Дискретная математика

Е.А.Перепелкин

АлтГТУ

2019

Темы курса

1) Теория множеств
2) Комбинаторика
3) Алгебра логики
4) Алгебраические структуры
5) Теория графов

Список литературы

1. Новиков Ф.А. Дискретная математика для программистов. – СПб: Питер, 2008. – 384 с.
2. Поздняков С.Н., Рыбин С.В. Дискретная математика. – М.: Академия, 2008. – 447 с.
3. Яблонский С.В. Введение в дискретную математику. – М.: Высшая школа, 2006. – 384 с.
4. Мальцев И.А. Дискретная математика. – СПб: «Лань», 2011. – 304 с. – ЭБС «Лань».
5. Шевелев Ю.П., Писаренко Л.А. Сборник задач по дискретной математике. – СПб: «Лань», 2013. – 528 с. – ЭБС «Лань».
6. Копылов В.И. Курс дискретной математики. СПб: «Лань», 2011. – 208 с. – ЭБС «Лань».

Тема 1. Теория множеств

1.1 Понятие множества

Понятие множества является первичным неопределяемым понятием математики.

Множество можно понимать как объединение элементов, обладающих заданным свойством.

Принадлежность элемента x множеству A обозначается: $x \in A$, непринадлежность: $x \notin A$.

Способы задания множеств:

1) Перечислением элементов конечного множества

$$A = \{x_1; x_2; \ldots; x_n\}.$$

2) Характеристическим свойством

$$A = \{x |\ P(x)\}.$$

3) Алгоритмом формирования элементов множества.

Пример

1) Множество цифр шестнадцатеричной системы счисления задаётся перечислением цифр

$$X = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F\}.$$

2) Множество точек окружности единичного радиуса задаётся уравнением

$$S = \{(x, y) |\ x^2 + y^2 = 1\}.$$

3) Множество простых чисел от 1 до n можно задать алгоритмом последовательного вычёркивания составных чисел. Этот алгоритм получил название «Решето Эратосфена». Сначала вычеркиваются числа кратные 2, затем кратные 3 и т.д. После окончания работы алгоритма остаются только простые числа.

Для числовых множеств приняты следующие обозначения:

N – множество натуральных чисел;
Z – множество целых чисел;
Q – множество рациональных чисел;
R – множество действительных чисел;
C – множество комплексных чисел.

Интервал на числовой оси обозначается как

$$(a, b) = \{x|\ a < x < b\}.$$

Полуинтервалы

$$(a, b] = \{x|\ a < x \leq b\}, \quad [a, b) = \{x|\ a \leq x < b\}.$$

Отрезок

$$[a, b] = \{x|\ a \leq x \leq b\}.$$

Промежуток – любое из указанных множеств: интервал, полуинтервал или отрезок.

Два особых множества: универсальное множество U и пустое множество $\emptyset$.

Определение

Универсальным множеством (универсумом) будем называть множество, содержащее все элементы заданной природы. Например, множество всех равносторонних треугольников на плоскости.

Определение

Пустым множеством будем называть множество, не содержащее элементов заданной природы. Например, пустым множеством является множество действительных решений уравнения $x^2 = -1$.

1.2 Операции над множествами

Пусть $A, B, C, \ldots$ есть множества, состоящие из элементов U.

Определение

Два множества A и B называются равными, $A = B$, если они состоят из одних и тех же элементов,

$$\forall x \in U : x \in A \Leftrightarrow x \in B.$$

Определение

Множество A является подмножеством B (A включается в B), если

$$\forall x \in U : x \in A \Rightarrow x \in B.$$

Включение обозначают $A \subseteq B$. Строгое включение $A \subset B$ означает, что $A \subseteq B$ и $A \neq B$.

Два множества A и B равны (совпадают), если они являются подмножествами друг друга, $A \subseteq B$ и $B \subseteq A$.

Основные операции над множествами:

1) Объединение
$$A \cup B = \{x |\ x \in A \text{ или } x \in B\}.$$
2) Пересечение
$$A \cap B = \{x |\ x \in A \text{ и } x \in B\}.$$
3) Разность
$$A \setminus B = \{\ x |\ x \in A \text{ и } x \notin B\}.$$
4) Симметрическая разность
$$A \triangle B = \{x |\ (x \in A \text{ и } x \notin B) \text{ или } (x \notin A \text{ и } x \in B)\ \},$$
$$A \triangle B = (A \setminus B) \cup (B \setminus A),$$
$$A \triangle B = (A \cup B) \setminus (A \cap B).$$
5) Дополнение
$$\overline{A} = \{x |\ x \notin A\},$$
$$\overline{A} = U \setminus A.$$

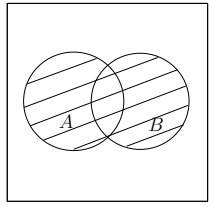
Пример

Пусть
$$U = \{1; 2; 3; 4; 5; 6; 7; 8; 9; 10\},$$
$$A = \{2; 4; 7\},$$
$$B = \{1; 4; 9\},$$
$$C = \{2; 5; 8; 9\}.$$

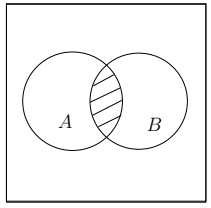
Построим множество
$$D = \overline{A \cup B} \setminus C.$$

Находим
$$A \cup B = \{1; 2; 4; 7; 9\},$$
$$\overline{A \cup B} = \{3; 5; 6; 8; 10\},$$
$$D = \{3; 6; 10\}.$$

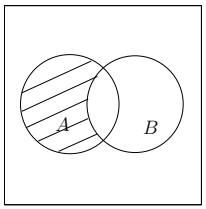
Наглядное представление операций над множествами дают диаграммы Эйлера-Венна



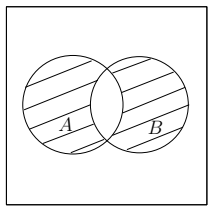
$A \cup B$



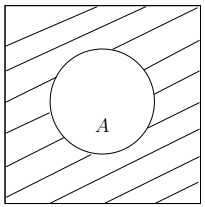
$A \cap B$



$A \setminus B$



$A \triangle B$

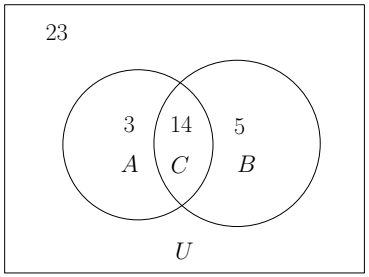


$\bar{A}$

Пример

В студенческой группе 23 человека. Экзамен по математике сдали 17 человек. Экзамен по информатике 19 человек. Оба экзамена сдали 14 человек. Сколько человек не сдали ни одного экзамена?
Обозначим:
U – множество студентов в группе;
A – множество студентов, сдавших экзамен по математике;
B – множество студентов, сдавших экзамен по информатике.

