочленения*, если удаление этой вершины из графа $G$ увеличивает число компонент связности, т.е. граф $G - a$ имеет больше компонент связности, чем граф $G$.

***Лемма 3.*** Ребро $e$ графа $G$ в том и только том случае является мостом, если это ребро $e$ не содержится в цикле.

***Лемма 4.*** Вершина $v$ графа $G$ в том и только том случае является точкой сочленения, если в графе $G$ найдутся такие вершины $v_1, v_2$, что любой $(v_1, v_2)$-маршрут проходит через вершину $v$.

**Определение.** В графе $G = (V, E)$ для любых его вершин $u, v \in V$ определяется *расстояние* $\rho(u, v)$ между этими вершинами по правилу: $\rho(u, v) = 0$, если $u = v$, $\rho(u, v) = \infty$, если вершины $u, v$ несвязные, и $\rho(u, v) = k$, если вершины $u, v$ связные и $k$ – длина кратчайшей цепи, соединяющей эти вершины.

С помощью расстояния для графа $G = (V, E)$ вводятся следующие числовые характеристики:

– $d(G) = \max_{u,v \in V} \rho(u, v)$ – *диаметр графа G;*

– $r(v) = \max_{x \in V} \rho(v, x)$ – *эксцентриситет вершины* $v$ графа $G$;

– $r(G) = \min_{v \in V} r(v)$ – *радиус графа* $G$.

Вершина $v_0$ называется *центром графа* $G$, если $r(G) = r(v_0)$ .

**Предложение.** Для любого связного графа $G$ выполняются неравенства: $\frac{d(G)}{2} \leq r(G) \leq d(G)$.

*Алгоритм вычисления радиуса и диаметра* графа $G = (V, E)$:

1. Фиксируем вершину $v_0 \in V$ и обозначаем:

– $V_0 = \{v_0\}$ – множество вершин графа $G$, которые находятся на расстоянии 0 от вершины $v_0$;

– $V_1 = \{v : \{v, v_0\} \in E\}$ – множество вершин графа $G$, которые находятся на расстоянии 1 от вершины $v_0$;

– $V_2 = \{v : v \notin V_0 \cup V_1$ и $\{v, v_1\} \in E$ для некоторого $v_1 \in V_1\}$ – множество вершин графа $G$, которые находятся на расстоянии 2 от вершины $v_0$, и так далее.

Этот процесс продолжаем до тех пор, пока не найдется число $k \leq n$, для которого $V_k \neq \emptyset$ и $V_{k+1} = \emptyset$.

2. В результате можно определить расстояние от вершины $v_0$ до любой вершины $v$ из множества $V' = \bigcup_{i=0}^{k} V_i$ как наименьшее значение индекса $i$ множества $V_i$, которому принадлежит вершина $v$. Очевидно, что множество $V'$ является компонентой связности графа $G$, содержащей вершину $v_0$. Поэтому для всех остальных вершин $v \in V \backslash V'$ полагаем $\rho(v_0, v) = \infty$.

В частности, для связного графа $G$ выполняется равенство $V' = V$, и, значит, по определению $r(v_0) = k$. В результате вычисления значений эксцентриситета $r(v)$ для всех вершин $v \in V$ находим радиус и диаметр графа $G$ по формулам: $r(G) = \min_{v \in V} r(v)$ и $d(G) = \max_{v \in V} r(v)$.

## 5.4. Деревья и остовы графов

**Определение.** *Деревом* называется связный граф без циклов.

***Теорема.*** Для связного графа $G = (V, E)$ следующие условия эквивалентны:

1) $G$ – дерево;
2) любые две вершины графа $G$ соединяются единственной цепью;
3) $|E| = |V| - 1$, т.е. число ребер графа $G$ на единицу меньше, чем число его вершин;
4) любое ребро графа $G$ является его мостом;
5) граф $G$ не содержит циклов, но добавление к нему любого нового ребра приводит к образованию ровно одного простого цикла.

**Определение.** Граф, компоненты связности которого являются деревьями, называется *лесом.*

***Лемма 1.*** Граф $G = (V, E)$ является лесом в том и только том случае, если он не содержит циклов. Такой лес удовлетворяет условию $|E| = |V| - C(G)$, где $C(G)$ – число компонент связности графа $G$ .

**Определение.** *Остовом* (или *каркасом*) графа $G = (V, E)$ называется остовной подграф $G' = (V, E')$ этого графа, сохраняющий компоненты связности графа $G$. Другими словами, граф $G' = (V, E')$ является остовом графа $G$, если он имеет одинаковые с графом $G$ компоненты связности и каждая такая компонента является деревом, т.е. ограничение графа $G'$ на каждой компоненте связности графа $G$ является деревом.

В частности, для связного графа $G$ с единственной компонентой связности $K = V$ остовной подграф $G'$ является деревом, которое называется *остовным деревом* графа *G*.

***Лемма 2.*** Пусть граф $G = (V, E)$ имеет $n$ вершин, $m$ ребер и $C(G)$ компонент связности. Тогда для получения остова графа $G$ необходимо удалить из исходного графа $m - n + C(G)$ ребер. Это число называется *циклическим рангом* графа и обозначается $\nu(G) = m - n + C(G)$.

**Следствие.** Граф $G$ в том и только том случае является лесом, если его циклический ранг $\nu(G) = 0$.

Пусть $G = (V, E, c)$ – взвешенный граф, в котором отображение $c: E \to \boldsymbol{R}$ каждому ребру $e \in E$ ставит в соответствие действительное число $c(e)$, называемое весом этого ребра *e*. Тогда каждый остов $T = (V, E')$ графа *G* имеет *вес*

$$c(T) = \sum_{e \in E'} c(e).$$

**Определение.** Остов $T_0$ взвешенного графа *G* называется *остовом минимального веса*, если выполняется условие

$$c(T_0) = \min\{c(T) : T - \text{остов графа } G\}.$$

*Алгоритм построения остова минимального веса для взвешенного графа* $G = (V, E, c)$:

1. Во взвешенном графе *G* строим остовной подграф $T_1 = (V, E_1)$, где $E_1 = \{e_1\}$ и $e_1$ – ребро минимального веса в графе *G*, т.е. $c(e_1) = \min\{c(e) : e \in E\}$;
2. Если во взвешенном графе *G* построен остовной подграф $T_i$ и $i < |V| - C(G)$, то строим новый остовной подграф $T_{i+1} = T_i + e_{i+1}$, где ребро $e_{i+1}$ имеет минимальный вес среди ребер графа *G*, которые не входят в граф $T_i$ и не имеют циклов с ребрами графа $T_i$, т.е.

$c(e_{i+1}) = \min\{c(e) : e \in E \backslash E_i$ и $e$ не образует циклов с ребрами $T_i\}$;

3. Если же во взвешенном графе *G* построен остовной подграф $T_i$ и $i = |V| - C(G)$, то этот подграф $T_i$ является остовом минимального веса взвешенного графа *G*.

*Алгоритм Краскала* построения остова минимального веса для взвешенного графа определяется по тому же принципу, но на каждом шаге алгоритма после выбора ребра минимального веса $e_i$ из графа *G* удаляются все ребра, которые образуют циклы с уже выбранными ребрами.

## 5.5. Обходы графов

Введенное выше для обыкновенного графа понятие цикла остается в силе для любого неориентированного мультиграфа $G$. При этом цикл такого мультиграфа называется *эйлеровым*, если он содержит все ребра мультиграфа $G$, и *гамильтоновым*, если он проходит через каждую вершину мультиграфа $G$ ровно один раз. *Мультиграф,* имеющий эйлеров или гамильтонов цикл, называется соответственно *эйлеровым* или *гамильтоновым*.

***Теорема Эйлера.*** Мультиграф эйлеров в том и только том случае, если он связен и степени всех его вершин четные.

*Алгоритм Флери построения эйлерова цикла в эйлеровом мультиграфе G*:

1. Выбираем произвольную вершину $a$ в мультиграфе $G$.
2. Выбираем произвольное ребро $e = \{a, b\}$ и переходим по нему в вершину $b$, присваиваем этому ребру номер 1, называем его пройденным и удаляем из рассматриваемого мультиграфа $G$.

3. Продолжаем этот процесс для очередных выбранных вершин и каждый раз увеличиваем номер очередного пройденного ребра на единицу до тех пор, пока опять не попадем в исходную вершину $a$. При этом, находясь в вершине $x$, руководствуемся правилами:

1) выбираем по возможности ребро $e = \{x, y\}$ с концом $y \neq a$;

2) не выбираем ребро, являющееся мостом рассматриваемого мультиграфа с непройденными ребрами.

4. Полученная последовательность занумерованных ребер мультиграфа $G$ образует его эйлеров цикл.

***Лемма.*** Если обыкновенный граф $G = (V, E)$ имеет не менее трех вершин и для любых его несмежных вершин $a$,$b$ выполняется условие $d(a) + d(b) \geq |V|$, то граф $G$ гамильтонов.

**Следствие.** Если обыкновенный граф $G = (V, E)$ имеет более трех вершин и для любой его вершины $a$ выполняется условие $d(a) \geq {}^{1}/_{2} \cdot |V|$, то граф $G$ гамильтонов.

Пусть $G = (V, E)$ – связный обыкновенный граф и $T = (V, E')$ – остов этого графа.

Фиксируем вершину $a \in V$ и называем ее корнем дерева $T$. Тогда множество вершин $V$ дерева $T$ разбивается на непересекающиеся уровни – подмножества $V_0, V_1, \ldots, V_k \subset V$, такие что:

1) $V_0 = \{a\}$ – верхний уровень состоит из корня $a$;

2) следующий нижележащий уровень $V_1$ состоит из вершин, смежных с единственной вершиной $a$ верхнего уровня;

3) для последующих значений $i = 2, \dots, k$ соответствующий нижележащий уровень $V_i$ состоит из вершин, смежных с вершинами предыдущего уровня $V_{i-1}$.

В результате получаем $r(a) + 1$ уровней, где $r(a)$ – эксцентриситет вершины $a$. Такое разбиение множества вершин исходного графа $G$ на уровни позволяет организовать упорядоченный перебор всех вершин этого графа следующими двумя способами:

1) *обход графа в глубину* заключается в выборе сначала корня $a$ и затем последовательном просмотре вершин из нижележащих слоев, смежных с предыдущими вершинами; если очередная просматриваемая вершина является концевой, то возвращаемся назад до ближайшей вершины с инцидентными ей еще не рассмотренными ребрами и аналогично просматриваем вершины другого, еще не пройденного маршрута в том же порядке;

2) *обход графа в ширину* заключается в выборе сначала корня $a$ и затем последовательном просмотре вершин строго по слоям, перемещаясь сверху вниз.

При обходе всего множества вершин эти обходы равносильны. Однако в случае поиска одной вершины с определенными свойствами, эффективность успешного завершения того или иного обхода вершин графа определяется структурой дерева: если дерево широкое и концевые вершины расположены на сравнительно близких уровнях, то целесообразней искать такую вершину поиском в глубину; если же дерево узкое и концевые вершины достаточно далеко разбросаны по уровням, то целесообразней искать такую вершину поиском в ширину.

Если при решении задача $A$ разбивается на подзадачи $A(1,1), A(1,2), \dots, A(1, n_1)$, каждая из которых $A(1, i)$, в свою очередь, разбивается на подзадачи $A(2, i, 1), A(2, i, 2), \dots, A(2, i, n_{2,i})$ и так далее, то в результате получается дерево решения задачи $A$, которое осуществляется путем обхода такого дерева поиском в глубину или в ширину. При этом обход дерева может существенно сокращаться с помощью специального *метода ветвей и границ* за счет искусственного отсечения лишних поддеревьев.

## 5.6. Фундаментальные циклы

**Определение.** Пусть обыкновенный граф $G = (V, E)$ имеет $n$ вершин, $m$ ребер и $c = C(G)$ компонент связности. Тогда любой остов этого графа $T = (V, E')$ имеет $n$-$c$ ребер $e_1, \dots, e_{n-c}$, которые называются *ветвями.* Остальные $m$-$n$+$c$ ребер $u_1, \dots, u_{m-n+c}$ графа $G$, которые не вошли в остов $T$, называются *хордами*.

Согласно теореме о деревьях из р. 5.4 при добавлении к остову $T$ любой из хорд $u_i$ получается граф $T + u_i$, содержащий единственный цикл $C_i$, который состоит из хорды $u_i$ и некоторых ветвей остова $T$, образующих единственную цепь, соединяющую вершины этой хорды $u_i$. Такой цикл называется *фундаментальным циклом* графа $G$ относительно хорды $u_i$ остова $T$.

**Определение.** Множество $\{C_1, \dots, C_{m-n+c}\}$ всех фундаментальных циклов графа $G$ относительно хорд остова $T$ называется *фундаментальным множеством циклов* графа $G$ относительно остова $T$. Число элементов такого множества $\nu = m - n + c$ равно цикломатическому числу $\nu(G)$ графа $G$.

Рассмотрим множество всех ребер $E$ графа $G$ в виде следующего упорядоченного набора $m$ элементов:

$$(v_1, \dots, v_m) = (u_1, \dots, u_{m-n+c}, e_1, \dots, e_{n-c}).$$

Тогда каждый фундаментальный цикл $C_i$ определяется $m$-мерным булевым вектором $\bar{a}_i = (a_{i1}, \dots, a_{im})$ с координатами $a_{ij} = 1$, если $v_j \in C_i$, и $a_{ij} = 0$, если $v_j \notin C_i$.

В результате фундаментальное множество циклов графа $G$ можно задать с помощью матрицы фундаментальных циклов $C$, строками которой являются $m$-мерные векторы $\bar{a}_1, \dots, \bar{a}_\nu$:

$$C = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{\nu 1} & \dots & a_{\nu m} \end{pmatrix}.$$

**Определение.** *Псевдоциклом* графа $G$ называется множество ребер $X \subset E$, для которого все вершины подграфа $G' = (V, X)$ имеют четные степени.

В частности, любой цикл графа $G$ является его псевдоциклом. По аналогии с фундаментальными циклами псевдоцикл $X$ определяется $m$-мерным булевым вектором $\bar{x} = (x_1, \dots, x_m)$ с координатами $x_j = 1$, если $v_j \in X$, и $x_j = 0$, если $v_j \notin X$. Тогда фундаментальное множество циклов графа $G$ является базисом векторного пространства его псев-

доциклов над полем $\boldsymbol{Z}_2 = (\{0,1\},\oplus,\cdot)$, т.е. любой псевдоцикл $X$ графа $G$ однозначно представляется в виде линейной комбинации:

$$X = \alpha_1 \cdot C_1 \oplus \ldots \oplus \alpha_{m-n+c} \cdot C_{m-n+c}$$

с булевыми коэффициентами $\alpha_1, \ldots, \alpha_{m-n+c} \in \{0,1\}$.

**Определение.** *Разрезом* графа $G = (V, E)$ называется множество всех ребер $K$, соединяющих вершины двух компонент $V_1, V_2$ некоторого разбиения множества вершин $V = V_1 + V_2$.

В этом случае множество ребер $K$ отделяет вершины множества $V_1$ от вершин множества $V_2$ , т.е. удаление в графе $G$ множества ребер $K$ приводит к тому, что вершины из множеств $V_1$ будут несмежны с вершинами из множества $V_2$ .

**Определение.** Минимальные по включению разрезы графа $G$ называются *коциклами* этого графа.

Другими словами, множество ребер $K \subset E$ является коциклом, если найдется такое разбиение множества вершин $V = V_1 + V_2$, что $K$ состоит из всех ребер, соединяющих вершины из множества $V_1$ с вершинами из множества $V_2$, и при этом любое собственное подмножество множества $K$ таким свойством не обладает ни для какого разбиения множества вершин $V$.

