

# Дискретная математика

## 1 Множества

### 1.1 Понятие множества. Множества и подмножества. Способы задания множества

Георг Кантор, основатель теории множеств, определял *множество* как «многое, мыслимое как единое целое». Можно дать и более строгую формулировку:

**Определение 1.1.1.** *Множество* — это математический объект, являющийся совокупностью объектов произвольной природы, которые называются *элементами* этого множества и обладают общим для них характеристическим свойством.

**Определение 1.1.2.** Множество  $S$  называется подмножеством множества  $M$ , если  $\forall s \in S \ s \in M$ .

Существует несколько способов задания множества. Во-первых, можно задать множество просто перечислив все его элементы:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Также можно задать множество с помощью так называемого *характеристического предиката*:

$$S = \{x : x \in \mathbb{Z} \wedge x > 30\}.$$

Другим вариантом будет задание порождающей процедуры, например, для генерирования множества чисел последовательности Фибоначчи:

$$F = \{a : a_1 = 0, a_2 = 0, a_i = a_{i-2} + a_{i-1}, \text{ где } i = 3, 4, \dots\}.$$

### 1.2 Конечные и бесконечные множества. Сравнимые множества. Мощность множества. Булеан

**Определение 1.2.1.** Множество называется *конечным*, если оно содержит конечное количество элементов. Пустое множество также считается конечным.

Соответственно, множество, которое содержит бесконечное количество элементов называется бесконечным. Например, множество натуральных чисел  $\mathbb{N}$  является бесконечным.

Бесконечные множества делятся еще на два вида: счетные и несчетные. Счетные множества — это те, элементы которых мы можем пронумеровать: первый, второй, третий, ... Очевидно, что множество натуральных чисел является счетным. А что насчет множества действительных чисел? Можем ли мы пронумеровать все его элементы? Очевидно, нет. Поэтому множество действительных чисел является несчетным. А все множества с такой же мощностью как у множества действительных чисел называются континуальными.

Говоря формально, множество является счетным, если его можно взаимно-однозначно сопоставить со множеством натуральных чисел.

**Определение 1.2.2.** Два множества  $A$  и  $B$  называют сравнимыми, если  $A \subset B$  или  $B \subset A$ .

Другими словами, два множества называются сравнимыми, если одно из них является подмножеством другого.

**Определение 1.2.3.** *Мощностью* множества или его *кардинальным числом* называют количество элементов, которые содержатся в этом множестве. Мощность множества  $A$  обозначается через  $\text{card}(A)$ ,  $\#A$  или  $|A|$ .

Рассмотрим множество  $\{1, 2, 3\}$ . В нем три элемента, значит его мощность равна 3. А какова мощность множества натуральных чисел? Мощность множества натуральных чисел обозначается как  $\aleph_0$  (читается «алеф-ноль»). Мощность множества действительных чисел обозначается как  $\mathfrak{c}$ . Предположение о том, что  $\mathfrak{c} = \aleph_0$  называется *континуум-гипотезой*.

**Определение 1.2.4.** Булеаном  $2^A$  называют множество всех подмножеств данного множества  $A$ .

**Пример.** Например, булеаном множества  $\{1, 2\}$  будет являться множество  $\{\{1, 2\}, \{1\}, \{2\}, \emptyset\}$ .

Очевидно, что количество элементов в булеане множества всегда больше количества элементов самого множества. Можно вывести и более общую формулу, выражающую зависимость между мощностью конечного множества и мощностью его булеана:

$$\text{card}(2^A) = 2^{\text{card}(A)}.$$

## 1.3 Парадоксы теории множеств

### 1.3.1 Парадокс Рассела

Одним из парадоксов наивной теории множеств является парадокс Рассела. Будем называть множество «обычным», если оно не содержит себя в

качестве своего элемента. И «необычным», если содержит. Допустим, у нас есть множество  $S$ , содержащее абсолютно все «обычные» множества. Парадокс возникает, когда мы пытаемся понять, каким является множество  $S$  — обычным или необычным.

С одной стороны, если оно «обычное», то оно должно включать себя в качестве своего элемента, поскольку состоит из всех «обычных» множеств. Но тогда оно не будет является «обычным», т. к. включает содержит само себя в качестве своего элемента.