Множество студентов, сдавших
оба экзамена равно $C = A \cap B$,
сдавших только математику равно $D = A \setminus C$,
сдавших только информатику равно $E = B \setminus C$,
сдавших, по крайней мере один экзамен, равно $C \cup D \cup E$.
Множество студентов, не сдавших ни одного экзамена равно
$U \setminus (C \cup D \cup E)$.



Число студентов, сдавших
оба экзамена: 14,
только математику: 17-14=3,
только информатику: 19-14=5.
Число студентов, не сдавших ни одного экзамена ровно
23-(14+3+5)=1.

Определение

Разбиением множества A называется набор его попарно непересекающихся подмножеств A_i, $i \in I$ таких, что

$$A = \bigcup_{i \in I} A_i, \quad A_i \cap A_j = \emptyset, \quad i \neq j.$$

Пример

Для любого натурального числа $p > 0$ множество целых чисел можно записать в виде

$$Z = Z_0 \cup Z_1 \cup \cdots \cup Z_{p-1},$$

где

$$Z_0 = kp, \quad Z_1 = kp + 1, \quad \ldots, \quad Z_{p-1} = kp + p - 1, \quad k \in Z.$$

При этом $Z_i \cap Z_j = \emptyset$, $i \neq j$.

Определение

Булеаном множества A называется множество всех его подмножеств

$$2^A = \{B | \ B \subseteq A\}.$$

Пустое множество $\emptyset$ и само множество A являются элементами булеана.

Пример

Для множества $A = \{x; y; z\}$

$$2^A = \{\emptyset; \{x\}; \{y\}; \{z\}; \{x; y\}; \{x; z\}; \{y; z\}; \{x; y; z\}\}.$$

Определение

Характеристической функцией множества A называется функция принадлежности элементов U множеству A

$$f_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Множества совпадают тогда и только тогда, когда совпадают их характеристические функции

$$A = B \Leftrightarrow f_A(x) = f_B(x).$$

Свойства характеристических функций:

1) $f_U(x) = 1,\ f_\emptyset(x) = 0$
2) $f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x)f_B(x)$
3) $f_{A\cap B}(x) = f_A(x)f_B(x)$
4) $f_{\overline{A}}(x) = 1 - f_A(x)$
5) $f_{A\setminus B}(x) = f_A(x) - f_A(x)f_B(x)$
6) $f_{A\triangle B}(x) = f_A(x) + f_B(x) - 2f_A(x)f_B(x)$

Докажем свойство 4

$$x \in \overline{A} \Rightarrow x \notin A \Rightarrow f_A(x) = 0 \Rightarrow 1 - f_A(x) = 1,$$

$$x \notin \overline{A} \Rightarrow x \in A \Rightarrow f_A(x) = 1 \Rightarrow 1 - f_A(x) = 0.$$

Определение

Характеристическим вектором конечного множества

$$A \subseteq U = \{x_1; x_2; \ldots; x_n\}$$

называется вектор

$$h_A = [f_A(x_1), \ldots, f_A(x_n)].$$

Элементы характеристических векторов принимают только два значения: 0 и 1.

Операции сложения, умножения и отрицания характеристических векторов:

$$h = [h_1, \ldots, h_n], \quad g = [g_1, \ldots, g_n]$$

$$h + g = [h_1 + g_1, \ldots, h_n + g_n],$$
$$hg = [h_1 g_1, \ldots, h_n g_n],$$
$$\overline{h} = [\overline{h}_1, \ldots, \overline{h}_n],$$

где

h_i	g_i	$h_i + g_i$	$h_i g_i$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

h_i	$\overline{h}_i$
1	0
0	1

Операции над конечными множествами можно выразить через операции над характеристическими векторами этих множеств:

1) $h_{A\cup B} = h_A + h_B$
2) $h_{A\cap B} = h_A h_B$
3) $h_{\overline{A}} = \bar{h}_A$
4) $h_{A\setminus B} = h_A \bar{h}_B$
5) $h_{A\triangle B} = h_A \bar{h}_B + \bar{h}_A h_B$

Пример

Пусть

$$U = \{1;2;3;4;5;6;7;8;9;10\},$$
$$A = \{3;4;7;9;10\},$$
$$B = \{2;4;6;7;8;9\}.$$

Тогда

$$h_A = [0011001011],$$
$$h_B = [0101011110],$$
$$h_{\bar{A}} = \bar{h}_A = [1100110100],$$
$$h_{\bar{B}} = \bar{h}_B = [1010100001],$$
$$h_{A\setminus B} = h_A \bar{h}_B = [0010000001],$$
$$h_{A\triangle B} = h_A \bar{h}_B + \bar{h}_A h_B = [0110010101].$$

1.3 Теоретико-множественные тождества

Справедливы следующие теоретико-множественные тождества:

1) Коммутативность

$$A\cup B = B\cup A, \quad A\cap B = B\cap A.$$

2) Ассоциативность

$$(A\cup B)\cup C = A\cup(B\cup C), \quad (A\cap B)\cap C = A\cap(B\cap C).$$

3) Дистрибутивность

$$(A\cup B)\cap C = (A\cap C)\cup(B\cap C), \quad (A\cap B)\cup C = (A\cup C)\cap(B\cup C).$$

4) Законы де Моргана

$$\overline{A\cup B} = \overline{B}\cap\overline{A}, \quad \overline{A\cap B} = \overline{B}\cup\overline{A}.$$

5) Идемпотентность

$$A\cup A = A, \quad A\cap A = A.$$

6) Поглощение

$$(A\cup B)\cap A = A, \quad (A\cap B)\cup A = A.$$

7) Свойства нуля

$$A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset.$$

8) Свойства единицы

$$A \cup U = U, \quad A \cap U = A.$$

9) Инволютивность

$$\overline{\overline{A}} = A.$$

10) Свойства дополнения

$$A \cup \overline{A} = U, \quad A \cap \overline{A} = \emptyset.$$

Доказать теоретико-множественные тождества можно методом включения и методом характеристических функций.