Для связного графа $G$ понятия остова и коцикла являются двойственными в том смысле, что остову графа $G$ соответствует минимальное множество его ребер, связывающее маршрутами все его вершины, а коциклу графа $G$ соответствует минимальное множество его ребер, отделяющее некоторые вершины графа $G$ от всех его остальных вершин.

***Теорема.*** В связном графе любое остовное дерево имеет, по крайней мере, одно общее ребро с каждым разрезом этого графа и любой цикл имеет четное число общих ребер с каждым разрезом этого графа.

Пусть обыкновенный граф $G = (V, E)$ имеет $n$ вершин, $m$ ребер, $c = C(G)$ компонент связности и $T = (V, E')$ – произвольный остов этого графа с $n$-$c$ ветвями $e_1, \ldots, e_{n-c}$ и $m$-$n$+$c$ хордами $u_1, \ldots, u_{m-n+c}$ . Тогда удаление из графа $G$ любой ветви $e_i$ приводит к разбиению множества вершин $V$ на две компоненты связности $V_1, V_2$, которые определяют минимальный по включению разрез $K_i = \{e_i, u_{i_1}, \ldots, u_{i_k}\}$ графа $G$, состоящий из всех ребер, соединяющих вершины множества $V_1$ с вершинами множества $V_2$ . Такой разрез $K_i$ называется *фундаментальным разрезом* графа $G$ относительно ветви $e_i$ остова $T$.

**Определение.** Множество $\{K_1, \dots, K_{n-c}\}$ всех фундаментальных разрезов графа $G$ относительно ветвей остова $T$ называется *фундаментальным множеством коциклов* графа $G$ относительно остова $T$. Число элементов такого множества равно значению $\nu^* = n - C(G)$, которое называется *корангом* графа $G$ и обозначается $\nu^*(G)$.

Рассмотрим множество всех ребер $E$ графа $G$ в виде упорядоченного набора $m$ элементов:

$$(v_1, \dots, v_m) = (u_1, \dots, u_{m-n+c}, e_1, \dots, e_{n-c}).$$

Тогда аналогично фундаментальным циклам каждый фундаментальный разрез $K_i$ определяется $m$-мерным булевым вектором $\bar{b}_i = (b_{i1}, \dots, b_{im})$ с координатами $b_{ij} = 1$, если $v_j \in K_i$, и $b_{ij} = 0$, если $v_j \notin K_i$.

В результате фундаментальное множество коциклов графа $G$ можно задать с помощью матрицы фундаментальных разрезов $K$, строками которой являются $m$-мерные векторы $\bar{b}_1, \dots, \bar{b}_{\nu^*}$:

$$K = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \dots & \dots & \dots \\ b_{\nu^* 1} & \dots & b_{\nu^* m} \end{pmatrix}.$$

По аналогии с фундаментальными циклами фундаментальное множество коциклов графа $G$ является базисом векторного пространства всех разрезов графа $G$ над полем $\boldsymbol{Z}_2 = (\{0,1\}, \oplus, \cdot)$, т.е. любой разрез $K$ графа $G$ однозначно представляется в виде линейной комбинации:

$$K = \alpha_1 \cdot K_1 \oplus \dots \oplus \alpha_{n-c} \cdot K_{n-c}$$

с булевыми коэффициентами $\alpha_1, \dots, \alpha_{n-c} \in \{0,1\}$.

## 5.7. Раскраски графов

**Определение.** Пусть $G = (V, E)$ – обыкновенный граф. *Раскраской* графа $G$ называется отображение $\varphi: V \to \boldsymbol{N}$, которое любым смежным вершинам $a, b \in V$ ставит в соответствие разные значения $\varphi(a) \neq \varphi(b)$. Другими словами, отображение $\varphi$ таким образом ставит в соответствие каждой вершине $a \in V$ значение $\varphi(a) \in \boldsymbol{N}$, называемое *раскраской* или *цветом* этой *вершины* $a$, что любые смежные вершины графа $G$ имеют различные цвета. Число цветов $k$ такой раскраски определяется числом элементов множества значений отображения $\varphi$, т.е. $k = |\{\varphi(a) : a \in V\}|$.

Наименьшее число цветов, позволяющее раскрасить граф $G$, обозначается $\chi(G)$ и называется *хроматическим числом* графа $G$.

**Примеры.**

1. Наименьшее число цветов, позволяющее раскрасить полный граф $K_n$ с $n$ вершинами, равно числу вершин этого графа, т.е. $\chi(K_n) = n$.
2. Наименьшее число цветов, позволяющее раскрасить цикл $C_n$ с $n$ вершинами, равно двум для четного числа $n$ и трем для нечетного числа $n$, т.е. $\chi(C_n) = 2$ для четного $n$ и $\chi(C_n) = 3$ для нечетного $n$.
3. Наименьшее число цветов, позволяющее раскрасить полный двудольный граф $K_{n,m}$ с $n + m$ вершинами, равно двум, т.е. $\chi(K_{n,m}) = 2$.

***Теорема.*** Хроматическое число любого графа $G$ удовлетворяет условию $\chi(G) \leq \deg(G) + 1$, где $\deg(G)$ – наибольшая степень вершин графа $G$.

*Алгоритм последовательной раскраски графа* $G = (V, E)$:

1. Для произвольной вершины $a_1 \in V$ определяем раскраску $\varphi(a_1) = 1$;
2. Если вершины $a_1, \dots, a_i \in V$ раскрашены в $k$ цветов 1,2,…,$k$ и имеется вершина $a_{i+1} \in V \backslash \{a_1, \dots, a_i\}$, то для новой вершина $a_{i+1}$ определяем раскраску $\varphi(a_{i+1})$ как наименьшее натуральное число, которое не используется для раскраски смежных с $a_{i+1}$ вершин, т.е.

$$\varphi(a_{i+1}) = \min \boldsymbol{N} \backslash \{\varphi(a_j) : \ 1 \leq j \leq i \text{ и } \{a_{i+1}, a_j\} \in E\}.$$

В общем случае такая последовательная раскраска графа не является минимальной, т.е. число красок последовательной раскраски графа $G$ может оказаться больше его хроматического числа $\chi(G)$ .

## 5.8. Планарные графы

**Определение.** Граф $G$ называется *планарным*, если он имеет геометрическую реализацию на плоскости в виде диаграммы с непересекающимися ребрами, т.е. граф $G$ можно так наглядно-геометрически изобразить на плоскости, что никакие два его ребра не будут иметь общих точек, за исключением, быть может, общих концов этих ребер. Такое изображение графа $G$ на плоскости называется плоским.

**Пример.** Полные графы $K_2, K_3, K_4$ и граф Петерсена являются планарными. С другой стороны, полный граф $K_5$ и полный двудольный граф $K_{3,3}$ не являются планарными.

Результатом подразбиения ребра $e = \{a, b\}$ в графе $G$ называется граф $G_{a|b} = \big(V \cup \{ab\}, (E \setminus e) \cup \big\{\{a, ab\}, \{ab, b\}\big\}\big)$, который получается из графа $G$ заменой ребра $e$ на $(a,b)$-цепь длины два, проходящую через новую добавленную вершину $ab$. Легко видеть, что графы $G$ и $G_{a|b}$ одновременно планарны или нет. Два графа называются *гомеоморфными*, если их можно получить из одного и того же графа с помощью последовательных подразбиений ребер.

Известный критерий планарности графа дает следующая теорема.

***Теорема Понтрягина – Куратовского.*** Граф $G$ планарен в том и только том случае, если он не содержит подграфа, гомеоморфного графу $K_5$ или графу $K_{3,3}$ .

Результатом стягивания ребра $e = \{a, b\}$ в графе $G = (V, E)$ называется граф $G_{\downarrow e} = \big(V \setminus \{b\}, (E \setminus \{e \in E : b \in e\}) \cup \big\{\{a, c\} : \{b, c\} \in E\big\}\big)$, который получается из графа $G$ удалением вершины $b$ и всех инцидентных ей ребер с последующей заменой этих ребер на смежные вершине $a$ ребра. Легко видеть, что графы $G$ и $G_{\downarrow e}$ одновременно планарны или нет. Граф $G$ называется *стягиваемым* к графу $G'$, если $G'$ можно получить из $G$ с помощью последовательных стягиваний ребер.

Альтернативная форма критерия планарности графа получена К. Вагнером, Ф. Харари и В. Таттом в следующем виде.

***Теорема.*** Граф $G$ планарен в том и только том случае, если он не содержит подграфа, стягиваемого к графу $K_5$ или к графу $K_{3,3}$ .

Оценка хроматического числа планарных графов связана с известной гипотезой четырех красок, которая формулируется следующим образом: хроматическое число любого планарного графа не превосходит четырех, т.е. любой планарный граф может быть раскрашен четырьмя цветами. Заметим, что доказать этот результат удалось только в 1977 году с помощью существенного использования компьютерных вычислений.

## 5.9. Ориентированные графы

Пусть $G = (V, \rho)$ – ориентированный граф (сокращенно – орграф) с множеством вершин $V$ и множеством дуг $\rho \subset V \times V$. Число дуг,

входящих в вершину $a \in V$, обозначается символом $d^+(a)$ и называется *полустепенью захода вершины a*. Число дуг, исходящих из вершины $a \in V$, обозначается символом $d^-(a)$ и называется *полустепенью исхода вершины a*. Вершина орграфа $a$ называется *источником* (соответственно, *стоком*), если ее полустепень захода $d^+(a) = 0$ (соответственно, полустепень исхода $d^-(a) = 0$).

**Определение.** *Ориентированным маршрутом* (сокращенно – *ормаршрутом*) орграфа $G$ называется последовательность его смежных дуг вида $(v_0, v_1), (v_1, v_2), \dots, (v_{m-1}, v_m)$. Такой ормаршрут обозначается $v_0 \to v_1 \to v_2 \to \cdots \to v_{m-1} \to v_m$ и называется ормаршрутом из вершины $v_0$ в вершину $v_m$, или кратко $(v_0, v_m)$-ормаршрутом. При этом $v_0$ называется *началом ормаршрута*, $v_m$ *– концом ормаршрута* и говорят, что $(v_0, v_m)$-ормаршрут соединяет вершину $v_0$ с вершиной $v_m$.

*Классификация ормаршрутов.*

Ормаршрут называется:

– *ориентированной цепью* (сокращенно, *орцепью*), если все его дуги различны;

– *простой орцепью*, если различны все его вершины, за исключением, быть может, его начала и конца;

– *замкнутой орцепью*, если он является орцепью, у которой начало и конец совпадают;

– *ориентированным циклом* (сокращенно, *орциклом*), если он является замкнутой простой орцепью, содержащей по крайней мере одну дугу.

*Отношение сильной связности* $\equiv$ на множестве вершин орграфа $G$ определяется по правилу: $v_1 \equiv v_2$ в том и только том случае, если вершины $v_1, v_2$ равные или каждая из этих вершин соединяется с другой вершиной орцепью. Легко видеть, что это отношение является эквивалентностью на множестве вершин графа, которая разбивает это множество на классы эквивалентности, называющиеся *компонентами сильной связности графа.*

**Определение.** Орграф называется *сильно связным*, если он имеет одну компоненту сильной связности, т.е. любая вершина такого орграфа соединяется орцепью с каждой другой его вершиной.

***Теорема.*** Орграф в том и только том случае *сильно связен,* если в нем существует циклический ормаршрут, проходящий через все вершины этого орграфа.

**Определение.** *Сетью* называется взвешенный орграф, т.е. алгебраическая система $G = (V, \rho, c)$, состоящая из непустого множества вершин $V$, множества дуг $\rho \subset V \times V$ и некоторого отображения $c\colon \rho \to \boldsymbol{R}$, которое каждой дуге $(a, b) \in \rho$ ставит в соответствие число $c(a, b) \in \boldsymbol{R}$, называемое *весом* этой дуги $(a, b)$.

**Определение.** *Длиной орцепи* в сети $G$ называется сумма длин дуг, входящих в эту орцепь.

**Определение.** В графе $G = (V, E)$ для любых его вершин $u, v \in V$ определяется *расстояние* $\rho(u, v)$ между этими вершинами по правилу: $\rho(u, v) = 0$, если $u = v$; $\rho(u, v) = \infty$, если в сети $G$ не существует $(u, v)$-орцепей, $\rho(u, v) = k$, если в сети $G$ существует $(u, v)$-орцепь и $k$ – длина кратчайшей такой орцепи.

Важные практические приложения имеет задача поиска в сети расстояний от фиксированной вершины $v_0 \in V$ до всех вершин $v \in V$.

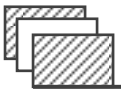
*Алгоритм Дейкстры вычисления расстояний от вершины $v_0 \in V$ до всех вершин $v \in V$*:

1. Обозначаем $v^* = v_0, S = V \backslash \{v_0\}$ и полагаем $\alpha(v^*) = 0$, $\alpha(v) = \infty$, $\beta(v) = \emptyset$ для всех $v \in S$. Переходим к шагу 2.

2. Берем произвольную вершину $v \in \rho(v^*)$ и проверяем неравенство $\alpha(v^*) + c(v^*, v) < \alpha(v)$: если оно выполняется, то полагаем $\alpha(v) = \alpha(v^*) + c(v^*, v), \beta(v) = v^*$, в противном случае значения $\alpha(v), \beta(v)$ оставляем без изменения. Переходим к шагу 3.

3. Если $|S| = 1$ или $\alpha(v) = \infty$ для всех вершин для всех $v \in S$, то работа алгоритма заканчивается: при этом для любой вершины сети $v \neq v_0$ расстояние $\rho(v_0, v) = \alpha(v)$ и в случае $\rho(v_0, v) \neq \infty$ кратчайшая $(v_0, v)$-орцепь строится обратным проходом от вершины $v$ к вершинам $\beta(v), \beta\big(\beta(v)\big)$ и так далее до тех пор, пока не достигнем начальной вершины $v_0$.

Если же $|S| > 1$ и $\alpha(v) \neq \infty$ для некоторой вершины $v \in S$, то находим $\min\{\alpha(v) \mid v \in S\} = \alpha(v')$ для некоторой вершины $v' \in S$ и полагаем $v^* = v'$. Переходим к шагу 2.



## *Контрольные вопросы для среза знаний*

1) Разновидности графов: их определения и способы задания.
2) Определение и классификация маршрутов в графе.
3) Отношение связности вершин графа и компоненты связности графа.
4) Определение расстояния между вершинами графа.
5) Алгоритм вычисления радиуса и диаметра графа.
6) Определение дерева и условия, при которых связный граф является деревом.
7) Алгоритм построения остова минимального веса.
8) Определение эйлерового цикла и алгоритм Флери построения эйлерова цикла в эйлеровом мультиграфе.
9) Определение и условия существования гамильтонового цикла.
10) Обходы графа в глубину и в ширину.
11) Фундаментальное множество циклов графа и пространство псевдоциклов.
12) Разрезы графа и фундаментальное множество коциклов.
13) Определение раскраски графа и хроматического числа графа.
14) Алгоритм последовательной раскраски графа.
15) Определение и критерии планарности графа.
16) Определение и классификация ормаршрутов в ориентированном графе.
17) Отношение сильной связности вершин ориентированого графа и компоненты сильной связности такого графа.
18) Алгоритм Дейкстры вычисления расстояний в сети.

ГЛАВА 6

# ТЕОРИЯ КОДИРОВАНИЯ

## 6.1. Начальные понятия теории кодирования

Пусть $A = \{a_1, \dots, a_r\}$ – конечное множество, называемое *исходным алфавитом*, $A^+$ – множество всех непустых слов над алфавитом и $A^* = A^+ \cup \{\Lambda\}$.

**Определение.** Слово $\alpha \in A^*$ называется *подсловом* слова $\beta \in A^*$, если для некоторых слов $\gamma, \delta \in A^*$ выполняется равенство $\beta = \gamma\alpha\delta$.