С другой стороны, если оно «необычное», то должно включать само себя в качестве своего элемента, т. к. это свойство всех «необычных» множеств. Однако оно не может включать себя в качестве своего элемента, т. к. состоит только из «обычных» множеств.

### 1.3.2 Парадокс Кантора

Пусть существует множество всех множеств  $S$ . Тогда, по-определению, оно должно содержать свой булеан, т. е.  $2^S \subset S$ . Очевидно, что если  $A \subset B$ , то  $\text{card}(A) < \text{card}(B)$ , но мощность булеана всегда больше мощности исходного множества. Получили противоречие.

## 2 Отношения

### 2.1 Отношение. Бинарное отношение. Обратное отношение. Композиция бинарных отношений. Тожественное отношение. Универсальное отношение

**Определение 2.1.1.** Множество  $\varphi$  называют  $n$ -арным отношением между элементами множеств  $A_1, A_2, \dots, A_n$ , если оно является подмножеством их декартова произведения  $A_1 \times A_2 \times \dots \times A_n$ .

**Определение 2.1.2.** Бинарным отношением  $\varphi$  между элементами множеств  $A$  и  $B$  называют любое подмножество их декартова произведения. Другими словами,  $\varphi \subseteq A \times B$ .

**Определение 2.1.3.** Пусть дано бинарное отношение  $\varphi \subseteq A \times B$ . Тогда обратным бинарным отношением будет называться отношение  $\varphi^{-1}$  такое, что

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

**Определение 2.1.4.** Пусть дано два бинарных отношения  $\rho \subseteq A \times B$  и  $\phi \subseteq B \times C$ . Тогда их композицией  $\rho \circ \phi$  будет называться бинарное отношение  $\mu \subseteq A \times C$ :

$$\mu = \rho \circ \phi = \{(a, c) : (\exists b \in B) [(a, b) \in \rho \text{ and } (b, c) \in \phi]\}.$$

**Определение 2.1.5.** Бинарное отношение  $\varphi \subseteq A^2 = \{(a, a) : a \in A\}$  называется *тождественным* и обозначается как  $\text{id}_A$ .

**Определение 2.1.6.** Отношение  $\varphi \subseteq A \times B = \{(a, b) : a \in A, b \in B\}$  называется *универсальным*.

## 2.2 Степень отношения. Ядро отношения

**Определение 2.2.1.** Степенью  $\rho^n$  бинарного отношения  $\rho$  называют композицию этого отношения с самим собой  $n$  раз:

$$\rho \underbrace{\circ \dots \circ}_{n \text{ раз}} \rho.$$

**Определение 2.2.2.** Ядром отношения  $\rho$  называется композиция отношения и обратного ему:  $\rho \circ \rho^{-1}$ .

## 2.3 Отношения эквивалентности. Теорема об отношении эквивалентности и разбиении множества. Классы эквивалентности. Фактор-множество

**Определение 2.3.1.** Бинарное отношение называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

**Определение 2.3.2.** Разбиением множества  $A$  называется множество его подмножеств такое, что

$$\bigcup_{i \in I} A_i = A \wedge [\forall i, j : i \neq j](A_i \cap A_j = \emptyset).$$

**Теорема.** Всякое отношение эквивалентности множества  $A$  определяет разбиение множества  $A$ , причем среди элементов разбиения нет пустых. Верно и обратное: всякое разбиение множества  $A$ , не содержащее пустых элементов, определяет отношение эквивалентности на множестве  $A$ .

**Определение 2.3.3.** Пусть  $\equiv$  является отношением эквивалентности на множестве  $A$  и  $x \in A$ . Тогда *классом эквивалентности* для  $x$  называют подмножество элементов из  $A$ , эквивалентных  $x$ :

$$[x]_{\equiv} = \{y : y \in A \wedge y \equiv x\}.$$

**Определение 2.3.4.** Пусть  $\sim$  — отношение эквивалентности на множестве  $A$ . Тогда *фактор-множеством* называют множество всех классов эквивалентности множества  $A$  по отношению  $\sim$  и обозначают как  $A/\sim$ .

## 2.4 Замыкание бинарных отношений. Теорема о транзитивном замыкании

Замкнутость множества относительно применения какой-либо операции означает, что многократное применение операции к элементам этого множества не выводит образующиеся в результате применения операции элементы за пределы исходного множества.