Метод включения заключается в следующем. Множества A и B равны, если $A \subseteq B$ и $B \subseteq A$. Следовательно, $A = B$, если

$$\forall x: \ x \in A \Rightarrow x \in B \text{ и } x \in B \Rightarrow x \in A,$$

или в виде одного утверждения

$$\forall x: \ x \in A \Leftrightarrow x \in B.$$

Докажем закон де Моргана

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

методом включения. В соответствии с определением операций над множествами

$$x \in \overline{A \cup B} \Rightarrow x \notin A \cup B \Rightarrow x \notin A \text{ и } x \notin B \Rightarrow$$
$$x \in \overline{A} \text{ и } x \in \overline{B} \Rightarrow x \in \overline{A} \cap \overline{B} \Rightarrow \overline{A \cup B} \subseteq \overline{A} \cap \overline{B}.$$

С другой стороны,

$$x \in \overline{A} \cap \overline{B} \Rightarrow x \in \overline{A} \text{ и } x \in \overline{B} \Rightarrow x \notin A \text{ и } x \notin B \Rightarrow$$
$$x \notin A \cup B \Rightarrow x \in \overline{A \cup B} \Rightarrow \overline{A} \cap \overline{B} \subseteq \overline{A \cup B}.$$

Объединим две эти записи в одну

$$x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \text{ и } x \notin B \Leftrightarrow$$
$$x \in \overline{A} \text{ и } x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B} \Rightarrow \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Докажем методом характеристических функций

$$f_{\overline{A \cup B}}(x) = 1 - f_{A \cup B}(x) = 1 - f_A(x) - f_B(x) + f_A(x) f_B(x),$$
$$f_{\overline{A} \cap \overline{B}}(x) = f_{\overline{A}}(x) f_{\overline{B}}(x) = (1 - f_A(x))(1 - f_B(x)) =$$
$$= 1 - f_A(x) - f_B(x) + f_A(x) f_B(x).$$

Следовательно,

$$f_{\overline{A \cup B}}(x) = f_{\overline{A} \cap \overline{B}}(x)$$

и

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Законы де Моргана можно обобщить на несколько множеств.

Теорема

Справедливы тождества

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A}_i, \quad \overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} \overline{A}_i.$$

Доказательство.

Докажем второе тождество

$$x \in \overline{\bigcap_{i=1}^{n} A_i} \Leftrightarrow x \notin \bigcap_{i=1}^{n} A_i \Leftrightarrow$$

$$\exists i: \ x \notin A_i \Leftrightarrow \exists i: \ x \in \overline{A}_i \Leftrightarrow x \in \bigcup_{i=1}^{n} \overline{A}_i.$$

□

1.4 Мощность конечного множества

Определение

Количество элементов конечного множества называется мощностью множества и обозначается $|A|$.

Мощность конечного множества A с характеристической функцией $f_A(x)$ равна

$$|A| = \sum_{x \in U} f_A(x).$$

Для разбиения конечного множества

$$A = \bigcup_{i=1}^{n} A_i, \quad A_i \cap A_j = \emptyset, \quad i \neq j,$$

справедливо равенство

$$|A| = \sum_{i=1}^{n} |A_i|.$$

Теорема

Для любых конечных множеств A и B справедливо равенство

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Доказательство.

$$|A \cup B| = \sum_{x \in U} f_{A \cup B}(x) = \sum_{x \in U} (f_A(x) + f_B(x) - f_{A \cap B}(x)) =$$
$$= |A| + |B| - |A \cap B|.$$

□

Теорема (Формула включения-исключения)

Пусть $A_1, \ldots, A_n$ есть подмножества некоторого конечного множества A. Тогда

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

Доказательство.

Докажем на основе принципа математической индукции.
Базис индукции. При $n = 2$ получим

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Шаг индукции. Пусть теорема справедлива для $(n-1)$-го подмножества. Тогда

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left|\bigcup_{i=1}^{n-1} A_i \cup A_n\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| =$$

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

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

□

Теорема

Пусть $A_1, \ldots, A_n$ есть подмножества некоторого конечного множества A. Тогда

$$\left|\bigcap_{i=1}^{n} \overline{A_i}\right| = |A| - \left(\sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \right.$$

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

Доказательство.

По закону де Моргана

$$\left|\bigcap_{i=1}^{n} \overline{A_i}\right| = \left|\overline{\bigcup_{i=1}^{n} A_i}\right| = \left|A \setminus \bigcup_{i=1}^{n} A_i\right| = |A| - \left|\bigcup_{i=1}^{n} A_i\right|.$$

□

Теорема

Пусть A – конечное множество. Тогда мощность булеана

$$|2^A| = 2^{|A|}.$$

Доказательство.

Докажем на основе принципа математической индукции. Обозначим $A_n = \{x_1; \ldots; x_n\}$. Базис индукции. При $n = 1$ получим

$$2^{A_1} = \{\{x_1\}; \emptyset\}, \quad |2^{A_1}| = 2^{|A_1|} = 2.$$

Шаг индукции. Пусть утверждение теоремы верно для множества A_{n-1}. Множество 2^{A_n} представим в виде объединения двух непересекающихся множеств

$$2^{A_n} = 2^{A_{n-1}} \cup B, \quad B = \left\{C \subseteq 2^{A_n} |\ a_n \in C\right\}, \quad 2^{A_{n-1}} \cap B = \emptyset.$$

Следовательно, $|2^{A_n}| = |2^{A_{n-1}}| + |B| = 2 \cdot 2^{n-1} = 2^n$. □

1.5 Декартово произведение множеств

Определение

Прямым (декартовым) произведением множеств A_i, $i = 1, \ldots, n$,

$$B = A_1 \times A_2 \times \cdots \times A_n$$

называется множество всех упорядоченных наборов

$$(x_1, x_2, \ldots, x_n),$$

где $x_i \in A_i$, $i = 1, \ldots, n$.

Если $A \neq B$, то $A \times B \neq B \times A$.

Пример

Пусть

$$A = \{x; y; z\}, \quad B = \{0; 1\}.$$

Тогда

$$A \times B = \{(x,0); (x,1); (y,0); (y,1); (z,0); (z,1)\},$$
$$B \times A = \{(0,x); (0,y); (0,z); (1,x); (1,y); (1,z)\}.$$

Определение

Пусть все множества A_i, $i = 1, \ldots, n$ равны между собой. Множество

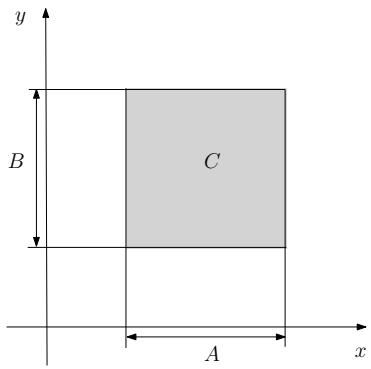
$$A^n = A \times \cdots \times A$$

называется n-ой степенью множества A.