**Определение.** Подслово $\alpha$ слова $\beta$ называется:

– *префиксом* (или *началом*) слова $\beta$, если для некоторого слова $\gamma \in A^*$ выполняется равенство $\beta = \alpha\gamma$;

– *суффиксом* (или *концом*) слова $\beta$, если для некоторого слова $\gamma \in A^*$ выполняется равенство $\beta = \gamma\alpha$.

Рассмотрим некоторое подмножество $S \subset A^+$, элементы которого называются *сообщениями*. Такое подмножество $S$ может порождаться различными объектами (техническими устройствами, людьми и др.), которые называются *источниками сообщений* и описываются следующим образом:

1) *теоретико-множественное описание* множества $S$ осуществляется с помощью предиката $P(\alpha)$, описывающего свойства сообщений $\alpha \in S$ (например, «сообщение $\alpha$ имеет фиксированную длину $m$»);

2) *статистическое описание* множества $S$ осуществляется заданием некоторых вероятностных характеристик (например, задаются вероятности появления букв алфавита);

3) *логическое описание* множества $S$ осуществляется с помощью некоторого специального формального языка математической логики (например, языка узкого исчисления предикатов).

Пусть $B = \{b_1, \dots, b_q\}$ – произвольное конечное множество, называемое *кодирующим алфавитом*, $B^+$ – множество всех непустых слов над алфавитом и $B^* = B^+ \cup \{\Lambda\}$.

**Определение.** *Кодированием* сообщений из множества $S \subset A^+$ словами кодирующего алфавита $B$ называется отображение $\varphi: S \to B^*$. Для слова $\alpha \in S$ значение $\varphi(\alpha)$ называется *кодом сообщения* $\alpha$. Кодирование $\varphi$ называется *взаимно однозначным* (или *декодируемым*), если различные сообщения $\alpha \neq \alpha'$ из множества $S$ имеют разные коды $\varphi(\alpha) \neq \varphi(\alpha')$.

Наиболее простой и естественный способ кодирования сообщений исходного алфавита $A$ заключается в кодировании букв этого алфавита $a \in A$ словами $\varphi(a)$ кодирующего алфавита $B$ и определении кода $\varphi(\alpha)$ любого слова $\alpha = a_1 \dots a_n$ из множества $A^+$ по правилу: $\varphi(\alpha) = \varphi(a_1) \dots \varphi(a_n)$, где в правой части равенства выполняется операция конкатенации (т.е. приписывание) слов $\varphi(a_1), \dots, \varphi(a_n)$. Такое кодирование называется *алфавитным кодированием* слов множества $A^+$, порожденным кодированием букв $\varphi: A \to B^*$. При этом множество $\beta_i = \varphi(a_i)$, где $i = \overline{1,r}$ называется множеством *кодовых слов* алфавитного кодирования $\varphi: A^+ \to B^*$.

**Пример.** Пусть исходный алфавит $A = \{a, b, c\}$, кодирующий алфавит $B = \{0,1\}$, и кодирование букв алфавита $A$ определяется по правилу: $\varphi(a) = 00, \varphi(b) = 01, \varphi(c) = 10$. Тогда коды слов $\alpha_1 = abc, \alpha_2 = cba, \alpha_3 = abcba$ имеют, соответственно, вид:

$$\varphi(\alpha_1) = \varphi(a)\varphi(b)\varphi(c) = 000110,\ \varphi(\alpha_2) = \varphi(c)\varphi(b)\varphi(a) = 100100,$$
$$\varphi(\alpha_3) = \varphi(a)\varphi(b)\varphi(c)\varphi(b)\varphi(a) = 0001100100.$$

## 6.2. Классификация алфавитных кодов

**Определение.** Алфавитное кодирование называется:

– *равномерным*, если длины всех его кодовых слов одинаковы;

– *префиксным*, если никакое его кодовое слово не является префиксом (т.е. началом) другого его кодового слова;

– *суффиксным*, если никакое его кодовое слово не является суффиксом (т.е. концом) другого его кодового слова.

**Предложение.** Равномерные, префиксные и суффиксные коды являются взаимно однозначными кодированиями.

В общем случае проверка взаимной однозначности кодирования сводится к проверке его взаимной однозначности на конечном множестве сообщений в силу следующего критерия.

***Критерий Маркова.*** Пусть $\beta_i = \varphi(a_i)$ $(i = \overline{1,r})$ – некоторое кодирование букв алфавита $A = \{a_1, \dots, a_r\}$, $l_i = l(\beta_i)$ $(i = \overline{1,r})$ – длины кодовых слов, $L = \sum_{i=1}^{r} l_i$ и $W$ – максимальное количество $k$ кодовых слов в представлениях кодовых слов $\beta_i$ $(i = \overline{1,r})$ в форме произведений следующего вида $\beta_i = \gamma\beta_{i_1} \dots \beta_{i_k}\delta$. Тогда алфавитное кодирование $\varphi: A^+ \to B^*$ в том и только том случае является взаимно однозначным, если оно взаимно однозначно на множестве сообщений $\alpha \in A^+$, длина которых $l(\alpha)$ не превосходит числа $\frac{(W+1)(L-r+2)}{2}$.

Другими словами, если кодирование $\varphi: A^+ \to B^*$ не является взаимно однозначным, то найдутся такие разные сообщения $\alpha, \alpha' \in A^+$, для которых $\varphi(\alpha) = \varphi(\alpha')$ и $l(\alpha), l(\alpha') \le \frac{(W+1)(L-r+2)}{2}$.

Необходимое условие взаимной однозначности алфавитного кодирования дает следующее неравенство.

***Неравенство Макмиллана.*** Пусть взаимно однозначное алфавитное кодирование $\varphi: A^+ \to B^*$ порождается кодированием букв $\beta_i = \varphi(a_i)$ $(i = \overline{1,r})$ алфавита $A = \{a_1, \dots, a_r\}$ словами кодирующего алфавита $B = \{b_1, \dots, b_q\}$. Тогда длины кодовых слов $l_i = l(\beta_i)$ $(i = \overline{1,r})$ удовлетворяют следующему неравенству: $\sum_{i=1}^{r} \frac{1}{q^{l_i}} \le 1$.

С другой стороны, любой набор натуральных чисел $l_1, \dots, l_r$, удовлетворяющий неравенству Макмиллана, реализуется множеством длин кодовых слов некоторого префиксного кода.

***Теорема.*** Если натуральные числа $l_1, \dots, l_r$ при некотором натуральном значении $q$ удовлетворяют неравенству $\sum_{i=1}^{r} \frac{1}{q^{l_i}} \le 1$, то существует префиксный код $\varphi: A^+ \to B^*$ словами кодирующего алфавита $B = \{b_1, \dots, b_q\}$, который порождается кодированием букв $\beta_i = \varphi(a_i)$ $(i = \overline{1,r})$ кодовыми словами длины $l(\beta_i) = l_i$ $(i = \overline{1,r})$.

## 6.3. Оптимальные алфавитные коды

Пусть для исходного *алфавита* $A = \{a_1, \dots, a_r\}$ известны частоты $p_1, \dots, p_r$ появления соответствующих символов $a_1, \dots, a_r$ в тексте. Очевидно, что все значения $p_i \ge 0$ и $p_1 + \dots + p_r = 1$. Тогда для кодов алфавита $A$ можно ввести численную меру, характеризующую увеличение длины кодируемого текста.

Рассмотрим алфавитное кодирование $\varphi: A^+ \to B^*$, которое порождается кодированием букв $\beta_i = \varphi(a_i)$ $(i = \overline{1,r})$ алфавита $A = \{a_1, \dots, a_r\}$ словами кодирующего алфавита $B = \{b_1, \dots, b_q\}$. Тогда длины кодовых слов $l_i = l(\beta_i)$ $(i = \overline{1,r})$ с соответствующими вероятностями $p_i$ $(i = \overline{1,r})$ можно рассматривать как закон распределения случайной величины $X$. С вероятностной точки зрения среднее значение такой случайной величины $X$ определяется ее математическим ожиданием $M(X) = \sum_{i=1}^{r} l_i p_i$, которое называется *ценой* (*стоимостью* или *избыточностью*) кодирования $\varphi$ и обозначается символом $c(\varphi)$. Ясно, что в этом случае при кодировании текста длины $N$ его длина становится примерно равной значению $Nc(\varphi)$.

**Определение.** Взаимно однозначное алфавитное кодирование $\varphi': A^+ \to B^*$ называется *оптимальным* (или *кодированием с минимальной избыточностью*), если на нем достигается точная нижняя грань $\inf c(\varphi)$ стоимостей всех взаимно однозначных алфавитных кодирований $\varphi$ алфавита $A = \{a_1, \dots, a_r\}$ словами кодирующего алфавита $B = \{b_1, \dots, b_q\}$.

Ясно, что кодирование с минимальной избыточностью дает в среднем минимальное увеличение длины текста при соответствующем кодировании.

**Предложение.** Если существует оптимальное кодирование алфавита $A$ словами кодирующего алфавита $B$, то существует оптимальное префиксное кодирование алфавита $A$ словами кодирующего алфавита $B$.

Оптимальное префиксное кодирование может быть эффективно построено с помощью *кодового дерева*, представляющего собой корневое дерево, ребра которого помечены символами кодирующего алфавита и концевым вершинам которого соответствуют кодовые слова, определяемые метками путей из корня в концевые вершины.

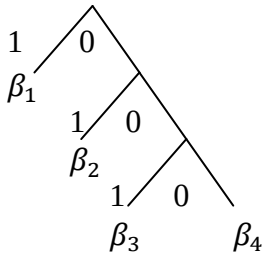
**Пример.** Пусть задан алфавит $A = \{a_1, a_2, a_3, a_4\}$ и набор вероятностей $p_1 = 0{,}35, p_2 = 0{,}3, p_3 = 0{,}2, p_4 = 0{,}15$ появления символов $a_1, a_2, a_3, a_4$. Рассмотрим кодирующий алфавит $B = \{0{,}1\}$ и определим префиксное кодирование букв алфавита $A$ по правилу:

$\varphi(a_1) = \beta_1 = 1, \varphi(a_2) = \beta_2 = 01, \varphi(a_3) = \beta_3 = 001, \varphi(a_4) = \beta_4 = 000.$

Ценой такого кодирования $\varphi$ является число:

$c(\varphi) = \sum_{i=1}^{r} l_i p_i = 1 \cdot 0{,}35 + 2 \cdot 0{,}3 + 3 \cdot (0{,}2 + 0{,}15) = 2.$

Кодовое дерево данного префиксного кодирования $\varphi$ имеет следующий вид:




## 6.4. Коды с исправлением ошибок

В этом разделе рассматриваются равномерные коды с кодирующим алфавитом $B = \{0,1\}$. Пусть длины всех кодовых слов такого кода равны натуральному числу $n$. При передаче закодированных сообщений по каналам связи в связи с действием помех возможны ошибки замещения символов: символ 0 заменяется символом 1 или, наоборот, символ 1 заменяется символом 0.

Теория кодов с исправлением ошибок была разработана в 1950 году Р. Хэммингом.

**Определение.** Код называется *исправляющим r ошибок*, если при наличии в любом кодовом слове не более $r$ ошибок типа замещения можно восстановить исходное кодовое слово.

**Определение.** *Расстоянием Хэмминга* между двумя словами одинаковой длины называется число разрядов, в которых эти слова различаются.

**Определение.** *Шаром* (соответственно, *сферой*) *радиуса r с центром в слове* $\beta_0 = b_1 \dots b_n$ называется множество всех слов $\beta$ длины $n$, расстояние от которых до слова $\beta_0$ не превосходит числа $r$ (соответственно, равно числу $r$). Число элементов такого шара радиуса $r$ обозначается символом $S_r(n)$. Легко видеть, что $S_r(n) = 1 + C_n^1 + \dots + C_n^r$.

Рассмотрим метод построения кода Хэмминга, исправляющего $r$ = 1 ошибок. Пусть сообщение $\alpha = a_1 \dots a_m$ длины $m$ кодируется словом $\beta = b_1 \dots b_n$ длины $n$ с $m$ информационными символами и $k = n - m$ избыточными символами, которые при передаче закодированного сообщения $\beta$ позволяют обнаруживать и исправлять одну ошибку.

Так как при передаче сообщения $\beta$ возможна одна ошибка в любом из $n$ двоичных разрядов $b_1, \dots, b_n$, то для кодировки $n + 1$ возможных результатов передачи сообщения $\beta$ число дополнительных разрядов $k$ в этом сообщении должно удовлетворять условию:

$$2^k \geq n+1, \text{ или } 2^{n-m} \geq n+1, 2^m \leq \frac{2^n}{n+1}.$$

В соответствии с этим необходимым условием обычно выбирается наименьшее целое число $n$, для которого выполняется неравенство $2^m \leq \frac{2^n}{n+1}$.

В кодовом сообщении $\beta = b_1 \ldots b_n\, k$ разрядов с номерами $2^i \left(i = \overline{0, k-1}\right)$ отводятся для контрольных символом и остальные $m = n - k$ разрядов отводятся для информационных символов. Расположенные в этих разрядах символы называются, соответственно, *контрольными* и *информационными* членами кодового сообщения.

Из $n$ номеров разрядов кодового сообщения формируются $k$ множеств $D_i$ $(i = \overline{0, k-1})$, которые состоят из номеров $0 \leq m \leq n$, имеющих в двоичной записи $m = (m_{k-1} \ldots m_i \ldots m_0)_2$ $i$-ую цифру $m_i = 1$. Например, множество $D_0$ состоит из номеров 1,3,5,7,9,…, множество $D_1$ состоит из номеров 2,3,6,7,10,…, множество $D_2$ состоит из номеров 4,5,6,7,12,…, множество $D_{k-1}$ состоит из номеров $2^{k-1}, 2^{k-1}+1, 2^{k-1}+2, \ldots$

Код Хэмминга порядка $n$ определяется как множество $H_n$ слов $\beta = b_1 \ldots b_n$ длины $n$ кодирующего алфавита $B = \{0,1\}$, символы которых удовлетворяют системе $k$ линейных уравнений:

$$\begin{cases} \underset{i \in D_0}{\oplus} b_i = b_1 \oplus b_3 \oplus b_5 \oplus b_7 \oplus b_9 \oplus \ldots = 0, \\ \ldots \\ \underset{i \in D_{k-1}}{\oplus} b_i = b_{2^{k-1}} \oplus b_{2^{k-1}+1} \oplus b_{2^{k-1}+2} \oplus \ldots = 0, \end{cases}$$

где операция суммирования $\oplus$ – это сумма Жегалкина, т.е. сумма элементов множества $B = \{0,1\}$ по модулю 2. Легко видеть, что эта система разрешима относительно $k$ контрольных членов кодового сообщения:

$$\begin{cases} b_1 = b_3 \oplus b_5 \oplus b_7 \oplus b_9 \oplus \ldots, \\ \ldots \\ b_{2^{k-1}} = b_{2^{k-1}+1} \oplus b_{2^{k-1}+2} \oplus \ldots. \end{cases}$$

Значит, общее решение этой системы зависит от $n - k$ произвольных значений информационных членов кодового сообщения, т.е. состоит из $2^{n-k}$ решений.

***Теорема.*** Код Хэмминга $H_n$ исправляет одну ошибку и состоит из $2^{n-k}$ слов, где $k$ – целая часть числа $\log_2 n + 1$.

Обнаружение ошибки в сообщении $\beta' = b'_1 \dots b'_n$, полученном при передаче сообщения $\beta = b_1 \dots b_n$, осуществляется путем суммирования соответствующих разрядов полученного сообщения с номерами из $k$ множеств $D_i$ $(i = \overline{0, k-1})$:

$$\begin{cases} c_0 = b'_1 \oplus b'_3 \oplus b'_5 \oplus b'_7 \oplus b'_9 \oplus \dots, \\ \dots \\ c_{k-1} = b'_{2^{k-1}} \oplus b'_{2^{k-1}+1} \oplus b'_{2^{k-1}+2} \oplus \dots . \end{cases}$$

Если полученная двоичная запись $c = (c_{k-1} \dots c_0)_2$ дает число $c = 0$, то при передаче сообщения ошибок не произошло. В противном случае число $c$ является номером искаженного помехами разряда. В этом случае производится коррекция полученного сообщения $\beta' = b'_1 \dots b'_n$: значение разряда $b'_c$ заменяется на двойственное значение $b'_c \oplus 1$.