Например, множество натуральных чисел  $\mathbb{N}$  замкнуто относительно операции сложения, потому что при сложении любых двух натуральных чисел получается натуральное число. Однако  $\mathbb{N}$  не является замкнутым относительно операции деления, т. к. при делении двух натуральных чисел может получиться число, не являющееся натуральным.

**Определение 2.4.1.**  $R^+ = \bigcup_{i=1}^{\infty} R^i$ .

**Определение 2.4.2.** Транзитивное замыкание отношения  $R$  на множестве  $M$  есть наименьшее транзитивное отношение на множестве  $M$ , включающее  $R$ .

**Пример.** Например, если элементами множества  $M$  являются люди, а отношение  $R \subset M^2$  — это отношение «является родителем», то транзитивным замыканием отношения  $R$  будет являться отношение «является предком».

**Теорема.**  $R^+$  есть транзитивное замыкание  $R$ .

## 2.5 Функции. Инъекция, сюръекция, биекция. Теорема о тотальной биекции

**Определение 2.5.1.** Функцией называют бинарное отношение, которое обладает свойством однозначности:

$$(a, b) \in f \wedge (a, c) \in f \rightarrow b = c.$$

Бинарное отношение  $f \subseteq X \times Y$ , обладающее свойством однозначности называется *функциональным* и записывается как  $f: X \rightarrow Y$ .

**Определение 2.5.2.** Функция называется *инъективной*, если у каждого значения функции есть только один прообраз:

$$y = f(x_1) \text{ and } y = f(x_2) \rightarrow x_1 = x_2.$$

**Определение 2.5.3.** Функция  $f: X \rightarrow Y$  является *сюръективной*, если областью ее значений является все множество  $Y$ , т. е. если она принимает все возможные значения:

$$\forall y \in Y \exists x \in X: (x, y) \in f.$$

**Определение 2.5.4.** Функция называется *биективной*, если она сюръективна и инъективна одновременно.

Биективная функция также называется взаимно-однозначным соответствием.

## 2.6 Ядро функции. Теорем о ядре функции

**Определение 2.6.1.** Ядром функции  $f$  называют  $\ker f = f \circ f^{-1}$ .

**Теорема.** Ядро функции  $f: A \rightarrow B$  задает отношение эквивалентности на  $A$ .

## 3 Алгебраические структуры

### 3.1 Операции и их свойства. Алгебраическая структура. Модель. Примеры алгебраических структур

**Определение 3.1.1.**  $n$ -арной (или  $n$ -местной) операцией на  $M$  называют всюду определенную на множестве  $M$  тотальную функцию от  $n$  аргументов.

Если  $\varphi$  — бинарная операция, т. е.  $\varphi: M^2 \rightarrow M$ , то её обозначают как  $\varphi(a, b)$ , где  $a, b \in M$ . Иногда используют инфиксную форму записи  $a \circ b$ , где  $\circ$  — знак операции.

**Определение 3.1.2.** Множество с набором определенных на нем операций  $\mathcal{A} = \langle M; \varphi_1, \dots, \varphi_m \rangle$ , где  $\varphi_i: M^{n_i} \rightarrow M$  называется *алгебраической структурой*.

**Определение 3.1.3.** Алгебраическая структура с пустым множеством операций называется *моделью*.

**Пример.** Одним из простейших примеров алгебраической структуры является множество целых чисел с операциями сложения и вычитания:  $\langle \mathbb{A}; +, - \rangle$ .

### 3.2 Булева алгебра. Примеры булевых алгебр. Теорема Стоуна

**Определение 3.2.1.** Булевой алгеброй называют алгебраическую систему  $\langle M; \wedge, \vee, \neg, 0, 1 \rangle$ , причем для любых  $a, b, c \in M$  верны следующие аксиомы:

- i.  $a \wedge (b \vee c) = (a \wedge b) \vee c$  и  $a \vee (b \wedge c) = (a \vee b) \wedge c$  (ассоциативность);
- ii.  $a \wedge b = b \wedge a$  и  $a \vee b = b \vee a$  (коммутативность);
- iii.  $a \wedge (a \vee c) = a$  и  $a \vee (a \wedge b) = a$  (законы поглощения);
- iv.  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$  и  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$  (дистрибутивность);

v.  $a \wedge \neg a = 0$  и  $a \vee \neg a = 1$  (дополнительность).