Пример

Множество $R^2 = R \times R$ является множеством точек плоскости с декартовой системой координат.

Геометрическая интерпретация декартового произведения. Здесь множества A и B отрезки числовой оси, $C = A \times B$.



Теорема

Справедливы тождества:

1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$,
2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$,
3) $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
4) $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
5) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$,
6) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$,
7) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$,
8) $\overline{A \times B} = (\overline{A} \times \overline{B}) \cup (\overline{A} \times B) \cup (A \times \overline{B})$.

Доказательство.

Докажем тождество 1

$$(x,y) \in A \times (B \cup C) \Leftrightarrow x \in A \text{ и } y \in B \cup C \Leftrightarrow$$
$$x \in A \text{ и } (y \in B \text{ или } y \in C) \Leftrightarrow (x \in A \text{ и } y \in B) \text{ или } (x \in A \text{ и } y \in C) \Leftrightarrow$$
$$(x,y) \in A \times B \text{ или } (x,y) \in A \times C \Leftrightarrow (x,y) \in (A \times B) \cup (A \times C)$$

□

Теорема

Пусть множества A_i, $i = 1, \ldots, n$ конечны. Тогда мощность прямого произведения

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1||A_2| \cdots |A_n|.$$

Доказательство.

При построении прямого произведения первый элемент выбираем $|A_1|$ способами, второй независимо от первого $|A_2|$ способами и т.д. Всего получим $|A_1||A_2| \cdots |A_n|$ различных элементов прямого произведения. □

Как следствие получим $|A^n| = |A|^n$.

1.6 Бинарные отношения и их свойства

Определение

Отношение R на множествах A_i, $i = 1, \ldots, n$ есть подмножество прямого произведения этих множеств

$$R \subseteq A_1 \times A_2 \times \ldots A_n.$$

Определение

Бинарным отношением называется отношение на двух множествах

$$R \subseteq A \times B.$$

Определение

Бинарным отношением на множестве называется отношение

$$R \subseteq A \times A = A^2.$$

Принадлежность пары (x,y) бинарному отношению R записывается в виде $(x,y) \in R$ или xRy.

Бинарные отношения на конечных множествах можно задавать в виде списка элементов, в виде матрицы, в виде графа.

Пусть $A = \{x_1; x_2; \ldots; x_n\}$, $B = \{y_1; y_2; \ldots; y_m\}$. Матрица бинарного отношения $R \subseteq A \times B$ состоит из элементов

$$M_{ij} = \begin{cases} 1, & (x_i, y_j) \in R \\ 0, & (x_i, y_j) \notin R \end{cases}.$$

Матрицу бинарного отношения R будем обозначать M_R.

Пример

На множестве чисел $A = \{1; 2; 3; 4; 5; 6\}$ зададим бинарное отношение

$$R = \{(x, y) |\ x \text{ делитель } y\}.$$

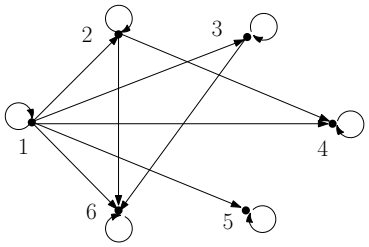
Отношение содержит элементы

$$R = \{(1,1); (1,2); (1,3); (1,4); (1,5); (1,6);$$
$$(2,2); (2,4); (2,6); (3,3); (3,6); (4,4); (5,5); (6,6)\}.$$

Матрица отношения равна

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Граф отношения



Определение

Тождественным отношением, заданным на множестве A, называется отношение

$$E = \{(x, x) |\ x \in A\}.$$

Матрица тождественного отношения, заданного на конечном множестве, есть единичная матрица.

Определение

Множество

$$D_R = \{x |\ \exists y \in B :\ xRy\} \subseteq A$$

называется областью определения отношения $R \subseteq A \times B$.

Определение

Множество

$$I_R = \{y |\ \exists x \in A :\ xRy\} \subseteq B$$

называется областью значений отношения $R \subseteq A \times B$.

Определение

Обратным отношением для отношения $R \subseteq A \times B$ называется отношение

$$R^{-1} = \{(y, x) |\ xRy\} \subseteq B \times A.$$

Определение

Композицией бинарных отношений

$$R_1 \subseteq A \times B, \quad R_2 \subseteq B \times C$$

называется отношение

$$R_1 \circ R_2 = \{(x, y) |\ x \in A,\ y \in C,\ \exists z \in B :\ xR_1z,\ zR_2y\} \subseteq A \times C.$$

Определение

Ядром отношения $R \subseteq A \times B$ называется отношение

$$K_R = R \circ R^{-1}.$$

Теорема

Справедливы тождества:

1) $\left(R^{-1}\right)^{-1} = R$,
2) $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$,
3) $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$,
4) $R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$,
5) $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$,
6) $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$,
7) $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.

Доказательство.

Докажем тождество 7

$$x(R_1 \circ R_2)^{-1} y \Leftrightarrow y(R_1 \circ R_2)x \Leftrightarrow \exists z : yR_1z,\ zR_2x \Leftrightarrow$$
$$zR_1^{-1}y,\ xR_2^{-1}z \Leftrightarrow x(R_2^{-1} \circ R_1^{-1})y.$$

□

Пусть R – бинарное отношение на множестве A. Обозначим

$$R^n = \underbrace{R \circ R \circ \cdots \circ R}_{n}.$$

Определим $R^0 = E$. Тогда справедливы следующие соотношения

$$R^n \circ R^m = R^{n+m}, \quad (R^n)^{-1} = \left(R^{-1}\right)^n = R^{-n}.$$

Определение

Отношение $R \subseteq A^2$ называется рефлексивным, если

$$\forall x \in A :\ xRx.$$

Определение

Отношение $R \subseteq A^2$ называется антирефлексивным, если не существует $x \in A$ такого, что xRx.

Определение

Отношение $R \subseteq A^2$ называется симметричным, если

$$\forall x, y \in A : xRy \Rightarrow yRx.$$

Определение

Отношение $R \subseteq A^2$ называется антисимметричным, если не существует $x, y \in A$ таких, что одновременно xRy и yRx.

Определение

Отношение $R \subseteq A^2$ называется транзитивным, если для

$$\forall x, y, z \in A: \ xRy, \ yRz \Rightarrow xRz.$$

Определение

Отношение $R \subseteq A^2$ называется плотным, если

$$\forall x, y \in A: x \neq y, \ xRy \Rightarrow \exists z \neq x, y: xRz, \ zRy.$$

Теорема

Отношение R симметрично $\Leftrightarrow R = R^{-1}$

Доказательство.