**Пример.** Построим код Хэмминга для передачи сообщений длины $m = 3$. Так как наименьшее натуральное число $n$, удовлетворяющее условию $2^3 \le \frac{2^n}{n+1}$ , равно 6, то получаем следующие значения параметров кода Хэмминга с исправлением одной ошибки: $m = 3, n = 6, k = n - m = 3$. Составляем таблицу с 6 столбцами, помеченными номерами разрядов сообщения $\beta = b_1 b_2 b_3 b_4 b_5 b_6$ длины 6:

| **1** | **2** | 3 | **4** | 5 | 6 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 |

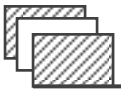
Номера контрольных членов кодового сообщения 1,2,4 выделены жирным шрифтом, и номера информационных членов кодового сообщения 3,5,6 набраны обычным шрифтом. В столбцах с номерами информационных членов в 8 строках выписываются все возможные наборы значений символов $b_3, b_5, b_6$ из 0 и 1: 000,001,010,011,100,101,110,111. Затем заполняются столбцы с номерами контрольных членов значениями символов

$b_1, b_2, b_4$, которые вычисляются по формулам: $b_1 = b_3 \oplus b_5$, $b_2 = b_3 \oplus b_6, b_4 = b_5 \oplus b_6$ .

Если на вход канала поступил код $\beta = 011110$, в котором источник помех исказил 5-й символ, то на выходе получается слово $\beta' = 011100$. Для определения номера $c = (c_2 c_1 c_0)_2$ члена, в котором произошла ошибка, вычисляем значения:

$$c_0 = b'_1 \oplus b'_3 \oplus b'_5 = 0 \oplus 1 \oplus 0 = 1;$$
$$c_1 = b'_2 \oplus b'_3 \oplus b'_6 = 1 \oplus 1 \oplus 0 = 0;$$
$$c_2 = b'_4 \oplus b'_5 \oplus b'_6 = 1 \oplus 0 \oplus 0 = 1.$$

Следовательно, $c = (101)_2 = 5$, т.е. ошибка произошла в 5-м символе. Для коррекции полученного сообщения $\beta' = 011100$ значение разряда $b'_5 = 0$ заменяем на двойственное значение $b'_5 \oplus 1 = 0 \oplus 1 = 1$ и получаем исходное сообщение $\beta = 011110$.



### *Контрольные вопросы для среза знаний*

1) Кодирование сообщений и проблема декодирования.
2) Разновидности алфавитного кодирования.
3) Критерий Маркова взаимной однозначности алфавитного кодирования.
4) Необходимое условие Макмиллана взаимной однозначности алфавитного кодирования.
5) Достаточное условие существования префиксного кода.
6) Избыточность кодирования и определение оптимального кодирования.
7) Взаимосвязь оптимального кодирования с префиксным кодированием.
8) Построение оптимального префиксного кодирования с помощью кодового дерева.
9) Коды с исправлением ошибок.
10) Расстояние Хэмминга и метод построения кода Хэмминга, исправляющего одну ошибку.
11) Свойства кодов Хэмминга.

ГЛАВА 7

# МАТЕМАТИЧЕСКИЕ МОДЕЛИ ВЫЧИСЛЕНИЙ

## 7.1. Переключательные схемы

Под переключательными схемами (сокращенно – ПС) понимаются схемы перемещения различных потоков, регулируемых специальными переключателями. Потоки могут быть, например, электрическими, транспортными, продуктовыми, информационными и др. Переключателями таких потоков являются соответственно электромагнитные реле, светофоры, задвижки трубопроводов, электронные коммутирующие устройства и др. Задачей математического моделирования ПС является математическое описание таких схем с целью построения ПС с заданными свойствами и их последующей оптимизации.

Для определенности далее будем рассматривать электрические ПС, представляющие собой соединенные проводниками переключатели и источники тока. Условимся обозначать символом 1 протекание тока в проводниках и символом 0 – отсутствие тока в проводниках.

**Пример.** На рис.7.1 изображена электрическая ПС с пятью соединенными проводниками переключателями $P_1, P_2, P_3, P_4, P_5$, к которым в точках $A,B$ подключен источник тока.

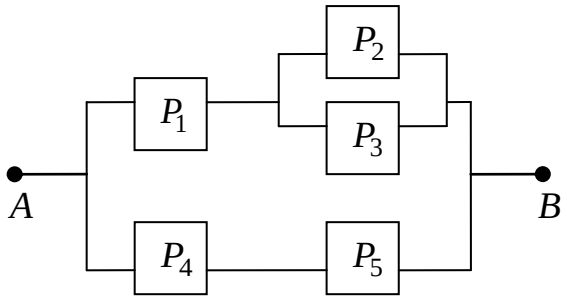



Рис.7.1.
ПС с пятью переключателями $P_1, P_2, P_3, P_4, P_5$

Переключатель электрической ПС представляет собой электромагнитное реле с контактами и индукционной катушкой, состояние которой моделируется с помощью булевой переменной $x$: условие $x = 1$ означает, что в катушке идет ток, и условие $x = 0$ означает, что в катушке тока нет. Контакты реле могут быть замыкающими, если при обесточенной катушке они разомкнуты, и размыкающими в противном случае. Так как через замыкающие контакты реле ток проходит в том и только том случае, если $x = 1$ , то такие контакты моделируется булевой переменной $x$. С другой стороны, поскольку через размыкающие контакты реле ток проходит в том и только том случае, если $x = 0$ , то такие контакты моделируется отрицанием булевой переменной $x'$. Таким образом, переключатели электрических схем моделируются простейшими булевыми многочленами $x$ и $x'$.

**Пример.** Пусть в ПС на рис.7.1 переключатели $P_1, P_5$ имеют общую катушку реле с током $x_1$ и переключатели $P_2, P_4$ имеют общую катушку реле с током $x_2$, причем контакты $P_1, P_2, P_4$ – замыкающие и контакты $P_3, P_5$ – размыкающие. Тогда такая ПС с помощью булевых переменных $x_1, x_2, x_3$ изображается диаграммой на рис.7.2.

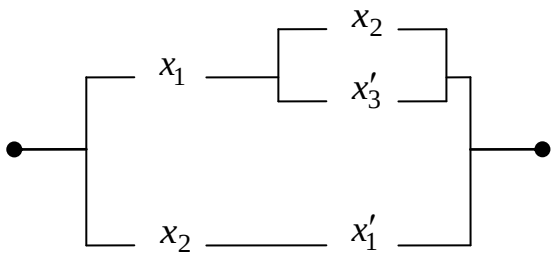



Рис. 7.2.
ПС с пятью переключателями,
изображенными простейшими булевыми многочленами

В электрической схеме два переключателя $p,q$ могут быть соединены последовательно (как показано на рис. 7.3) или параллельно (как показано на рис. 7.4).

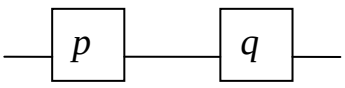



Рис.7.3.
Последовательное соединение
переключателей $p,q$

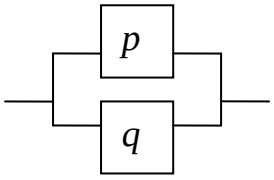



Рис.7.4.
Параллельное соединение
переключателей $p,q$

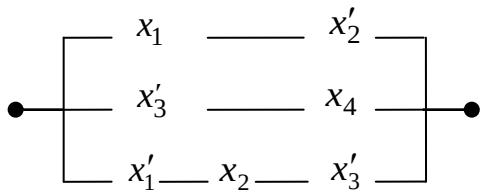
Поскольку через последовательно соединенные переключатели $p,q$ ток проходит в том и только том случае, если $p = q = 1$, то такое соединение моделируется булевым многочленом $p \cdot q$. С другой стороны, поскольку через параллельно соединенные переключатели $p,q$ ток не проходит в том и только том случае, если $p = q = 0$, то такое соединение моделируется булевым многочленом $p + q$.

В результате любая электрическая ПС моделируется некоторым булевым многочленом $p$, который принимает значение 1 в том и только том случае, если в ПС идет ток. Соответствующая такому многочлену $p$ булева функция $\overline{p}$ называется *функцией проводимости ПС*, так как она показывает, при каких значениях булевых переменных (т.е. переключателей данной схемы) в ПС идет электрический ток.

**Пример.** ПС на рис.7.2 моделируется булевым многочленом $p = x_1(x_2 + x_3') + x_2x_1'$.

С другой стороны, каждый булев многочлен $p = p(x_1,...,x_n)$ моделирует ПС с функцией проводимости $\overline{p}$: эта схема так конструируется из переключателей $x_1, x_1',...,x_n, x_n'$, что в ней при значениях $x_1 = a_1,...,x_n = a_n$ проходит ток в том и только том случае, если $\overline{p}(a_1,...,a_n) = 1$.

**Пример.** Булев многочлен $p = x_1x_2' + x_3'x_4 + x_1'x_2x_3'$ моделирует следующую ПС с семью переключателями:




Ясно, что переключательные схемы, моделируемые булевыми многочленами $p$ и $q$, будут действовать идентично в том и только том случае, если определяемые этими многочленами булевы функции $\overline{p}, \overline{q}$ совпадают, т.е. булевы многочлены $p,q$ эквивалентны. Это позволяет оптимизировать переключательные схемы построением идентичных им переключательных схем с минимальным числом переключателей посредством минимизации моделирующих исходную схему булевых многочленов. Так, в силу примера из раздела 4.4 ПС, моделируемая булевым многочленом $p = x'yz' + x'yz + xy'z + xyz' + xyz$, идентична ПС, моделируемой булевым многочленом $xz + y$, который является минимальной ДНФ многочлена $p$.

## 7.2. Схемы из функциональных элементов

Рассмотрим систему булевых функций $B$, которую будем называть *базисом функциональных элементов*. Каждая функция $f = f(x_1, \dots, x_n)$ этого базиса называется *функциональным элементом* и наглядно изображается графом с одной помеченной символом $f$ вершиной, которая имеет одну выходящую дугу и $n$ входящих дуг, помеченных символами $x_1, \dots, x_n$.

Важный пример базиса функциональных элементов дает система $B_0 = \{+, \cdot, '\}$, состоящая из дизъюнкции, конъюнкции и отрицания.

*Схемой из функциональных элементов* (сокращенно – СФЭ) в базисе $B$ называется орграф без ориентированных циклов, в котором источники помечены переменными и называются *входами схемы*, остальные вершины являются функциональными элементами базиса $B$ и некоторые вершины выделены как *выходы схемы*.

Индукцией по глубине $n$ вершины $v$ определяется булева *функция* $f_v$, *реализуемая схемой* в данной вершине:

1) если $n$=0, то $v$ – источник орграфа с приписанной ему некоторой переменной $x$ и по определению $f_v \equiv x$;

2) если $n > 0$ и вершина $v$, помеченная символом $f = f(x_1, \dots, x_k)$, имеет $k$ входящих дуг из вершин $v_1, \dots, v_k$, реализующих функции $g_1, \dots, g_k$, то по определению $f_v = f(g_1, \dots, g_k)$ – суперпозиция функций $f$ и $g_1, \dots, g_k$.

Если схема из функциональных элементов имеет выходы $v_1, \dots, v_m$ , в которых реализуются функции $f_{v_1}, \dots, f_{v_m}$, то говорят, что данная *схема реализует систему функций* $\{f_{v_1}, \dots, f_{v_m}\}$.

*Сложностью* схемы из функциональных элементов называется число функциональных элементов в этой схеме.

***Теорема полноты***. Схемы из функциональных элементов в базисе $B$ в том и только том случае реализуют любую систему булевых функций $\{f_1, \dots, f_m\}$, если базис $B$ является полной системой булевых функций.

В частности, схемы из функциональных элементов в базисе $B_0$ реализуют любые системы булевых функций.

Далее для определенности рассматривается базис функциональных элементов $B_0 = \{+, \cdot, '\}$.

**Примеры.**

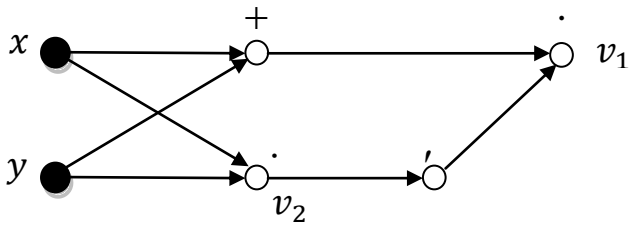
1. Построим схему из функциональных элементов, которая реализует сложение двух двоичных цифр и называется *полусумматором*. Такая схема имеет два входа $x, y$ и два выхода $v_1, v_2$, которые реализуют два разряда $f_{v_1}, f_{v_2}$ суммы чисел $x, y$. Таблица этих булевых функций имеет следующий вид:

| $x$ | $y$ | $f_{v_1}(x,y)$ | $f_{v_2}(x,y)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |

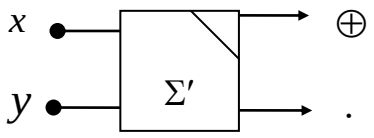
С помощью СКНФ функции $f_{v_1}$ получаем равенства:

$$f_{v_1} = x \oplus y = (x + y)(x' + y') = (x + y)(xy)'.$$

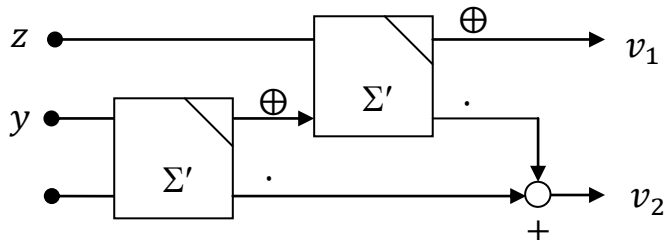
С другой стороны, очевидно, что $f_{v_2} = x \cdot y$. Значит, система булевых функций $\{f_{v_1}, f_{v_2}\}$ реализуется следующей схемой сложности 4:



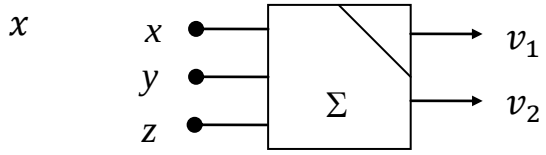

Символически полусумматор обозначается $\Sigma'$ и изображается диаграммой:




2. Построим схему из функциональных элементов, которая реализует сложение трех двоичных цифр и называется *сумматором*. Такая схема имеет три входа $x, y, z$ и два выхода $v_1, v_2$, которые реализуют два разряда $f_{v_1}, f_{v_2}$ суммы чисел $x, y, z$. Очевидно, что $f_{v_1} = (x \oplus y) \oplus z$ и булева функция $f_{v_2}$ имеет СДНФ $f_{v_2} = xyz' + xy'z + x'yz + xyz = xy + (xy' + x'y)z = xy + (x \oplus y)z$. Такая система функций $\{f_{v_1}, f_{v_2}\}$ реализуется следующей схемой сложности 9:




Символически сумматор обозначается Σ и изображается диаграммой:




***Теорема 1.*** Суммирование двух *n*-разрядных двоичных чисел реализуется схемой из функциональных элементов сложности $9n-5$, которая обозначается $S_n$ и называется *сумматором* порядка *n*.

***Теорема 2.*** Умножение двух *n*-разрядных двоичных чисел реализуется схемой из функциональных элементов сложности $O\left(n^{\log_2 3}\right)$, которая обозначается $M_n$ и называется *умножителем* порядка *n*.