**Пример.** В качестве примера булевой алгебры можно привести множество всех подмножеств данного множества  $M$ , которое образует булеву алгебру относительно операций объединения, пересечения и унарной операции дополнения.

**Теорема (Стоуна).** Всякую булеву алгебру можно интерпретировать как булеву алгебру подмножеств некоторого множества.

Другими словами, какой бы ни была булева алгебра мы можем считать её элементы подмножествами некоторого множества, а операции, соответственно, — теоретико-множественными операциями.

### 3.3 Подалгебра. Теорема о непустом пересечении подалгебры

**Определение 3.3.1.** Если в алгебре  $\langle M; \Sigma \rangle$  мы рассмотрим  $X \subset M$  такое, что  $X$  замкнуто относительно всех операций из  $\Sigma$ , то система  $\langle X; \Sigma_X \rangle$  образует подалгебру алгебры  $\langle M; \Sigma \rangle$ , где  $\Sigma_X$  состоит из сужений операций из  $\Sigma$  на  $X$ .

**Теорема** (о не пустом пересечении подалгебр). Непустое пересечение подалгебр одной алгебры образует подалгебру той же алгебры.

### 3.4 Полугруппа. Примеры. Свободная полугруппа

**Определение 3.4.1.** Полугруппой называют алгебраическую структуру с одной бинарной ассоциативной операций.

**Пример.** Например, алгебраическая система  $\langle A^+; \cdot \rangle$ , где  $A^+$  — множество слов в алфавите, а  $\cdot$  — операция конкатенации строк, является полугруппой.

**Определение 3.4.2.** Если в полугруппе все различные слова, состоящие из образующих определяют различные элементы носителя, то полугруппа называется свободной.

**Пример.** Например, системой образующих полугруппы  $\langle \mathbb{N}; + \rangle$  является множество  $\{1\}$ . Так как различные слова в алфавите  $\{1\}$  — суть различные элементы носителя, то  $\langle \mathbb{N}; + \rangle$  является полугруппой.

### 3.5 Моноид. Примеры. Теорема о единственности единицы в моноиде

**Определение 3.5.1.** Моноидом называют полугруппу  $\langle M; \circ, e \rangle$ , в которой существует нейтральный элемент (также называемый единицей)  $e$  такой, что  $\forall t \in M \quad t \circ e = e \circ t = t$ .

**Пример.** Простейшими примерами моноидов являются  $\langle \mathbb{N}; +, 0 \rangle$  и  $\langle \mathbb{R}; \cdot, 1 \rangle$ .

**Теорема.** Единица в моноиде единственна.

*Доказательство.* Пойдем от противного и предположим, что существует два нейтральных элемента  $e_1$  и  $e_2$ . Тогда  $e_1 = e_1 \circ e_2 = e_2 \circ e_1 = e_2$ .  $\square$

### 3.6 Группа. Примеры. Теорема о единственности обратного элемента в группе

**Определение 3.6.1.** Группой называют моноид, в котором для каждого элемента существует элемент, обратный ему.

**Пример.** Примером группы является  $\langle \mathbb{Z}; + \rangle$ , где для каждого целого числа существует обратное ему число с противоположным знаком.

**Теорема.** Обратный элемент в группе единственен.

*Доказательство.* Пойдем от противного и предположим, что в группе  $\langle M; \circ \rangle$  для данного  $t \in M$  существует два обратных элемента  $a$  и  $b$ . Тогда  $a = a \circ e = a \circ (t \circ b) = (a \circ t) \circ b = e \circ b = b$ .  $\square$

### 3.7 Теорема о свойствах операций в группе

**Теорема.** В группе выполняются следующие соотношения:

1.  $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ ;
2.  $a \circ b = a \circ c \Rightarrow b = c$ ;
3.  $b \circ a = c \circ a \Rightarrow b = c$ ;
4.  $(a^{-1})^{-1} = a$ .