Необходимость. Пусть R – симметрично. Тогда

$$xRy \Rightarrow yRx \Rightarrow xR^{-1}y \Rightarrow R \subseteq R^{-1},$$
$$xR^{-1}y \Rightarrow yRx \Rightarrow xRy \Rightarrow R^{-1} \subseteq R.$$

Следовательно, $R = R^{-1}$.
Достаточность. Пусть $R = R^{-1}$. Тогда

$$xRy \Rightarrow xR^{-1}y \Rightarrow yRx.$$

Следовательно, R – симметрично. □

Теорема

Отношение R транзитивно $\Leftrightarrow R^2 \subseteq R$.

Доказательство.

Необходимость. Пусть R транзитивно. Тогда

$$\forall x, y: xR^2y \Rightarrow \exists z: xRz, \ zRy \Rightarrow xRy \Rightarrow R^2 \subseteq R.$$

Достаточность. Пусть $R^2 \subseteq R$. Тогда

$$\forall x, y, z: xRz, \ zRy \Rightarrow xR^2y \Rightarrow xRy.$$

Следовательно, отношение транзитивно. □

Теорема

Транзитивное отношение R плотно $\Leftrightarrow R^2 = R$.

Доказательство.

Необходимость. Пусть R плотно. Тогда

$$\forall x, y: \ xRy \Rightarrow \exists z: \ xRz, \ zRy \Rightarrow xR^2y \Rightarrow R \subseteq R^2.$$

В силу транзитвности $R^2 \subseteq R$. Следовательно, $R^2 = R$.
Достаточность. Пусть $R^2 = R$. Тогда

$$\forall x, y: \ xRy \Rightarrow xR^2y \Rightarrow \exists z: \ xRz, \ zRy.$$

Следовательно, R плотно. □

1.7 Отношение эквивалентности

Определение

Отношение $R \subseteq A^2$ называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Отношение эквивалентности обозначают $x \sim y$.

Пример

1) Два целых числа x, y сравнимы по модулю натурального числа p

$$x \equiv y \pmod{p},$$

если совпадают остатки от деления этих чисел на p. Отношение сравнения по модулю является отношением эквивалентности.

2) Отношение подобия фигур в геометрии является отношением эквивалентности.

Определение

Пусть $x \in A$. Множество $[x] = \{y \in A |\ x \sim y\}$ называется классом эквивалентности.

Теорема

Классы эквивалентности образуют разбиение множества A.

Доказательство.

$$\forall x \in A:\ x \sim x \Rightarrow x \in [x] \Rightarrow \bigcup_{x \in A} [x] = A,$$

$$\forall x, y \in A:\ [x] \cap [y] \neq \emptyset \Rightarrow \exists z \in A:\ z \in [x] \cap [y] \Rightarrow$$

$$x \sim z,\ z \sim y \Rightarrow x \sim y \Rightarrow [x] = [y].$$

□

Теорема

Любое разбиение множества A порождает отношение эквивалентности на этом множестве.

Доказательство.

Пусть

$$A = \bigcup_{i \in I} A_i, \quad A_i \cap A_j = \emptyset, \quad i \neq j.$$

Определим отношение

$$x \sim y \Leftrightarrow x, y \in A_i.$$

Выполняются все три свойства: рефлексивность, симметричность, транзитивность. □

Определение

Если R – отношение эквивалентности на множестве A, то множество классов эквивалентности называется фактормножеством и обозначается $A|R$.

Фактормножество является подмножеством булеана $A|R \subseteq 2^A$.

Пример

Рассмотрим отношение сравнения по модулю 2 на множестве целых чисел Z. Существует два класса эквивалентности: множество чётных чисел

$$[0] = \{2k |\ k \in Z\}$$

и множество нечётных чисел

$$[1] = \{2k + 1 |\ k \in Z\}.$$

При этом

$$Z = [0] \cup [1], \quad [0] \cap [1] = \emptyset.$$

1.8 Замыкания бинарных отношений

Определение

Отношение R_p называется замыканием отношения $R \subseteq A^2$ относительно свойства p, если:

1) R_p обладает свойством p;
2) $R \subseteq R_p$;
3) R_p является подмножеством любого другого отношения, включающего в себя R и обладающего свойством p.

Теорема

Справедливы представления замыканий

1) *Рефлексивное замыкание*

$$R_r = R \cup E$$

2) *Симметричное замыкание*

$$R_s = R \cup R^{-1}$$

3) *Транзитивное замыкание*

$$R_t = \bigcup_{i=1}^{\infty} R^i$$

Доказательство.

Докажем 3.

$$\forall x, y, z : xR_t y,\ yR_t z \Rightarrow \exists m, k : xR^m y,\ yR^k z \Rightarrow xR^{m+k} z \Rightarrow xR_t z.$$

Следовательно, R_t – транзитивное отношение.
Условие $R \subseteq R_t$ также выполняется, поскольку $R = R^1 \subseteq R_t$.
Пусть R' – транзитивно и $R \subseteq R'$. Тогда

$$\forall x, y :\ xR_t y \Rightarrow \exists m : xR^m y \Rightarrow$$
$$\exists z_1, z_2, \ldots, z_{m-1} :\ xRz_1, z_1Rz_2, \ldots, z_{m-1}Ry \Rightarrow$$
$$xR'z_1, z_1R'z_2, \ldots, z_{m-1}R'y \Rightarrow xR'y \Rightarrow R_t \subseteq R'.$$

□

Теорема

Пусть R – бинарное отношение на конечном множестве с n элементами. Транзитивное замыкание R равно

$$R_t = \bigcup_{i=1}^{n} R^i.$$

Доказательство.

Транзитивное замыкание равно

$$R_t = \bigcup_{i=1}^{\infty} R^i.$$

Обозначим

$$R_n = \bigcup_{i=1}^{n} R^i.$$

Справедливо включение $R_n \subseteq R_t$. Покажем, что $R_t \subseteq R_n$. Для этого достаточно показать, что $R^m \subseteq R_n$ при $m > n$. Пусть $xR^m y$, $m > n$. Существует последовательность элементов

$$z = (z_1, z_2, \ldots, z_{m-1})$$

таких, что

$$xRz_1, z_1Rz_2, \ldots, z_{m-1}Ry.$$

В этой последовательности обязательно найдутся два одинаковых элемента $z_i = z_j$, $j > i$, поскольку всего элементов во множестве n.