## 7.3. Автоматы и рациональные языки

Пусть $A$ – произвольный конечный алфавит, $A^+$ – множество всех непустых слов над алфавитом и $A^* = A^+ \cup \{\Lambda\}$.

**Определение.** Подмножества множества $A^*$ называются *языками* над алфавитом *A*. Для языков $K,L \subset A^*$ определяются три алгебраические операции – сложение, умножение и итерация «звездочка»:

1)сложение $K+L = \{ u : u \in K$ или $u \in L \}$;

2)умножение $K \cdot L = \{uv : u \in K$ и $v \in L\}$;

3)итерация «звездочка» $L^* = \{u_1 \ldots u_n : n \geq 0$ и $u_1, \ldots, u_n \in L\}$.

Кроме того, положим $L^+ = LL^* = \{u_1 \ldots u_n : n > 0$ и $u_1, \ldots, u_n \in L\}$.

Такие операции над языками называются *рациональными операциями*, так как их свойства описываются формулами с символами алгебраических операций +, · , $^*$ и $^+$, которые называются *рациональными выражениями*.

**Определение.** Подмножество $L \subset A^*$ называется *рациональным языком* над алфавитом *A*, если оно получается из конечных подмножеств множества $A^*$ с помощью алгебраических операций сложения, умножения и итерации языков.

Другими словами, рациональные языки – это подмножества $L \subset A^*$, которые получаются из однобуквенных языков $\{a\}$ $(a \in A \cup \{\Lambda\})$с помощью алгебраических операций $+, \cdot, {}^*$ и ${}^+$. Такие языки называются *рациональными*, потому что они определяются рациональными выражениями, т.е. формулами с постоянными символами $a \in A$ и символами рациональных операций $+, \cdot, {}^*$ и ${}^+$.

**Пример.** Рациональный язык $L = \{a, a^2, a^3, \ldots\} \cup \{ab\}$ определяется рациональным выражением $a^+ + ab$.

Обозначим символом $A^\omega$ множество всех бесконечных слов над алфавитом $A$ вида $a_1 a_2 \ldots$. Для слов $w = b_1 \ldots b_n$ из множества $A^*$ и $\alpha = a_1 a_2 \ldots$ из множества $A^\omega$ определяется произведение $w\alpha \in A^\omega$ по следующему правилу: $w\alpha = b_1 \ldots b_n a_1 a_2 \ldots$.

**Определение.** *Автоматом* называется конечная алгебраическая система $\boldsymbol{A} = (Q, A, E, I, F)$, где $Q$ – множество *состояний* автомата, $A$ – *входной алфавит*, $E$ – множество *переходов*, состоящее из упорядоченных троек $(p, a, q) \in Q \times A \times Q$, $I$ – подмножество множества $Q$, называемое множеством *начальных состояний*, и $F$ – подмножество множества $Q$, называемое множеством *заключительных состояний* автомата. Переход $(p, a, q) \in E$ означает, что автомат $\boldsymbol{A}$ под действием входного сигнала $a \in A$ переходит из состояния $p$ в состояние $q$.

Множество $E$ переходов автомата $\boldsymbol{A}$ определяет его *функцию переходов* $\delta$ как отображение множества $A$ в множество всех бинарных отношений на множестве $Q$, которое каждому элементу $a \in A$ ставит в соответствие бинарное отношение $\delta_a \subset Q \times Q$ по следующей формуле:

$$\delta_a = \{(p,q) \in Q \times Q : (p,a,q) \in E\}.$$

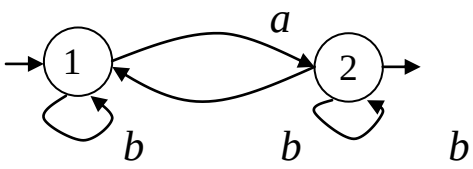
Бинарное отношение $\delta_a$ можно рассматривать как многозначную функцию, которая каждому состоянию автомата $p \in Q$ ставит в соответствие множество состояний $\delta_a(p)$, в которые автомат может переходить из состояния $p$ под действием входного сигнала $a$. Такое отношение $\delta_a$ также называется *функцией переходов* автомата $\boldsymbol{A}$ под действием входного сигнала $a$.

***Способы задания автоматов.***

1. *Графический способ* задания автомата $\boldsymbol{A} = (Q, A, E, I, F)$ заключается в представлении автомата помеченным ориентированным графом, вершины которого изображают состояния автомата $p \in Q$ и дуги

$(p, q)$ с меткой $a \in A$ изображают переходы автомата $(p, a, q) \in E$**.** При этом начальные состояния помечаются входящими в соответствующие вершины короткими стрелками и заключительные состояния – выходящими из соответствующих вершин короткими стрелками.

**Пример.** Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ с множеством состояний $Q = \{1,2\}$, входным алфавитом $A = \{a, b\}$, множеством переходов $E = \{(1, a, 2), (1, b, 1), (2, b, 1), (2, b, 2)\}$, множеством начальных состояний $I = \{1\}$ и множеством заключительных состояний $F = \{2\}$ изображается следующим помеченным ориентированным графом




2. *Матричный способ* задания автомата $\boldsymbol{A} = (Q, A, E, I, F)$ заключается в представлении функций переходов автомата $\delta_a$ $(a \in A)$ квадратными матрицами $\mu_a$ порядка $|Q|$, строки и столбцы которых помечены элементами множества $Q$ и на пересечении строки, помеченной символом $p \in Q$, и столбца, помеченного символом $q \in Q$, стоит элемент $\mu_a(p, q)$, определяющийся по правилу: $\mu_a(p, q) = 1$, если $(p, a, q) \in E$, и $\mu_a(p, q) = 0$, в противном случае.

**Пример.** Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ из предыдущего примера задается двумя матрицами $\mu_a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ и $\mu_b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

3. *Табличный способ* задания автомата $\boldsymbol{A} = (Q, A, E, I, F)$ заключается в представлении его множества переходов $E$ таблицей с $|Q|$ строками, помеченными элементами множества состояний $Q$, и $|A|$ столбцами, помеченными символами входного алфавита $A$, в которой на пересечении строки, помеченной символом $p \in Q$, и столбца, помеченного символом $a \in A$, стоят элементы множества $\delta_a(p)$, т.е. все те состояния автомата, в которые может перейти состояние $p$ под действием входного сигнала $a$. При этом строки таблицы с начальными состояниями помечаются стрелкой $\rightarrow$ и строки с заключительными состояниями помечаются стрелкой $\leftarrow$.

**Пример.** Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ из предыдущего примера задается таблицей

| | | $a$ | $b$ |
|---|---|---|---|
| $\rightarrow$ | 1 | 2 | 1 |
| $\leftarrow$ | 2 | | 1,2 |

Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ называется:

1) *детерминированным*, если для любого $a \in A$ функция переходов $\delta_a$ является преобразованием множества состояний $Q$;

2) *инициальным*, если он имеет единственное начальное состояние $i$, т.е. множество начальных состояний $I = \{i\}$;

3) *акцептором*, если он является инициальным детерминированным автоматом.

**Определение.** *Путем* в автомате $\boldsymbol{A} = (Q, A, E, I, F)$ называется конечная последовательность $p$ его смежных переходов:

$$(q_1, a_1, q_2), (q_2, a_2, q_3), \ldots, (q_n, a_n, q_{n+1}).$$

При этом состояние $q_1$ (соответственно, $q_{n+1}$) называется *началом* (соответственно, *концом*) пути $p$ и слово $a_1 a_2 \ldots a_n$ – *меткой* пути $p$.

Пустое слово $\Lambda$ является меткой пустого пути с совпадающими началом и концом.

**Определение.** Путь $p$ в автомате $\boldsymbol{A}$ называется *успешным*, если его началом является некоторое начальное состояние из множества $I$ и концом – некоторое заключительное состояние из множества $F$.

**Определение.** Множество меток всех успешных путей в автомате $\boldsymbol{A}$ обозначается символом $L(\boldsymbol{A})$ и называется *языком, распознаваемым автоматом* $\boldsymbol{A}$.

Таким образом, по определению

$$L(\boldsymbol{A}) = \{w \in A^* : w \text{ – метка успешного пути в автомате } \boldsymbol{A}\}.$$

**Определение.** Язык $L \subset W(A)$ называется *распознаваемым автоматом*, если $L = L(\boldsymbol{A})$ для некоторого автомата $\boldsymbol{A}$.

**Примеры.**

1. Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ с множеством состояний $Q = \{1\}$, входным алфавитом $A = \{a\}$, пустым множеством переходов $E = \varnothing$, множеством начальных состояний $I = \{1\}$ и множеством заключительных состояний $F = \{1\}$ распознает язык $L(\boldsymbol{A}) = \{\emptyset\}$.

2. Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ с множеством состояний $Q = \{1,2\}$, входным алфавитом $A$, множеством переходов $E = \{(1, a, 2)\}$, множеством начальных состояний $I = \{1\}$ и множеством заключительных состояний $F = \{2\}$ распознает однобуквенный язык $L(\boldsymbol{A}) = \{a\}$.

3. Автомат $\boldsymbol{A} = (Q, A, E, I, F)$ с множеством состояний $Q = \{1,2\}$, входным алфавитом $A = \{a, b\}$, множеством переходов $E = \{(1, a, 2), (1, b, 1), (2, b, 1), (2, b, 2)\}$, множеством начальных состояний $I = \{1\}$ и множеством заключительных состояний $F = \{2\}$ распознает язык:

$$L(\boldsymbol{A}) = \{a, ab, ba, aba, bab, ab^2, \dots\}.$$

***Теорема.*** Язык $L \subset A^*$ в том и только том случае распознаваем автоматом, если этот язык распознаваем акцептором.

***Основные операции над автоматами.***

1. *Суммой автоматов* $\boldsymbol{A}_1 = (Q_1, A, E_1, I_1, F_1)$ и $\boldsymbol{A}_2 = (Q_2, A, E_2, I_2, F_2)$ с непересекающимися множествами состояний $Q_1, Q_2$ называется автомат:

$$\boldsymbol{A}_1 + \boldsymbol{A}_2 = (Q_1 \cup Q_2, A, E_1 \cup E_2, I_1 \cup I_2, F_1 \cup F_2).$$

Легко видеть, что в этом случае $L(\boldsymbol{A}_1 + \boldsymbol{A}_2) = L(\boldsymbol{A}_1) + L(\boldsymbol{A}_2)$.

2. *Произведением акцепторов* $\boldsymbol{A}_1 = (Q_1, A, E_1, \{i_1\}, F_1)$ и $\boldsymbol{A}_2 = (Q_2, A, E_2, \{i_2\}, F_2)$ с непересекающимися множествами состояний $Q_1, Q_2$ называется автомат:

$$\boldsymbol{A}_1 \times \boldsymbol{A}_2 = (Q_1 \cup Q_2, A, E, \{i_1\}, F_2),$$

где $E = E_1 \cup E_2 \cup \{(p, a, i_2) \mid (p, a, f) \in E_1$ для некоторого $f \in F_1\}$.

Легко видеть, что в этом случае $L(\boldsymbol{A}_1 \times \boldsymbol{A}_2) = L(\boldsymbol{A}_1) \cdot L(\boldsymbol{A}_2)$.

3. *Итерацией акцептора* $\boldsymbol{A} = (Q, A, E, \{i\}, F)$ называется автомат:

$$\boldsymbol{A}^{\circ} = (Q, A, E^{\circ}, \{i\}, F),$$

где $E^{\circ} = E \cup \{(p, a, i) \mid (p, a, f) \in E$ для некоторого $f \in F\}$.

Легко видеть, что в этом случае $L(\boldsymbol{A}^{\circ}) = L(\boldsymbol{A})^+$.

***Теорема Клини.*** Язык $L \subset A^*$ в том и только том случае распознаваем автоматом, если этот язык $L$ является рациональным языком.

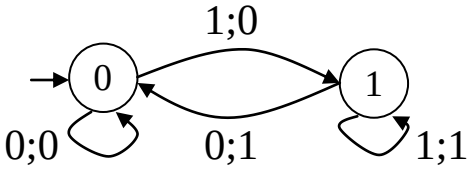
## 7.4. Автоматные отображения

В этом разделе рассматриваются так называемые автоматы Мили, которые определяются следующим образом.

**Определение.** *Автоматом* называется алгебраическая система $\boldsymbol{A} = (Q, A, B, \delta, \lambda, q_0)$, состоящая из *множества состояний* $Q$, множества *входных символов* $A$, множества *выходных символов* $B$, *функции переходов* $\delta: Q \times A \to Q$, *функции выходов* $\lambda: Q \times A \to B$ и *начального состояния* $q_0 \in Q$.

Графический способ задания автомата $\boldsymbol{A} = (Q, A, B, \delta, \lambda, q_0)$ заключается в представлении автомата помеченным ориентированным графом, вершины которого изображают состояния автомата $p \in Q$ и для значений $p \in Q, a \in A, b = \lambda(p, a)$ и $q = \delta(p, a)$ вершины $p, q$ соединяются дугой $(p, q)$ с меткой $a; b$ . При этом начальное состояние автомата помечается входящей в соответствующую вершину $q_0$ короткой стрелкой.

> **Пример.** Автомат $\boldsymbol{A} = (Q, A, B, \delta, \lambda, q_0)$ с множествами $Q = A = B = \{0,1\}$, начальным состоянием $q_0 = 0$ , функцией переходов $\delta(0,0) = \delta(1,0) = 0, \delta(0,1) = \delta(1,1) = 1$ и функцией выходов $\lambda(0,0) = \lambda(0,1) = 0,\ \lambda(1,0) = \lambda(1,1) = 1$ называется *единичной задержкой* и изображается следующим помеченным ориентированным графом:




Автомат называется конечным, если все его основные множества $A,B,Q$ конечные. Такие конечные автоматы являются математическими моделями вычислительных устройств с конечной памятью, которые функционируют в дискретные моменты времени $t = 1,2,\ldots$ (называемые тактами работы автомата). Сигналы, поступающие на вход такого устройства, кодируются символами входного алфавита $A$ и сигналы на выходе устройства кодируются символами выходного алфавита $B$. Состояния автомата определяют распределение памяти вычислительного устройства.

Таким образом, работа автомата может быть описана следующим образом. На первом такте в начальный момент времени $t = 0$ автомат

находится в начальном состоянии $q_0$. Далее, на каждом $t$-м такте работы ($t = 1,2, \ldots$) автомат находится в некотором состоянии $q_{t-1} \in Q$, воспринимает некоторый входной символ $a_t \in A$, согласно функции выходов $\lambda$ выдает выходной символ $b_t = \lambda(q_{t-1}, a_t)$ и затем согласно функции переходов $\delta$ переходит в состояние $q_t = \delta(q_{t-1}, a_t)$. Такой закон функционирования автомата символически определяется следующими соотношениями:

$$b(t) = \lambda(q(t-1), a(t)),\ q(t) = \delta\big(q(t-1), a(t)\big), q(0) = q_0.$$

Такая система равенств называется *системой канонических уравнений*, определяющей работу автомата. Очевидно, что эта система определяет преобразование бесконечных слов входных символов $a_1 a_2 \ldots a_t \ldots$ в бесконечные слова выходных символов $b_1 b_2 \ldots b_t \ldots$ по правилу: $b_t = \lambda(q_{t-1}, a_t)$ и $q_t = \delta(q_{t-1}, a_t)$, где $t = 1,2, \ldots$ Такое отображение множества $A^\omega$ в множество $B^\omega$ обозначается символом $f_{\boldsymbol{A}}$ и называется отображением, реализуемым автоматом $\boldsymbol{A}$.

Отображение $\varphi: A^\omega \to B^\omega$ называется *автоматной функцией*, если оно реализуется некоторым автоматом (т.е. $\varphi = f_{\boldsymbol{A}}$ для некоторого автомата $\boldsymbol{A}$).