*Доказательство.* Каждое соотношение легко доказывается с помощью простых логических выводов:

1.  $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \Rightarrow (a \circ b) \circ b^{-1} \circ a^{-1} = e \Rightarrow a \circ (b \circ b^{-1}) \circ a^{-1} = e \Rightarrow a \circ e \circ a^{-1} = e \Rightarrow a \circ a^{-1} = e \Rightarrow e = e$ ;
2.  $a \circ b = a \circ c \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) \Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \Rightarrow e \circ b = e \circ c \Rightarrow b = c$ ;
3. (доказывается по аналогии с предыдущим соотношением);
4. (прямо следует из факта единственности обратного элемента в группе).

$\square$



### 3.8 Теорема об однозначности решения в группе уравнения $a \times x = b$

**Теорема.** В группе можно однозначно решить уравнение  $a \times x = b$ .

*Доказательство.*  $a \times x = b \Rightarrow a^{-1} \times (a \times x) = a^{-1} \times b \Rightarrow (a^{-1} \times a) \times x = a^{-1} \times b \Rightarrow e \times x = a^{-1} \times b \Rightarrow x = a^{-1} \times b.$   $\square$

### 3.9 Коммутативная группа. Примеры

**Определение 3.9.1.** Коммутативной (или абелевой) группой называют группу, в которой бинарная операция коммутативна.

**Пример.** Например, группа  $\langle \mathbb{Z}; + \rangle$  является абелевой группой, так как операция  $+$  обладает свойством коммутативности.

### 3.10 Кольцо. Примеры. Теорема о соотношениях в кольце

**Определение 3.10.1.** Кольцом называют алгебраическую систему  $\langle M; +, \times \rangle$ , являющуюся абелевой группой по сложению, полугруппой по умножению, и обладающая двухсторонней дистрибутивностью умножения относительно сложения.

**Пример.** Простейшим примером кольца является множество целых чисел с обычными операциями сложения и умножения.

**Теорема.** В кольце выполняются следующие соотношения:

1.  $0 \cdot a = a \cdot 0 = 0$ ;
2.  $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ ;
3.  $(-a) \cdot (-b) = a \cdot b$ .

*Доказательство.* Все соотношения доказываются простыми логическими цепочками:

1.  $a \cdot 0 = a \cdot (x - x) = ax - ax = 0$ , а также  $0 \cdot a = (x - x) \cdot a = xa - xa = 0$ ;
2.  $ab + (-a)b = [a + (-a)]b = 0 \cdot b = 0$ , а также  $ab + a(-b) = a[b + (-b)] = a \cdot 0 = 0$ ;
3.  $(-a)(-b) = -[a(-b)] = -(-ab) = ab.$

$\square$

## 4 Булевы функции

### 4.1 Булевы функции. Элементарные булевы функции. Способы задания булевых функций

**Определение 4.1.1.** Отображение  $B^n \rightarrow B$ , где  $B = \{0, 1\}$  называется *булевой функцией от  $n$ -переменных*.

При  $n$  равным нулю количество булевых функций сводится к двум. Первая из них тождественно равна 0, а вторая — 1. Их называют *булевыми константами* — тождественный ноль и тождественная единица.

Всякая булева функция задается конечным набором значений, что позволяет представить ее в виде, например, *таблицы истинности*.

Множество всех булевых функций обозначается как  $P_2$ , а множество всех булевых функций от  $n$  переменных как  $P_2(n)$ .

### 4.2 Существенная и несущественная переменные. Теорема о числе булевых функций, зависящих от $n$ переменных

**Определение 4.2.1.** Есть для любых двух булевых векторов, отличающихся лишь в значении этой переменной, значение функции на них совпадает, то такая переменная называется *несущественной* или *фиктивной*.

Другими словами, переменная является фиктивной, если значение функции не зависит от значения этой переменной.

**Теорема.** Число булевых функций, зависящих от  $n$  переменных равно  $2^{2^n}$ .

*Доказательство.* Количество булевых векторов длины  $n$  равно  $2^n$ . Поскольку на каждом из булевых векторов функция может принимать значение либо 0, либо 1, то количество всех булевых функций от  $n$  переменных равно  $2^{2^n}$ .  $\square$

### 4.3 Формулы. Интерпретация формул. Равносильные формулы. Правила эквивалентных преобразований формул

**Определение 4.3.1.** Пусть даны две функции  $f(x_1, \dots, x_n)$  и  $g(y_1, \dots, y_m)$  тогда *подстановкой* функции  $g$  в функцию  $f$  называется замена  $i$ -того аргумента функции  $f$  значением функции  $g$ :

$$h(x_1, \dots, x_{n+m-1}) = f(x_1, \dots, x_{i-1}, g(x_i, \dots, x_{i+m-1}), x_{i+m}, \dots, x_{n+m-1}),$$

а сама функция  $h$  называется *суперпозицией* функций  $f$  и  $g$ .