Следовательно,

$$xRz_1, \ldots, z_iRz_{j+1}, \ldots, z_{m-1}Ry.$$

Продолжая сокращать последовательность элементов z, придем к последовательности, длина которой $k \leq n-1$ и, таким образом, $xR^{k+1}y$. Следовательно,

$$xR^m y \Rightarrow xR_n y \Rightarrow R^m \subseteq R_n.$$

□

1.9 Матрицы бинарных отношений

Пусть $R \subseteq A \times B$ – бинарное отношение на конечных множествах.

Матрица M_R отношения R состоит из $n = |A|$ строк и $m = |B|$ столбцов.

Элементы M_R принимают два значения: $0, 1$. Такого рода матрицы называются логическими или булевыми.

Для булевых матриц определяются операции суммы и произведения с учётом булевых операций сложения и умножения

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 1,$$
$$0 \cdot 0 = 0, \quad 1 \cdot 0 = 0 \cdot 1 = 0, \quad 1 \cdot 1 = 1.$$

Для матриц бинарных отношений справедливы равенства:

1) $M_{R_1 \cup R_2} = M_{R_1} + M_{R_2}$
2) $M_{R_1 \circ R_2} = M_{R_1} \cdot M_{R_2}$
3) $M_{R^k} = (M_R)^k$
4) $M_{R^{-1}} = (M_R)^T$
5) $M_{R_r} = M_R + M_E$
6) $M_{R_s} = M_R + (M_R)^T$
7) $M_{R_t} = \sum_{i=1}^{n} (M_R)^i$

Пример

Рассмотрим множество $A = \{1; 2; 3; 4; 5\}$ и бинарное отношение на этом множестве

$$R = \{(1,2); (2,1); (2,5); (3,3); (4,1); (4,5); (5,4)\}.$$

Матрица отношения равна

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Матрицы замыканий

$$M_{R_r} = M_R + M_E = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$M_{R_s} = M_R + M_R{}^T = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix},$$

$$M_{R_t} = M_R + M_R{}^2 + M_R{}^3 + M_R{}^4 + M_R{}^5 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

1.10 Отношение порядка

Определение

Антисимметричное транзитивное отношение называется отношением порядка. Обозначается $\prec$.

Если $x \prec y$, то говорят, что x предшествует y.

Определение

Рефлексивное отношение порядка называется отношением нестрогого порядка. Обозначается $\leq$.

Определение

Антирефлексивное отношение порядка называется отношением строгого порядка. Обозначается $<$.

Определение

Отношение порядка называется отношением полного (линейного) порядка, если для любых x, y или $x \prec y$ или $y \prec x$. Иначе отношение порядка называется отношением частичного порядка.

Определение

Множество A с заданным на нём отношением порядка $\prec$ называется упорядоченным и обозначается $(A, \prec)$.

Пример

На множестве целых чисел рассмотрим отношение делимости $x|y$. Это отношение является отношением нестрогого частичного порядка.

Пример

На множестве точек окружности

$$A = \{(x, y) |\ x^2 + y^2 = 1\}$$

зададим отношение

$$(x_1, y_1) \prec (x_2, y_2),$$

если $x_1 < x_2$ и $y_1 < y_2$. Это отношение является отношением строгого частичного порядка.

Пример

Лексикографический порядок на множестве слов русского языка является отношением полного порядка.

Определение

Элемент x упорядоченного множества $(A, \prec)$ называется максимальным, если

$$\forall y \in A:\ x \prec y \Rightarrow y = x.$$

Определение

Элемент x упорядоченного множества $(A, \prec)$ называется минимальным, если

$$\forall y \in A:\ y \prec x \Rightarrow y = x.$$

Определение

Элемент x упорядоченного множества $(A, \prec)$ называется наибольшим (supremum), если

$$\forall y \in A:\ y \prec x.$$

Определение

Элемент x упорядоченного множества $(A, \prec)$ называется наименьшим (infinum), если

$$\forall y \in A:\ x \prec y.$$

Теорема

Наибольший (наименьший) элемент упорядоченного множества $(A, \prec)$, если существует, то является единственным.

Доказательство.

Пусть существуют два наибольших элемента x и y. Тогда $x \prec y$ и $y \prec x$. В силу антисимметричности получим $x = y$. Аналогично доказывается единственность наименьшего элемента. □

Максимальных (минимальных) элементов может быть несколько или бесконечно много.

Если существует наибольший элемент, то он является и максимальным элементом.

Аналогичное утверждение верно и для наименьшего элемента.

Определение

Упорядоченное множество с полным порядком называется вполне упорядоченным, если в любом его непустом подмножестве есть минимальный элемент.

Пример

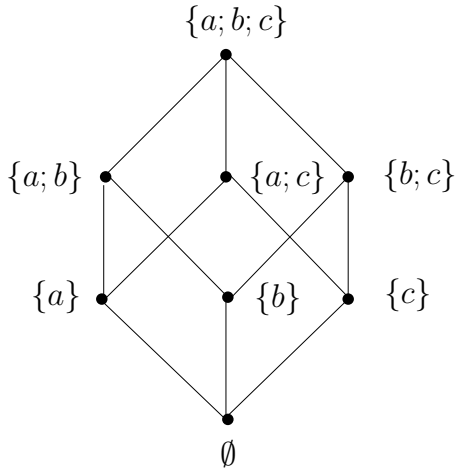
Множество неотрицательных целых чисел является вполне упорядоченным.
Множество неотрицательных действительных чисел вполне упорядоченным не является.

Конечное упорядоченное множество можно представить в виде диаграммы Хассе. В диаграмме Хассе элементы множества изображаются в виде точек на плоскости. Точки x и y соединяются линией, если $x \prec y$ и не существует z такого, что $x \prec z \prec y$. При этом точка x находится ниже точки y.

Пример

Рассмотрим множество всех подмножеств трехэлементного множества $A = \{a; b; c\}$. Отношение включения подмножеств является отношением частичного порядка.

Диаграмма Хассе



1.11 Функции

Определение

Функцией, отображающей множество A во множество B, называется бинарное отношение $R \subseteq A \times B$ такое, что $D_R = A$ и

$$\forall x \in A\ \forall y, z \in B:\ xRy, xRz \Rightarrow y = z.$$

Функцию принято обозначать $f : A \to B$ или $y = f(x)$. Областью определения функции является множество A, областью значений – множество

$$f(A) = \{y \in B \mid \exists x \in A:\ y = f(x)\}.$$

Определение

Функция называется инъективной, если

$$\forall x_1, x_2 \in A\ \forall y \in B:\ y = f(x_1), y = f(x_2) \Rightarrow x_1 = x_2.$$

Определение

Функция называется сюръективной, если

$$\forall y \in B\ \exists x \in A:\ y = f(x).$$

Область значений сюръективной функции совпадает со множеством B. Сюръективная функция задаёт отображение множества A на множество B.