> **Пример.** Автомат единичной задержки $\boldsymbol{A} = (Q, A, B, \delta, \lambda, q_0)$ имеет систему канонических уравнений $b(t) = q(t-1)$, $q(t) = a(t), q(0) = 0$ и реализует отображение $f_{\boldsymbol{A}}: A^\omega \to B^\omega$, которое для слов $a_1 a_2 \ldots a_t \ldots$ из множества $A^\omega$ определяется по формуле: $f_{\boldsymbol{A}}(a_1 a_2 \ldots a_t \ldots) = 0 a_1 a_2 \ldots a_t \ldots$.

Отображение $\varphi: A^\omega \to B^\omega$ называется *детерминированной функцией*, если для любого бесконечного слова $\alpha = a_1 a_2 \ldots a_t \ldots$ из множества $A^\omega$ образ $\varphi(\alpha) = b_1 b_2 \ldots b_t \ldots$ состоит из символов $b_t$ ($t = 1,2, \ldots$), которые определяются символами $a_1, a_2, \ldots, a_t$ слова $\alpha$ и не зависят от символов $a_n$ слова $\alpha$ с последующими номерами $n = t+1, t+2, \ldots$.

Для детерминированной функции $\varphi: A^\omega \to B^\omega$ и конечного слова $w = a_1 a_2 \ldots a_n$ над алфавитом $A$ *остаточной функцией* по слову $w$ называется отображение $\varphi_w: A^\omega \to B^\omega$, значение которого для слов $\alpha \in A^\omega$ определяется равенством $\varphi(a_1 a_2 \ldots a_n \alpha) = b_1 b_2 \ldots b_t \varphi_w(\alpha)$.

Детерминированные функции с конечным числом различных остаточных функций называются *ограниченно детерминированными функциями*.

***Теорема 1.*** Отображение $\varphi: A^{\omega} \to B^{\omega}$ в том и только том случае будет автоматной функцией, если оно является ограниченно детерминированной функцией.

Рассмотрим произвольный конечный автомат $\boldsymbol{A} = (Q, A, B, \delta, \lambda, q_0)$. Для $n > \log_2|A|$ входные символы автомата $a \in A$ взимно однозначно кодируются элементами $\bar{a} = (x_1, \dots, x_n)$ множества $\{0,1\}^n$. Аналогично для $m > \log_2|Q|$ состояния автомата $q \in Q$ взимно однозначно кодируются элементами $\bar{q} = (y_1, \dots, y_m)$ множества $\{0,1\}^m$ и для $k > \log_2|B|$ выходные символы автомата $b \in B$ взимно однозначно кодируются элементами $\bar{b} = (z_1, \dots, z_k)$ множества $\{0,1\}^k$. При этом, не нарушая общности, можно считать, что $\overline{q_0} = (0, \dots, 0)$. Тогда функция переходов автомата $\delta: Q \times A \to Q$ будет кодироваться булевой вектор-функцией $\bar{\delta}: \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^m$ от $n + m$ переменных по правилу $\bar{\delta}(\bar{q}, \bar{a}) = \overline{\delta(q, a)}$ (при необходимости функция $\bar{\delta}$ произвольно доопределяется на всем множестве $\{0,1\}^m \times \{0,1\}^n$). Аналогично функция выходов автомата $\lambda: Q \times A \to B$ будет кодироваться булевой вектор-функцией $\bar{\lambda}: \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^k$ от $n + m$ переменных по правилу $\bar{\lambda}(\bar{q}, \bar{a}) = \overline{\lambda(q, a)}$ (при необходимости функция $\bar{\lambda}$ произвольно доопределяется на всем множестве $\{0,1\}^m \times \{0,1\}^n$).

В результате система канонических уравнений автомата кодируется системой уравнений булевых вектор-функций:

$$\bar{b}(t) = \bar{\lambda}(\bar{q}(t-1), \bar{a}(t)), \bar{q}(t) = \bar{\delta}\big(\bar{q}(t-1), \bar{a}(t)\big), \bar{q}(0) = (0, \dots, 0).$$

В координатной форме эта система имеет вид $k + 2m$ булевых уравнений:

$$z_i(t) = \bar{\lambda}_i\big(x_1(t), \dots, x_n(t), y_1'(t), \dots, y_m'(t)\big), i = \overline{1,k},$$
$$y_j(t) = \bar{\delta}_i\big(x_1(t), \dots, x_n(t), y_1'(t), \dots, y_m'(t)\big), j = \overline{1,m},$$
$$y_j(0) = 0, j = \overline{1,m}.$$

Тогда можно построить схему из функциональных элементов в базисе $\{\wedge, \vee, '\}$ с $n + m$ входами и $k + m$ выходами, которая реализует семейство булевых функций:

$$z_i = \bar{\lambda}_i(x_1, \dots, x_n, y_1', \dots, y_m'), \quad y_j = \bar{\delta}_i(x_1, \dots, x_n, y_1', \dots, y_m'),$$
$$(i = \overline{1,k}, j = \overline{1,m}).$$

В этой схеме каждую вершину $y_j$ $(j = \overline{1,m})$ соединим дугой с соответствующей вершиной $y_j'$ и сопоставим вершине $y_j'$ элемент за-

держки. В результате получим схему из функциональных элементов и элементов задержки, функционирование которой описывается каноническими уравнениями:

$$z_i(t) = \bar{\lambda}_i\big(x_1(t), \dots, x_n(t), y_1(t-1), \dots, y_m(t-1)\big), i = \overline{1,k},$$
$$y_j(t) = \bar{\delta}_i\big(x_1(t), \dots, x_n(t), y_1(t-1), \dots, y_m(t-1)\big), j = \overline{1,m},$$
$$y_j(0) = 0, j = \overline{1,m}\,.$$

Следовательно, построенная схема из функциональных элементов и элементов задержки моделирует кодировку отображения $f_{\boldsymbol{A}}$, реализуемого автоматом ***A.***

***Теорема 2.*** Любая автоматная функция моделируется схемой из функциональных элементов в базисе из функциональных элементов конъюнкции, дизъюнкции, отрицания и элемента задержки.

## 7.5. Рекурсивные функции

С самого начала развития математики в ней рассматривались вычислительные процессы механического характера, которые для данных исходных величин позволяют находить искомые величины с помощью вполне определенных правил, называющихся алгоритмами.

Примерами алгоритмов являются известные из элементарной математики правило сложения целых чисел столбиком и правило деления целых чисел углом, а также процесс нахождения наибольшего общего делителя двух натуральных чисел, известный под названием алгоритма Евклида.

В общем случае многие важные математические проблемы сводятся к нахождению эффективной процедуры (т.е. алгоритма), с помощью которой можно определить за конечное число шагов для каждого элемента некоторого рассматриваемого множества, будет этот элемент обладать некоторым данным свойством или нет. Решением такой проблемы является построение и обоснование искомого алгоритма в виде совокупности инструкций о том, как решать рассматриваемую задачу.

Интуитивное понятие алгоритма характеризуется следующими свойствами:

1) *дискретность алгоритма* – это свойство, которое означает, что алгоритм представляет собой процесс построения величин, идущий в дискретном времени таким образом, что в начальный момент времени задается исходная конечная система величин, и в каждый следу-

ющий момент времени новая система величин получается из имевшейся в предыдущий момент времени системы величин по определенному закону с помощью последовательности дискретных предписаний (при этом входные данные алгоритма также представляют собой дискретные, конструктивные объекты);

2) *детерминированность алгоритма* – это свойство, которое означает, что в каждый момент времени система вычисляемых величин однозначно определяется системой величин, полученных в предшествующие моменты времени;

3) *элементарность шагов алгоритма* – это свойство, которое означает, что закон получения каждой последующей системы величин из предшествующей должен быть простым;

4) *направленность алгоритма* – это свойство, которое означает, что если закон получения последующей системы величин из какой-нибудь заданной системы величин не дает результата, то должно быть указано, что надо считать результатом алгоритма;

5) *массовость алгоритма* – это свойство, которое означает, что он пригоден для решения всех задач из рассматриваемого потенциально бесконечного класса задач.

Важную роль в теоретических и прикладных исследованиях играет проблема поиска алгоритма решения рассматриваемых задач. При этом рассматриваемая задача называется *алгоритмически разрешимой* или *алгоритмически неразрешимой* в зависимости от того, имеется или нет алгоритм решения этой задачи.

С целью исследования проблемы алгоритмической разрешимости разнообразных задач необходимо строго математическое определение алгоритма.

Рассмотрим общее понятие алгоритма $\boldsymbol{A}$. Ясно, что для алгоритма $\boldsymbol{A}$ имеется *множество* $D_A$ *возможных исходных данных* этого алгоритма. Например, для вышеупомянутых алгоритмов элементарной математики множеством возможных исходных данных является множество всех упорядоченных пар натуральных чисел. В результате применения алгоритма $\boldsymbol{A}$ к любому значению $x \in D_A$ возможны три исхода:

1) применение алгоритма $\boldsymbol{A}$ к значению $x$ закончится за конечное число шагов и алгоритм выдаст некоторый результат $\boldsymbol{A}(x)$;

2) применение алгоритма $\boldsymbol{A}$ к значению $x$ закончится без какого-либо результата;

3) применение алгоритма $\boldsymbol{A}$ к значению $x$ ничем не закончится, т.е. в этом случае алгоритм будет работать бесконечно.

В первом случае принято говорить, что алгоритм $\boldsymbol{A}$ применим к значению $x$, и в остальных двух случаях принято говорить, что алгоритм $\boldsymbol{A}$ не применим к значению $x$.

Множество всех значений $x \in D_{\boldsymbol{A}}$, к которым применим алгоритм $\boldsymbol{A}$, называется *областью применения алгоритма* $\boldsymbol{A}$.

Например, алгоритм сложения применим к любой упорядоченной паре натуральных чисел. Результатом применения такого алгоритма является сумма этих чисел, и, значит, область применения такого алгоритма совпадает с множеством его возможных исходных данных. С другой стороны, алгоритма Евклида применим только к упорядоченным парам ненулевых натуральных чисел. Результатом применения такого алгоритма является наибольший общий делитель этих чисел, и, значит, область применения такого алгоритма отлична от множества его возможных исходных данных.

Таким образом, для каждого алгоритма $\boldsymbol{A}$ на множестве его возможных исходных данных $D_A$ определяется частичная функция $f$ со значениями $f(x)=\boldsymbol{A}(x)$ для всех значений $x \in D_{\boldsymbol{A}}$, принадлежащих области применения алгоритма $\boldsymbol{A}$. В этом случае принято говорить, что алгоритм $\boldsymbol{A}$ *вычисляет* частичную функцию $f$.

Например, алгоритм сложения натуральных чисел вычисляет всюду определенную функцию $f: \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$, которая определяется равенством $f(x,y) = x + y$ для любых $x, y \in \boldsymbol{N}$.

Таким образом, функция называется *вычислимой*, если существует вычисляющий ее алгоритм. Например, функция $f(x,y) = x + y$ с натуральными аргументами $x,y$ вычислима.

С другой стороны, понятие вычислимой функции можно ввести на основе таких простейших численных вычислений, как фиксирование нуля, прибавление единицы и др. Такой подход к понятию алгоритма был введен в 1936 году выдающимися математиками К. Геделем, А. Черчем и С. Клини.

Пусть $\boldsymbol{N}$ – множество неотрицательных целых чисел и $\boldsymbol{F}$ – множество всех частичных функций нескольких числовых переменных из $\boldsymbol{N}$ со значениями в $\boldsymbol{N}$, т.е. отображений вида $f: X \to \boldsymbol{N}$, где $X \subset \boldsymbol{N} \times ... \times \boldsymbol{N}$ – здесь $n$ множителей.

Рассмотрим числовые функции $o: \boldsymbol{N} \to \boldsymbol{N}$, $s: \boldsymbol{N} \to \boldsymbol{N}$, $I_m^n: \boldsymbol{N^n} \to \boldsymbol{N}$ (где $1 \le m \le n$), которые называются соответственно 0-*функция*, *функция следования*, $n$-местная *функция проекции* на $m$-ю координату и определяются по формулам:

$$o(x) = 0, s(x) = x + 1, I_m^n(x_1, \dots, x_n) = x_m$$

для любых значений $x, x_1, \dots, x_n \in \boldsymbol{N}$.

Функции $o(x)$, $s(x)$, $I_m^n$ называются также *простейшими примитивно рекурсивными функциями*.

На множестве $\boldsymbol{F}$ всех частичных функций нескольких числовых переменных рассмотрим следующих два оператора:

– *оператор суперпозиции S* ставит в соответствие каждой функции $m$ переменных $f \in \boldsymbol{F}$ и $m$ функциям $n$ переменных $g_1, \dots, g_m \in \boldsymbol{F}$ функцию $n$ переменных $h = S(f, g_1, \dots, g_m)$, определяемую равенством:

$$h(x_1,\dots,x_n) = f(g_1(x_1,\dots,x_n),\dots,g_m(x_1,\dots,x_n));$$

– *оператор примитивной рекурсии R* ставит в соответствие каждой функции $n+2$ переменных $f \in \boldsymbol{F}$ и функции $n$ переменных $g \in \boldsymbol{F}$ функцию $n+1$ переменных $h = R(f, g)$, удовлетворяющую следующей *схеме примитивной рекурсии:*

$$\begin{cases} h(x_1,\dots,x_n,0) = g(x_1,\dots,x_n), \\ h(x_1,\dots,x_n,y+1) = f(x_1,\dots,x_n,y,h(x_1,\dots,x_n,y)). \end{cases}$$

В частности, при $n = 0$ схема примитивной рекурсии имеет следующий вид:

$$\begin{cases} h(0) = a, \\ h(y+1) = f(y, h(y)), \end{cases}$$

где $a$ – постоянная одноместная функция, равная числу $a$.

Схема примитивной рекурсии определяет индуктивный процесс построения функции $h$, при котором на нулевом шаге используется функция $g$ и на каждом последующем шаге – значение функции $f$ от аргументов $(x_1,\dots,x_n)$, номера $y$ предыдущего шага и значения функции $h$, вычисленного на предыдущем шаге.

**Определение.** Функция $f \in \boldsymbol{F}$ называется *примитивно рекурсивной* (сокращенно – ПРФ), если существует последовательность функций $f_1, \dots, f_n \in \boldsymbol{F}$, в которой $f_n = f$ и всякая функция $f_i$ является простей-

шей ПРФ или получается из предыдущих функций с помощью оператора суперпозиции *S* или оператора примитивной рекурсии *R*.

**Примеры.**

1. Функция *сложения* $x + y$ примитивно рекурсивна в силу схемы примитивной рекурсии:

$$\begin{cases} x + 0 = I_1^1(x), \\ x + (y + 1) = s(x + y). \end{cases}$$

2. Функция *умножения* $x \cdot y$ примитивно рекурсивна в силу схемы примитивной рекурсии:

$$\begin{cases} x \cdot 0 = o(x), \\ x \cdot (y + 1) = x \cdot y + x. \end{cases}$$

Определим на множестве $\boldsymbol{F}$ еще одно важное преобразование, с помощью которого расширяется понятие примитивно рекурсивной функции. Пусть для частичной функции $m$ переменных $g \in \boldsymbol{F}$ и набора значений $(x_1, \dots, x_m) \in \boldsymbol{N}^m$ множество решений уравнения $g(x_1, \dots, x_{m-1}, y) = x_m$ относительно переменной $y$ имеет наименьший элемент $a$, т.е. для всех неотрицательных чисел $0 \le b \le a$ значения $g(x_1, \dots, x_{m-1}, b)$ определены и удовлетворяют условиям:

$g(x_1, \dots, x_{m-1}, b) \neq x_m$ при всех $0 \le b < a$ и $g(x_1, \dots, x_{m-1}, a) = x_m$.