**Определение 4.3.2.** Пусть  $\Sigma \subset P_2$ .

1. Каждая функция  $\varphi(x_1, \dots, x_n) \in \Sigma$  является *формулой* над  $\Sigma$ .
2. Рассмотрим функцию  $\varphi(x_1, \dots, x_n)$  и выражения  $A_1, \dots, A_n$ , где  $A_i$  — выражение, являющееся либо формулой над  $\Sigma$ , либо символом переменной из множества  $U$ . Тогда выражение  $\varphi(A_1, \dots, A_n)$  называется *формулой* над  $\Sigma$ .

Сопоставим теперь каждой формуле над  $\Sigma$  функцию из  $P_2$ :

1. Если  $F = f(x_1, \dots, x_n)$ , где  $F$  есть формула над  $\Sigma$ , то формуле  $F$  сопоставим функцию  $f(x_1, \dots, x_n)$ .
2. Пусть  $F = f(A_1, \dots, A_n)$ , где  $A_i$  — это выражение, представляющее либо формулу над  $\Sigma$ , либо символ переменной из множества  $U$ . Тогда согласно предположению индукции каждому выражению  $A_i$  сопоставлена либо функция  $f_i \in P_2$ , либо тождественная функция  $f_i = x_s$ . Тогда формуле  $F = f(A_1, \dots, A_n)$  соответствует функция  $f(f_1, \dots, f_n)$ .

**Определение 4.3.3.** Две формулы называются *равносильными* (эквивалентными), если им соответствуют равные функции.

#### 4.4 Алгебра булевых функций. Теорема об алгебре булевых функций

**Определение 4.4.1.** Алгебра  $\langle P_2; \wedge, \vee, \neg \rangle$  называется *алгеброй булевых функций*.

#### 4.5 Функция двойственная к данной. Теорема о принципе двойственности

**Определение 4.5.1.** Функция  $g(x_1, \dots, x_n)$  является *двойственной* функции  $f(x_1, \dots, x_n)$ , если

$$f(\overline{x_1}, \dots, \overline{x_n}) = \overline{g(x_1, \dots, x_n)}.$$

**Теорема** (о принципе двойственности). Если в формуле  $F$ , представляющей булеву функцию  $\varphi(x_1, \dots, x_n)$ , все знаки функций заменить на соответствующие им знаки двойственных функций, то полученная формула  $F^*$  будет представлять функцию  $\varphi^*$ , двойственную исходной.

#### 4.6 Алгебра Жигалкина. Полином Жигалкина. Теорема о полиноме Жигалкина

**Определение 4.6.1.** Алгебра  $\langle P_2; \&, \oplus \rangle$  называется *алгеброй Жигалкина*.

**Определение 4.6.2.** Полином вида

$$a \oplus a_1 X_1 \oplus a_2 X_2 \oplus \dots \oplus a_n X_n \oplus a_{12} X_1 X_2 \oplus \dots \oplus a_{1\dots n} X_1 \dots X_n,$$

$$a, \dots, a_{1\dots n} \in \{0, 1\}$$

называют *полиномом Жигалкина*.

**Теорема.** *Любая булева функция может быть единственным образом представлена в виде полинома Жигалкина.*

*Доказательство.* Количество всех булевых функций от  $n$  переменных равно  $2^{2^n}$ . Количество различных слагаемых полинома Жигалкина от  $n$  переменных равно количеству различных подмножеств множества из  $n$  элементов, то есть  $2^n$ . Количество различных полиномов, которые можно образовать из этих слагаемых равно  $2^{2^n}$ . Таким образом, количество всех булевых функций от  $n$  переменных равно количеству всех различных полиномов Жигалкина от  $n$  переменных.