Определение

Функция называется биективной, если она инъективная и сюръективная.

Биективная функция устанавливает взаимно-однозначное соответствие множеств A и B. Биективная функция обозначается

$$f : A \leftrightarrow B.$$

Для биективной функции существует обратная функция

$$f^{-1} : B \leftrightarrow A, \quad y = f(x) \Leftrightarrow x = f^{-1}(y).$$

Справедливы соотношения

$$f^{-1}(f(x)) = x, \quad f(f^{-1}(y)) = y.$$

Пример

Функция

$$f : Z \to \{0; 1\}, \quad f(x) = x \pmod 2$$

является сюръективной, но не является инъективной.
Пусть M – множество чётных натуральных чисел. Функция

$$f : N \to M, \quad y = 2x$$

является инъективной и сюръективной.

Определение

Композицией функций $f : A \to B$, $g : B \to C$ называется функция $f \circ g : A \to C$, которая строится как композиция соответствующих отношений,

$$\forall x \in A:\ (f \circ g)(x) = g(f(x)).$$

Теорема

Пусть $f : A \leftrightarrow B$ и $g : B \leftrightarrow C$ биективные функции. Тогда $f \circ g$ также биективная функция и

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Доказательство.

Биективность композиции следует из биективности f и g.
Покажем, что

$$\forall x \in C: \ (f \circ g)^{-1}(x) = (g^{-1} \circ f^{-1})(x).$$

Обозначим

$$y = (f \circ g)^{-1}(x).$$

Тогда

$$x = (f \circ g)(y) = g(f(y)),$$
$$(g^{-1} \circ f^{-1})(x) = f^{-1}(g^{-1}(x)) = f^{-1}(g^{-1}(g(f(y)))) = y.$$

□

Пример

Пусть

$$f: N \to N, \quad f(x) = x^2,$$
$$g: N \to N, \quad g(x) = x + 1.$$

Тогда

$$(f \circ g)(x) = x^2 + 1, \quad (g \circ f)(x) = (x + 1)^2.$$

Пусть $f: A \to B$ есть сюръекция. На множестве A зададим отношение эквивалентности

$$R_f = \{(x_i, x_j) |\ f(x_i) = f(x_j)\}.$$

Рассмотрим фактор множество

$$A|R_f = \{A_i |\ i \in I\}$$

и функцию $g: A|R \to B$ такую, что

$$g(A_i) = y_i, \quad y_i = f(x), \quad x \in A_i.$$

Функция g является биекцией. Таким образом можно перейти от сюръекции к биекции, заменив множество A на фактор множество $A|R_f$.

1.12 Мощность бесконечного множества

Определение

Множества A и B называются равномощными (эквивалентными), если существует биекция $A \leftrightarrow B$. Эквивалентность множеств A и B обозначают $A \sim B$.

Определение

Мощностью или кардинальным числом множества A называется класс эквивалентных A множеств.

Мощность множества обозначают $|A|$. Мощности множеств можно сравнивать:

1) Если $A \sim B$, то $|A| = |B|$.
2) Пусть существует инъекция $A \to B$. Тогда $|A| \leq |B|$.
3) Если $|A| \leq |B|$ и $A \approx B$, то $|A| < |B|$.

Теорема

Мощность любого множества A меньше мощности множества всех его подмножеств 2^A.

Доказательство.

Все элементы A являются элементами 2^A, поэтому $|A| \leq |2^A|$.
Покажем, что $|A| < |2^A|$. Пусть существует биекция $f : A \leftrightarrow 2^A$.
Составим множество

$$B = \{a \in A |\ a \notin f(a)\}.$$

Пусть $f(b) = B$. Тогда

$$b \in B \Rightarrow b \notin f(b) = B,$$
$$b \notin B \Rightarrow b \in f(b) = B.$$

Получили противоречие. □

Определение

Множество A называется счётным, если $A \sim N$. Мощность счётного множества обозначают $\aleph_0$ – «алеф нуль».

Теорема

1) *Счётными являются множества целых чисел, множество рациональных чисел.*
2) *Множество действительных чисел счётным не является.*

Доказательство.

Докажем 2. Предположим, что существует биекция $f : N \leftrightarrow R$. Каждое действительное число можно записать в виде бесконечной дроби

$$c = a, b_1 b_2 \ldots,$$

где a – целая часть, $b = 0, b_1 b_2 \ldots$ – дробная часть числа. Конечную дробную часть дополним бесконечным числом нулей.
Составим число

$$d = 0, d_1 d_2 \ldots$$

по правилу: $d_i = 0$ если в числе $f(i)$ значение $b_i \neq 0$ и $d_i = 1$ если в числе $f(i)$ значение $b_i = 0$. В результате получим действительное число, которое не совпадает ни с одним из чисел $f(N)$. □

Определение

Мощность множества всех подмножеств множества натуральных чисел 2^N называется мощностью континуума и обозначается c. Множество, равномощное 2^N, называется континуальным множеством.

Теорема

Множество действительных чисел R и множество 2^N равномощны.

Доказательство.

Рассмотрим множество B всех бесконечных последовательностей из нулей и единиц. Покажем, что $B \sim 2^N$.

Биекцию

$$g : 2^N \leftrightarrow B$$

можно установить по следующему правилу. Пусть $A \subseteq 2^N$ и $f_A(x)$ – характеристическая функция A. Тогда

$$g(A) = (f_A(1)f_A(2)\dots).$$

Множество B эквивалентно полуинтервалу $[0,1)$, поскольку каждое действительное число $0 \le a < 1$ можно записать в двоичной системе счисления в виде последовательности нулей и единиц

$$a = 0, b_1 b_2 \dots.$$

Полуинтервал $[0,1)$ эквивалентен интервалу $(0,1)$. Биекцию можно установить по правилу:

$$f(x) = \begin{cases} 1/2, & x = 0 \\ 1/(n+1), & x = 1/n,\ n = 2,3,\dots \\ x, & x \ne 0,\ x \ne 1/n,\ n = 2,3,\dots \end{cases}$$

Множества R и $(0,1)$ эквивалентны в силу биекции

$$f(x) = \frac{1}{\pi}\operatorname{arctg} x + \frac{1}{2}.$$

Следовательно, $2^N \sim B \sim [0,1) \sim (0,1) \sim R$.

□

Обозначим

$$A_0 = N, \quad A_i = 2^{A_{i-1}}, \quad \aleph_i = |A_i|, \quad i = 0,1,2,\dots$$

Справедливы неравенства

$$\aleph_0 < \aleph_1 < \aleph_2 < \dots$$

Континуум-гипотеза заключается в том, что других кардинальных чисел бесконечных множеств, отличных от $\aleph_i$, $i = 0,1,2,\dots$, не существует.