Обозначим такой элемент $a$ символом $\mu_y(g(x_1, \dots, x_{m-1}, y) = x_m)$. Тогда для каждой частичной функции $m$ переменных $g \in \boldsymbol{F}$ можно однозначно определить частичную функцию $m$ переменных $f \in \boldsymbol{F}$ по формуле:

$$f(x_1, \dots, x_m) = \mu_y(g(x_1, \dots, x_{m-1}, y) = x_m).$$

Это равенство означает, что для набора $(x_1, \dots, x_m) \in \boldsymbol{N}^m$ значение функции $f(x_1, \dots, x_m)$ в том и только том случае определено и равно числу $a$, если наименьшее решение $\mu_y(g(x_1, \dots, x_{m-1}, y) = x_m)$ уравнения $g(x_1, \dots, x_{m-1}, y) = x_m$ относительно переменной $y$ существует и равно числу $a$.

Так определенная для функции $g$ функция $f$ обозначается символом $f = M(g)$. Полученное преобразование $M$ элементов множества $\boldsymbol{F}$ называется *оператором минимизации.*

**Определение.** Функция $f \in \boldsymbol{F}$ называется *частично рекурсивной* (сокращенно – ЧРФ), если существует последовательность функций

$f_1, \ldots, f_n \in \boldsymbol{F}$, в которой $f_n = f$ и всякая функция $f_i$ является простейшей ПРФ или получается из предыдущих функций с помощью оператора суперпозиции *S*, оператора примитивной рекурсии *R* или оператора минимизации *M*.

Строго определенное понятие частично рекурсивной функции является математической моделью описанного выше понятия вычислимой функции.

При этом частично рекурсивная функция называется *рекурсивной* (сокращенно – РФ), если она всюду определена, и *общерекурсивной*, если в определяющей ее последовательности $f_1, \ldots, f_n \in \boldsymbol{F}$ все функции являются всюду определенными.

Множества всех рекурсивных, общерекурсивных, частично рекурсивных и примитивно рекурсивных функций из множества $\boldsymbol{F}$ обозначим соответственно $\boldsymbol{F}_{\text{РФ}}, \boldsymbol{F}_{\text{ОРФ}}, \boldsymbol{F}_{\text{ЧРФ}}$ и $\boldsymbol{F}_{\text{ПРФ}}$.

Из определений следуют включения множеств:

$$\boldsymbol{F}_{\text{ПРФ}} \subset \boldsymbol{F}_{\text{ОРФ}} \subset \boldsymbol{F}_{\text{РФ}} \subset \boldsymbol{F}_{\text{ЧРФ}}.$$

Известно, что выполняется равенство $\boldsymbol{F}_{\text{ОРФ}} = \boldsymbol{F}_{\text{РФ}}$, но все остальные включения являются собственными, т.е. $\boldsymbol{F}_{\text{ПРФ}} \neq \boldsymbol{F}_{\text{ОРФ}}, \boldsymbol{F}_{\text{РФ}} \neq \boldsymbol{F}_{\text{ЧРФ}}$.

**Определение.** Подмножество *A* множества $\boldsymbol{N}^n$ называется *рекурсивным* (или *разрешимым*), если его характеристическая функция $\chi_P$ частично рекурсивна.

**Определение.** Подмножество *A* множества $\boldsymbol{N}^n$ называется *рекурсивно перечислимым*, если *A* является множеством значений некоторой частично рекурсивной функции.

Легко видеть, что дополнения, конечные пересечения и конечные объединения рекурсивных множеств являются рекурсивными множествами. С другой стороны, конечные пересечения и конечные объединения рекурсивно перечислимых множеств являются рекурсивно перечислимыми множествами, но дополнения рекурсивно перечислимых множеств в общем случае не будут рекурсивно перечислимыми.

***Теорема об универсальной функции.*** Существует такая частично рекурсивная функция *G* из $\boldsymbol{N} \times \boldsymbol{N}$ в $\boldsymbol{N}$, что для любой частичной функции одной переменной $f \in \boldsymbol{F}_{\text{ЧРФ}}$ найдется такое $n \in \boldsymbol{N}$, что *f* совпадает с частично рекурсивной функцией $G_n(x) = G(n, x)$ из $\boldsymbol{N}$ в $\boldsymbol{N}$.

В этом случае уравнение $f(n) = G(n, n) + 1$ определяет частично рекурсивную функцию *f* из $\boldsymbol{N}$ в $\boldsymbol{N}$, которая не имеет всюду определенного рекурсивного продолжения на все множество $\boldsymbol{N}$. Пусть $g: \boldsymbol{N} \to \boldsymbol{N}$ –

всюду определенная функция, которая является продолжением функции *f*, т.е. для любых *n* из области определения функции *f* выполняется равенство: $f(n) = g(n)$. Тогда $g$ не может быть рекурсивной функцией, так как в противном случае $g = G_k$ для некоторого $k \in \boldsymbol{N}$ и определены два различных значения функций $g(k) = G_k(k) = G(k,k)$, $f(k) = G(k,k) + 1$, что противоречит равенству $f(k) = g(k)$. Это обосновывает следующий принципиально важный результат.

***Теорема.*** Существует рекурсивно перечислимое нерекурсивное множество.

Содержательно эта теорема означает, что существует алгоритм $\boldsymbol{A}$ с множеством возможных исходных данных $\boldsymbol{N}$, для которого алгоритмически неразрешима следующая задача: «определить по данному $x \in \boldsymbol{N}$, применим ли алгоритм $\boldsymbol{A}$ к значению *x*»?

В заключение отметим, что понятия рекурсивной функции и частично рекурсивной функции, а также рекурсивного множества и рекурсивно перечислимого множества естественно переносятся на словарные функции и языки над любым конечным алфавитом $A = \{a_1, \ldots, a_{p-1}\}$ с помощью биекции $\lambda$ множества $\boldsymbol{N}$ на множество всех слов $A^*$, которая определяется по правилу: $\lambda(0) = \Lambda$ и $\lambda(x) = a_{i_0} \ldots a_{i_n}$, если $x = i_0 p^n + \cdots i_{n-1}\, p + i_n$ – представление натурального числа *x* в *p*-ичной системе со значениями $1 \le i_k < p, k = \overline{0,n}$.

Такая биекция $\lambda$ естественно продолжается на множество всех частичных числовых функций *f* из множества $\boldsymbol{N}^n$ со значениями в $\boldsymbol{N}$ по правилу: $\lambda(f)$ есть частичная словарная функция из множества $(A^*)^n$ со значениями в $A^*$, которая для значений $(x_1,\ldots,x_n) \in (A^*)^n$ определяется по формуле: $\lambda(f)(x_1,\ldots,x_n) = \lambda\left(f\left(\lambda^{-1}(x_1),\ldots,\lambda^{-1}(x_n)\right)\right)$.

**Определение.** Частичная словарная функция $f : (A^*)^n \to A^*$ называется *частично рекурсивной* (соответственно, *рекурсивной* или *примитивно рекурсивной*), если частичная числовая функция $\lambda(f)$ частично рекурсивна (соответственно, рекурсивна или примитивно рекурсивна).

**Определение.** Язык $L \subset A^*$ называется *рекурсивным* (соответственно, *рекурсивно перечислимым*), если числовое множество $\lambda(L)$ рекурсивно (соответственно, рекурсивно перечислимо).

## 7.6. Машины Тьюринга

Альтернативный подход к понятию алгоритма был введен в 1936 году выдающимися математиками Э. Постом и А. Тьюрингом, которые исходили из того, что все действия любого алгоритма можно разложить на некоторые канонические элементарные шаги, выполняемые подходяще устроенными вычислительными машинами. Такие машины строго математически определяются следующим образом.

**Определение.** *Машина Тьюринга T* представляет собой систему, работающую в дискретные моменты времени $t = 0,1,2,\ldots$ и состоящую из следующих частей:

1. *Конечная лента,* разбитая на конечное число *ячеек,* которая называется *внешней памятью машины.* При этом в каждый момент времени $t$ в ячейках записаны буквы из некоторого конечного алфавита $A = \{a_0, a_1, \ldots, a_m\}$, называемого *внешним алфавитом машины.* Не нарушая общности, можно считать, что $a_0 = 0, a_1 = 1$. Ячейки, в которых записан символ 0, называются *пустыми.* В процессе работы машины: 1) ячейки ленты могут менять свои состояния путем замены записанных в них букв алфавита $A$ на его другие буквы и 2) к существующим ячейкам ленты может пристраиваться неограниченное число дополнительных ячеек, которые изначально считаются пустыми. Лента считается направленной, и ее ячейки просматриваются слева направо. Таким образом, если в какой-то момент времени лента имеет $r$ ячеек, то *состояние ленты* полностью описывается словом $w = a_{i_1} a_{i_2} \ldots a_{i_r}$, где $a_{i_1}$ – состояние первой (слева) ячейки, $a_{i_2}$ – состояние второй ячейки и т.д.

2. *Управляющая головка,* представляющая собой устройство, которое может перемещаться вдоль ленты так, что в каждый рассматриваемый момент времени $t$ оно находится напротив определенной ячейки и имеет некоторое состояние $q_i$ из конечного *множества внутренних состояний машины* $Q = \{q_0, q_1, \ldots, q_n\}$, удовлетворяющего условию $Q \cap A = \varnothing$. Состояние $q_0$ называется *заключительным* и означает завершение работы машины, а состояние $q_1$ называется *начальным* и означает начало работы машины. Если головка в состоянии $q_i$ находится напротив ячейки в состоянии $a_j$, то говорят, что машина в состоянии $q_i$ просматривает содержание ячейки $a_j$. В процессе работы машины управляющая головка: 1) может смещаться для просмотра соседних ячеек и 2) менять свои состояния путем замены записанных в ней букв алфавита $Q$ на его другие буквы.

3. *Список команд, или программа* П, представляющая собой множество выражений $T(i,j)$ (для всех $i=1,...,n$, $j=0,1,...,m$), каждое из которых имеет один из следующих видов:

– $q_i a_j \to L q_l$ – означает сдвиг управляющей головки, находящейся в состоянии $q_i$ напротив ячейки с буквой $a_j$, на одну ячейку *влево* с заменой состояния управляющей головки $q_i$ на состояние $q_l$;

– $q_i a_j \to R q_l$ – означает сдвиг управляющей головки, находящейся в состоянии $q_i$ напротив ячейки с буквой $a_j$, на одну ячейку *вправо* с заменой состояния управляющей головки $q_i$ на состояние $q_l$;

– $q_i a_j \to q_l a_k$ – означает замену буквы $a_j$ в ячейке, напротив которой находится управляющая головка в состоянии $q_i$, на букву $a_k$ с одновременной заменой состояния управляющей головки $q_i$ на состояние $q_l$.

Выражения $T(i,j)$ называются *командами.* При этом предполагается, что команды не могут начинаться со слов $q_0 a_j$, содержащих символ заключительного состояния $q_0$, и что символы $L,R$ не принадлежат множеству $A \cup Q$.

Таким образом, машина Тьюринга $T$ есть упорядоченная пятерка объектов $T = (A, Q, П, q_0, q_1)$. Работа машины $T$ происходит под действием команд из множества П и заключается в изменении ее *конфигураций,* описывающих состояния ленты и управляющей головки, а также положение управляющей головки относительно ячеек ленты. Если лента находится в состоянии, которое описывается словом $\alpha a_j \beta$ над алфавитом $A$, и управляющая головка в состоянии $q_i$ просматривает на ленте $j$-ю ячейку с состоянием $a_j$, то соответствующая конфигурация $K$ машины $T$ описывается выражением $M = \alpha q_i a_j \beta$, которое называется *машинным словом.*

По определению описывающие конфигурации $K$ машинные слова являются словами над алфавитом $A \cup Q$, содержащими единственный символ алфавита $Q$, правее которого в слове непременно есть символ алфавита $A$. При этом $K$ называется *начальной конфигурацией*, если описывающее ее машинное слово содержит символ начального состояния $q_1$, и *заключительной конфигурацией*, если описывающее ее машинное слово содержит символ заключительного состояния $q_0$.

Программа П указывает, что машина делает в каждый момент времени в зависимости от ее настоящей конфигурации *К:* если *К* – заключительная конфигурация, то машина заканчивает работу, если

же $K$ не является заключительной конфигурацией и описывается машинным словом $M = \alpha q_i a_j \beta$, то в программе П машина находит команду $T(i,j)$ с левой частью $q_i a_j$ (по определению программы в ней есть точно одна такая команда) и в зависимости от вида правой части такой команды $T(i,j)$ машина выполняет следующие действия:

– если $T(i, j) = q_i a_j \to L q_l$, то машина сдвигает управляющую головку, находящуюся в состоянии $q_i$ напротив ячейки с буквой $a_j$, на одну ячейку влево с заменой состояния управляющей головки $q_i$ на состояние $q_l$;

– если $T(i, j) = q_i a_j \to R q_l$, то машина сдвигает управляющую головку, находящуюся в состоянии $q_i$ напротив ячейки с буквой $a_j$, на одну ячейку вправо с заменой состояния управляющей головки $q_i$ на состояние $q_l$;

– если $T(i, j) = q_i a_j \to q_l a_k$, то машина заменяет букву $a_j$ в ячейке, напротив которой находится управляющая головка в состоянии $q_i$, на букву $a_k$ с одновременной заменой состояния управляющей головки $q_i$ на состояние $q_l$.

Изменение конфигураций $K_0, K_1, K_2, \ldots$ машины $T$ под действием команд из множества П происходит в дискретные моменты времени $t = 0,1,2,\ldots$ и описывается преобразованием соответствующих машинных слов $M_0, M_1, M_2, \ldots$ следующим образом. За один шаг работы машины $T$ ее машинное слово $M = \alpha q_i a_j \beta$ под действием команды $T(i,j)$ преобразуется в новое машинное слово $M'$ по правилам:

– если $T(i, j) = q_i a_j \to L q_l$ и слово $M$ имеет вид $M = q_i a_j \beta$ (т.е. $\alpha$ – пустое слово), то $M' = q_l 0 a_j \beta$;

– если $T(i, j) = q_i a_j \to L q_l$ и слово $M$ имеет вид $M = \alpha' a_k q_i a_j \beta$, то $M' = \alpha' q_l a_k a_j \beta$;

– если $T(i, j) = q_i a_j \to R q_l$ и слово $M$ имеет вид $M = \alpha q_i a_j$ (т.е. $\beta$ – пустое слово), то $M' = \alpha a_j q_l 0$;

– если $T(i, j) = q_i a_j \to R q_l$ и слово $M$ имеет вид $M = \alpha q_i a_j a_k \beta'$, то $M' = \alpha a_j q_l a_k \beta'$;

– если $T(i, j) = q_i a_j \to q_l a_k$, то $M' = \alpha q_l a_k \beta$.

Символически такое одношаговое преобразование машинных слов обозначается $M \to^T M'$.

Если существует такая последовательность преобразований машинных слов $M_i \to^T M_{i+1}$ (где $i = 0,1,\ldots,k-1$), для которой $M_0 = M$ и $M_k = M'$, то пишут $M \Rightarrow^T M'$ и говорят, что *машинное слово $M'$ получается из машинного слова $M$ с помощью машины $T$*. Если при этом во всех преобразованиях $M_i \to^T M_{i+1}$ *не достраиваются ячейки слева*, то пишут также $M \equiv\!>^T M'$.

В дальнейшем в записях $\to^T$, $\Rightarrow^T$ и $\equiv\!>^T$ символ $^T$ будет опускаться, если из контекста будет ясно, о какой машине $T$ идет речь.