Так как разным функциям соответствует разные полиномы (одна и та же формула не может представлять разные функции), то между множеством всех булевых функций от  $n$  переменных и множеством всех полиномов Жигалкина от  $n$  переменных установлено взаимно-однозначное соответствие.  $\square$

## 5 Кодирование

### 5.1 Кодирование. Функция кодирования. Декодирование

**Определение 5.1.1.** Пусть задан алфавит  $\mathfrak{A} = \{a_1, \dots, a_n\}$  состоящий из конечного числа букв. Конечную последовательность символов из  $\mathfrak{A}$

$$A = a_{i_1} a_{i_2} \dots a_{i_n}$$

будем называть *словом* в алфавите  $\mathfrak{A}$ .

**Определение 5.1.2.** Пусть  $S = S(\mathfrak{A})$  — множество всех непустых слов в алфавите  $\mathfrak{A}$ , а  $S' \subset S$ . Слова из  $S'$  называются *сообщениями*.

**Определение 5.1.3.** Пусть дан алфавит  $\mathfrak{B} = \{b_1, \dots, b_q\}$ . Через  $B$  обозначим слово в алфавите  $\mathfrak{B}$ , через  $S(\mathfrak{B})$  — множество всех непустых слов в алфавите  $\mathfrak{B}$ . Пусть дана функция

$$F: S'(\mathfrak{A}) \rightarrow S(\mathfrak{B}),$$

которая каждому слову  $A \in S'(\mathfrak{A})$  ставит в соответствие слово  $B = F(A)$ ,  $B \in S(\mathfrak{B})$ .

Слово  $B$  будем называть *кодом сообщения*  $A$ , а переход от слова  $A$  к его коду — *кодированием*.

**Определение 5.1.4.** Обратная функция  $F^{-1}$  (если она существует) называется *функцией декодирования*.

## 5.2 Алфавитное кодирование. Схема кодирования. Равномерное кодирование

**Определение 5.2.1.** Рассмотрим соответствие между символами алфавита  $\mathfrak{A}$  и некоторыми словами в алфавите  $\mathfrak{B}$ :

$$a_i \mapsto B_i.$$

Это соответствие называют *схемой кодирования*. Схема определяет *алфавитное кодирование* следующим образом: каждому слову  $A = a_1 \dots a_n$  из  $S(\mathfrak{A})$  ставится в соответствие слово  $B = B_{i_1} \dots B_{i_n}$ , называемое *кодом* слова  $A$ . Слова  $B_{i_1}, \dots, B_{i_n}$  называют *элементарными кодами*.

Примером алфавитного кодирования может служить *азбука Морзе*, в которой каждой букве латинского алфавита ставится в соответствие последовательность точек и тире. Другим примером является *двоично-десятичное кодирование*.

**Определение 5.2.2.** Если длины всех элементарных кодов равны, то кодирование называют *равномерным*.

## 5.3 Свойство префиксности схемы кодирования. Взаимно-однозначное кодирование. Теорема- условие однозначности декодирования

**Определение 5.3.1.** Допустим,  $S'(\mathfrak{A}) = S(\mathfrak{A})$ , т. е. источник сообщений порождает множество всех слова алфавита  $\mathfrak{A}$ . Если отображение множества всех слов исходного алфавита на множество всех кодов взаимно-однозначно, то такое кодирование называется *взаимно-однозначным*.

Возникает вопрос: можно ли по схеме  $\Sigma$  понять, обладает ли кодирование свойством взаимной однозначности. Трудность решения состоит в том, что для непосредственной проверки взаимной однозначности необходимо проверить бесконечное количество слов. Однако простым достаточным признаком взаимно-однозначности кодирования является *условие префиксности*.

**Определение 5.3.2.** Пусть слово  $B$  имеет вид  $B = B_1 B_2$ . Тогда  $B_1$  называется *началом* или *префиксом* слова  $B$ , а  $B_2$ , соответственно, — *концом* или *окончанием* слова  $B$ .

**Определение 5.3.3.** Схема  $\Sigma$  обладает *свойством префикса*, если для любых  $i$  и  $j$  ( $1 \leq i, j \leq r, i \neq j$ ) слово  $B_i$  не является префиксом слова  $B_j$ .

**Теорема** (об однозначности декодирования). *Если схема  $\Sigma$  обладает свойством префикса, то алфавитное кодирование будет взаимно-однозначным.*