Для машинного слова $M$ обозначим $M^*$ слово в редуцированном алфавите $A_1 = \{a_1,\ldots,a_m\}$, которое получается из $M$ вычеркиванием единственного вхождения буквы алфавита $Q = \{q_0, q_1,\ldots,q_n\}$ и всех вхождений пустого символа $a_0 = 0$. Будем говорить, что слово $\alpha$ алфавита $A$ *перерабатывается* машиной $T$ в слово $\beta$ редуцированного алфавита $A_1$, если существует такая последовательность преобразований машинных слов $M_i \to^T M_{i+1}$ (где $i = 0,1,\ldots,k-1$), для которой $M_0 = q_1 0\alpha$, $M_k$ – машинное слово заключительной конфигурации и $M_k^* = \beta$. В этом случае будем говорить, что машина $T$ *применима* к слову $\alpha$, и результат переработки машиной $T$ такого слова $\alpha$ будем обозначать $\beta = T(\alpha)$. Если же машина $T$ слово $M_0 = q_1 0\alpha$ не переводит в слово заключительной конфигурации, то будем говорить, что машина $T$ *неприменима* к слову $\alpha$.

**Пример.** Пусть машина Тьюринга $T$ имеет внешний алфавит $A = \{a_0, a_1\} = \{0,1\}$, внутренний алфавит $Q = \{q_0, q_1, q_2\}$ и программу П, которая состоит из команд: $q_1 0 \to Rq_2$, $q_2 0 \to q_0 1$, $q_1 1 \to Rq_1$, $q_2 1 \to Rq_2$. Тогда редуцированный алфавит имеет вид: $A_1 = \{1\}$ и слово $\alpha = 11$ машиной $T$ перерабатывается в слово $\beta = 111$, так как

$$q_1 011 \to^T 0q_2 11 \to^T 01q_2 1 \to^T 011q_2 0 \to^T 011q_0 1 \text{ и } (011q_0 1)^* = 111.$$

Легко видеть, что любое слово $\alpha = 1^n$ над редуцированным алфавитом $A_1 = \{1\}$ машиной $T$ перерабатывается в слово $\beta = \alpha 1 = 1^{n+1}$. Это означает, что машина $T$ к любому слову над алфавитом $A_1 = \{1\}$ приписывает справа символ 1.

Таким образом, любая машина Тьюринга $T$ определяет частичную функцию $f$ из $A^*$ в $A_1^*$, область определения которой $D_f$ состоит из

всех слов алфавита $A$, к которым применима машина $T$, и значения которой для слов $\alpha \in D_f$ определяются по формуле: $f(\alpha) = T(\alpha)$.

**Определение.** Частичная функция $f$ из $A_1^*$ в $A_1^*$ называется *вычислимой по Тьюрингу*, если она определяется некоторой машиной Тьюринга.

**Определение.** Частичная словарная функция $f:(A_1^*)^n \to A_1^*$ над алфавитом $A_1$ называется *вычислимой по Тьюрингу*, если существует машина Тьюринга $T$ с внешним алфавитом $A$, для которой при любых $w_1,...,w_n \in A_1^*$ условие $(w_1, w_2,...,w_n) \in D_f$ равносильно тому, что машина $T$ применима к слову $\alpha = w_1 0 w_2 0 ... 0 w_n$ и результат $T(\alpha)$ переработки машиной $T$ такого слова равен значению функции $f(w_1,...,w_n)$.

Принципиально важным фактом является то, что рассмотренные выше два подхода к понятию алгоритма оказываются эквивалентными между собой.

***Теорема.*** Частичная словарная функция в том и только том случае будет вычислимой по Тьюрингу, если она частично рекурсивна.

Более того, на основе анализа идей теории рекурсивных функций А. Черч и С. Клини выдвинули гипотезу, известную под названием *тезис Черча*: класс алгоритмических задач, решаемых на основе понятия рекурсивной функции (а, значит, и на основе любой из равносильных ему формальных моделей алгоритма), совпадает с классом задач, которые могут быть решены интуитивно эффективными вычислениями, т.е. интуитивными алгоритмическими методами.

Тезис Черча не является математическим утверждением и его невозможно доказать или опровергнуть, так как в его формулировку входит нестрогое интуитивное понятие алгоритма. Однако тезис Черча важен для приложений математики, поскольку с помощью его точными математическими средствами обосновывается алгоритмическая неразрешимость исследуемых математических задач.

## 7.7. Формальные грамматики

**Определение.** *Грамматикой* называется алгебраическая система $\Gamma = (A, G, \pi)$, состоящая из непустых конечных множеств $A, G$ и конечного бинарного отношения $\pi$ между словами из множества $G^+$ и словами из множества $(A \cup G)^*$. Множество $A$ называется *алфавитом* грамматики и множество $V = A \cup G$ – *полным словарем* грамматики.

Элементы множества $G$ не принадлежат алфавиту $A$ и называются *грамматическими* (или *металингвистическими*) *символами* грамматики. Элементы $(u,v)\in\pi$ отношения $\pi$ называются *правилами* грамматики и символически обозначаются $u\to v$ . В этом случае говорят, что слово $v$ получается из слова $u$ по правилу $\pi$.

Правила грамматики позволяют так преобразовать слова ее полного словаря, что из любого фиксированного грамматического символа $g_0\in G$ образуется некоторое множество слов $L(\Gamma, g_0)$ над алфавитом $A$.

**Определение.** Пусть $y, z \in V^*$ – слова над полным словарем $V$ грамматики $\Gamma$. Будем говорить, что:

– слово $z$ *непосредственно выводится* из слова $y$ и писать $y \Rightarrow z$, если слово $z$ можно получить из слова $y$ заменой некоторого его подслова $u$ на слово $w$ по некоторому правилу грамматики $u\to w$, т.е. если найдутся такие слова $u\in G^+$ и $u_1, u_2, w \in V^*$, что $y = u_1 u\, u_2$, $z = u_1 w\, u_2$ и $u\to w$ ;

– слово $z$ *выводится* из слова $y$ и писать $y \Rightarrow^t z$ ,если слово $z$ можно получить из слова $y$ конечным числом замен некоторых подслов по некоторым правилам грамматики, т.е. если найдется такая последовательность слов $w_1, \ldots, w_n \in V^*$, что $y = w_1, z = w_n$ и $w_i \Rightarrow w_{i+1}$ для всех $i = \overline{1, n-1}$.

**Определение**. Для произвольно фиксированного грамматического символа $g_0\in G$ множество всех слов над алфавитом $A$, которые выводятся из $g_0$, обозначается $L(\Gamma, g_0)$ и называется *языком, порождаемым* грамматикой $\Gamma$ и *начальным символом* $g_0\in G$.

Таким образом, по определению $L(\Gamma, g_0) = \{w \in A^* : g_0 \Rightarrow^t w\}$.

**Пример.** Пусть грамматика $\Gamma = (A, G, \pi)$ имеет однобуквенный алфавит $A=\{a\}$, один грамматический символ $g_0\in G$, $g_0\neq a$ и два правила: $g_0\to a$, $g_0\to a g_0$. В этом случае для слова $z\in V^*$ из условия $g_0 \Rightarrow z$ следует, что $z=a$ или $z=a g_0$. Если теперь для слов $w_1, w_2, \ldots, w_n \in V^*$ выполняется условие $g_0 = w_1 \Rightarrow w_2 \Rightarrow \ldots \Rightarrow w_n = z$, то либо $w_2 = a$, либо $w_2 = a g_0$. Так как соотношение $a \Rightarrow w$ не выполняется ни при каком $w\in V^*$, то либо в первом случае $z = w_2 = a$, либо во втором случае $w_3 = aa$ или $w_3 = a a g_0$. Тогда либо $z = w_3 = aa$, либо $w_3 = a a g_0$ и, значит, $w_4 = aaa$ или $w_4 = aaa g_0$. Схематически этот процесс можно изобразить в виде следующей диаграммы:


Так как язык $L(\Gamma, g_0)$ состоит только из слов над алфавитом $A$, то, отбрасывая на диаграмме элементы, не принадлежащие множеству $A^*$, получаем:

$$L(\Gamma, g_0) = \{a, aa, aaa, aaaa, \ldots\} = A^+.$$

В естественных языках алфавит грамматики Г состоит из слов языка (например, всех слов некоторого толкового словаря со всеми их склонениями и т. д.), грамматическими символами грамматики Г являются имена для грамматических терминов (таких, как «предложение», «существительное», «наречие», ...), правило грамматики состоит из правил вида «предложение» → «подлежащее» «сказуемое» и подстановочных правил, например, вида «подлежащее» → «стол». Таким путем в языках можно получать грамматически правильные предложения, которые, однако, не обязаны быть осмысленными с точки зрения содержания.

В качестве еще одного применения грамматик рассмотрим общепринятый подход к языкам программирования на примере построения известного языка ALGOL 60. Алфавит $A$ такого языка состоит из букв, цифр, алгебраических символов и специальных зарезервированных слов, его грамматическими символами являются некоторые подмножества множества $A$* и, наконец, имеются определенные грамматические правила, по которым строятся программы этого языка. Это означает, что рассматривается грамматика $\Gamma = (A, G, \pi)$ с алфавитом:

$A$={$A,B,\ldots,Z,a,b,\ldots,z$,0,1,…,9,+,–,*,/,÷,↑,=,≠,<,≤,>,≥,∧,∨,≡,;,·,:,(,),[,],
BEGIN, TRUE, FALSE, GOTO, FOR, STEP, UNTIL, END}

и множеством грамматических символов $G$, состоящим из множеств $I,U,R,B,D,L,\ldots$ подмножеств множества $A^*$, которые обозначаются символами <идентификатор>, <целое без знака>, <вещественное>, <булево>, <цифра>, <буква>,… и неявно определяются последовательностью уравнений вида:

$$I = L \cup IL \cup ID,\ U = D \cup UD \text{ и т.д.},$$

где $IL,ID,UD$ – произведения подмножеств в полугруппе слов $A^*$. Эти уравнения определяются соответствующими правилами языка

ALGOL, которые следующим образом записываются в форме Бэкуса – Наура:

<идентификатор> ::= <буква> | <идентификатор><буква> |
<идентификатор><цифра>,
<число без знака> ::= <цифра>|<число без знака><цифра>, …

Пусть $g_0$ – произвольный начальный символ, удовлетворяющий условию $g_0 \notin A$ и $\pi$ – множество правил грамматики вида: $g_0 \to I$, $g_0 \to g_0 D$, $g_0 \to g_0 7$ и т. п. Языки, порождаемые такими грамматиками с произвольным конечным алфавитом $A$ и определяемым уравнениями множеством грамматических символов $G \subset A^*$, называются *языками типа* ALGOL.

**Определение.** Язык $L \subset A^+$ называется языком, *порожденным грамматикой* (или *языком типа* 0), если $L = L(\Gamma, g_0)$ для некоторой грамматики $\Gamma$ с начальным символом $g_0$.

Класс таких языков очень обширен и совпадает с классом рекурсивно перечислимых множеств.

***Теорема 1.*** Язык $L \subset A^+$ в том и только том случае порождается некоторой грамматикой, если он является рекурсивно перечислимым языком (см. раздел 7.5).

**Определение.** Грамматика $\Gamma = (A, G, \pi)$ называется:

– *контекстно-зависимой* (или *типа* 1), если любое ее правило имеет вид $ugv \to uxv$ для некоторого грамматического символа $g \in G$ и некоторых слов $u, v \in G^*$, $x \in V^+$;

– *контекстно-свободной* (или *типа* 2), если любое ее правило имеет вид $g \to x$ для некоторого грамматического символа $g \in G$ и некоторого слова $x \in V^+$;

– *праволинейной* (или *рациональной*, или *типа* 3), если любое ее правило имеет вид $g \to xf$ или $g \to y$ для некоторых грамматических символов $g, f \in G$ и некоторых слов $x, y \in A^*$.

Так, в приведенном выше примере грамматика является контекстно-свободной.

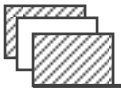
Для каждого типа $0 \le i \le 3$ обозначим $K_i$ класс всех языков, порожденных грамматиками типа $i$. Известно, что $K_3 \subset K_2 \subset K_1 \subset K_0$, причем все эти включения строгие. Класс языков $K_0$ описан в теореме 1. Остальные классы языков $K_i$ для значений $1 \le i \le 3$ описываются в следующих теоремах.

***Теорема 2.*** *Я*зык $L \subset A^+$ в том и только том случае порождается некоторой контекстно-зависимой грамматикой, если он является рекурсивным языком (см. раздел 7.5).

***Теорема 3.*** *Я*зык $L \subset A^+$ в том и только том случае порождается некоторой контекстно-свободной грамматикой, если он является языком типа языка программирования ALGOL.

***Теорема 4.*** *Я*зык $L \subset A^+$ в том и только том случае порождается некоторой праволинейной грамматикой, если он является рациональным языком.

Таким образом, формальная грамматика, с одной стороны, является адекватной моделью алгоритма и, с другой стороны, дает инструмент эффективного построения иерархии вычислимых множеств.



### *Контрольные вопросы для среза знаний*

1) Переключательная схема и ее функция проводимости.
2) Реализация булевых функций переключательными схемами.
3) Схемы из функциональных элементов.
4) Теорема полноты для схем из функциональных элементов.
5) Операции над формальными языками и понятие рационального языка.
6) Определение и формы задания конечных автоматов, распознающих формальные языки.
7) Теорема Клини о распознаваемых автоматами языках.
8) Определение и формы задания автоматов Мили.
9) Определения детерминированной и ограниченно детерминированной функций. Определение и критерий автоматной функции.
10) Теорема о моделировании автоматных функций схемами из функциональных элементов.
11) Определения и свойства рекурсивных, общерекурсивных, частично рекурсивных и примитивно рекурсивных функций.
12) Определения и свойства рекурсивных и рекурсивно перечислимых множеств.
13) Теорема об универсальной функции.
14) Определение машины Тьюринга и вычислимой ею функции.
15) Определение грамматики и порождаемого ею языка.
16) Классификация грамматик и порождаемых ими языков.

# Библиографический список

## Основная литература

1. *Андерсон Дж.А.* Дискретная математика и комбинаторика. М.; СПб.; Киев: Вильямс, 2003.

2. *Игошин В.И.* Математическая логика и теория алгоритмов. М.: Академия, 2004.

3. *Молчанов В.А.* Математическая логика: учеб. пособие. Саратов: Изд-во СГСЭУ, 2011.

4. *Судоплатов С.В., Овчинникова Е.В.* Дискретная математика. М.: ИНФРА-М; Новосибирск: Изд-во НГТУ, 2005.

5. *Яблонский С.В.* Введение в дискретную математику. М.: Высшая школа, 2006.

## Дополнительная литература

1. *Булос Дж., Джеффри Р.* Вычислимость и логика. М.: Мир, 1994.

2. *Ершов Ю.Л., Палютин Е.А.* Математическая логика. М.: Лань, 2005.

3. *Кострикин А.И.* Введение в алгебру: в 3 ч. М.: МЦНМО, 2009.

4. *Уилсон Р.* Введение в теорию графов. М.: Мир, 1977.

## Сборники задач

1. *Игошин В.И.* Сборник задач по математической логике и теории алгоритмов. М.: Академия, 2005.

2. *Лавров И.А., Максимова Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов. М.: ФИЗМАТЛИТ, 2004.

3. Сборник задач по алгебре / под ред. А.И. Кострикина. М.: МЦНМО, 2009.

СОДЕРЖАНИЕ

*Учебное издание*

Автор-составитель
**Молчанов Владимир Александрович**

# ДИСКРЕТНАЯ МАТЕМАТИКА

*Рекомендовано*
*Учебно-методическим объединением в области экономики*
*и менеджмента, логистики и бизнес-информатики*
*в качестве учебного пособия*
*для студентов бакалавриата высших учебных заведений,*
*обучающихся по направлению подготовки 080500.62*
*«Бизнес-информатика»*

Редактор *Л.В. Реброва*
Компьютерная верстка *Е.Н. Доронкиной*

Темплан 2013 г.

Подписано в печать 16.09.2013. Формат 60×84 1/16.
Бумага типогр. № 1. Печать RISO.
Уч.-изд. л. 7,37. Усл. печ. л. 8,25.
Тираж 300. Заказ 360.

410003, г. Саратов, ул. Радищева, 89. СГСЭУ.