В частности, не существует бесконечного подмножества множества действительных чисел, мощность которого больше мощности множества натуральных чисел и меньше мощности действительных чисел.

Континуум-гипотеза независима от аксиом теории множеств. Эту гипотезу нельзя ни доказать ни опровергнуть.

Тема 2. Комбинаторика

2.1 Правила комбинаторики

Большинство задач комбинаторики связаны с выбором и определением числа элементов конечного множества, обладающих заданным свойством.

Комбинаторика основана на двух правилах.

Утверждение (Правило суммы)

Пусть объект A может быть выбран n способами, объект B – m способами. Тогда выбор «или A или B» может быть осуществлён $n + m$ способами.

Утверждение (Правило произведения)

Пусть последовательно выбираются два объекта A и B. Если объект A может быть выбран n способами и после каждого такого выбора объект B может быть выбран m способами, то последовательный выбор «A и B» может быть осуществлён nm способами.

Пример

На книжной полке стоят 5 книг по математике и 7 книг по информатике. Сколько существует способов выбрать одну книгу с полки?
Таких способов 12. Здесь мы применили правило суммы.

Пример

Сколько слов, содержащих 5 букв, можно составить из 26 букв латинского алфавита при условии, что любые две стоящие рядом буквы различны?
При составлении слов первую букву можно выбрать любой из 26 букв алфавита.
Вторая буква не должна совпадать с первой. Поэтому вторую букву можно выбрать 25-ю способами.
Аналогично третья, четвертая и пятая буквы могут быть выбраны 25-ю способами.
Согласно правилу умножения получаем $26 \cdot 25^4 = 10156250$ различных слов.

В теории множеств правилу суммы соответствует формула

$$|A \cup B| = |A| + |B|, \quad A \cap B = \emptyset,$$

правилу произведения – формула

$$|A \times B| = |A||B|.$$

Правило суммы и произведения можно обобщить на выбор нескольких объектов.

2.2 Перестановки, размещения, сочетания, разбиения

Пусть $A = \{a_1; a_2; \ldots; a_n\}$ конечное множество из n элементов.

Будем строить выборки элементов множества A, содержащие m элементов. Такие выборки будем называть (n, m)-выборками.

При построении выборки сначала выбираем первый элемент, затем второй и так далее, всего m элементов. Обозначим эти элементы

$$b_1, b_2, \ldots, b_m.$$

Если нас интересует порядок элементов в выборке, то будем говорить о упорядоченной выборке, иначе – о неупорядоченной выборке.

Упорядоченную выборку будем записывать в виде последовательности

$$(b_1, b_2, \ldots, b_m),$$

неупорядоченную – в виде множества

$$\{b_1; b_2; \ldots; b_m\}.$$

При построении выборки, выбирая очередной элемент, мы можем исключить этот элемент из множества A, и тем самым запретить его повторный выбор, или можем вернуть выбранный элемент во множество A, и тем самым разрешить его повторный выбор.

Соответственно будем говорить о выборке без повторений и выборке с повторениями.

Пример

Рассмотрим множество $A = \{a; b; c; d; e; f\}$ из 6 элементов. Примеры выборок:

1) неупорядоченная $(6, 2)$-выборка без повторений $\{b; e\}$;
2) упорядоченная $(6, 3)$-выборка без повторений (a, c, d);
3) неупорядоченная $(6, 5)$-выборка с повторениями $\{c; e; e; f; f\}$;
4) упорядоченная $(6, 4)$-выборка с повторениями (b, c, c, f);

Заметим, что $(a, b, c) \neq (a, c, b)$, $\{a; b; c\} = \{a; c; b\}$.

Определение

Перестановкой n элементов называется упорядоченная (n, n)-выборка без повторений.

Пример

Всевозможные перестановки элементов множества $\{1; 2; 3\}$ имеют следующий вид:

$$(1,2,3),\ (1,3,2),\ (2,1,3),\ (2,3,1),\ (3,1,2),\ (3,2,1).$$

Определение

Размещением из n элементов по m называется упорядоченная (n, m)-выборка.

Определение

Сочетанием из n элементов по m называется неупорядоченная (n, m)-выборка.

Для размещений и сочетаний можно дать следующую интерпретацию.

Пусть есть n различных предметов и m различных корзин. Необходимо разместить по одному предмету во все корзины.

Каждое такое размещение есть упорядоченная (n, m)-выборка, то есть размещение из n по m.

Пусть необходимо выбрать m предметов и поместить их в одну корзину.

Каждый такой выбор есть сочетание из n по m.

Обозначим:

P_n – число перестановок n элементов;
A_n^m – число размещений из n элементов по m без повторений;
$\overline{A}_n^m$ – число размещений из n элементов по m с повторениями;
C_n^m – число сочетаний из n элементов по m без повторений;
$\overline{C}_n^m$ – число сочетаний из n элементов по m с повторениями.

Теорема

Справедливы формулы:

$$P_n = n!,$$
$$A_n^m = \frac{n!}{(n-m)!}, \quad \overline{A}_n^m = n^m,$$
$$C_n^m = \frac{n!}{(n-m)!m!}, \quad \overline{C}_n^m = \frac{(n+m-1)!}{m!(n-1)!}.$$

Доказательство.

При построении размещений без повторений первый элемент размещения можем выбрать n способами, второй $n-1$ способами, последний $n-m+1$ способами.
Выбор осуществляется последовательно. Таким образом, по правилу произведения

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

Перестановки – это размещения без повторений в случае $m = n$.
Поэтому

$$P_n = A_n^n = n!$$

Сочетания без повторений – это неупорядоченные (n, m)-выборки. Из каждого сочетания можно получить $m!$ размещений с помощью перестановки элементов сочетания.
Поэтому справедливо соотношение $C_n^m m! = A_n^m$, из которого получим

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

При построении размещений с повторениями первый элемент размещения можем выбрать n способами, второй и последующие также n способами. Поэтому по правилу произведения

$$\overline{A}_n^m = \underbrace{nn\cdots n}_{m} = n^m.$$

Рассмотрим сочетания с повторениями. Пусть

$$A = \{a_1; a_2; \ldots; a_n\}.$$

Каждая неупорядоченная выборка с повторениями может быть записана в следующем виде

$$\{\underbrace{a_1; \ldots; a_1}_{k_1}; \underbrace{a_2; \ldots; a_2}_{k_2}; \ldots; \underbrace{a_n; \ldots; a_n}_{k_n}\},$$

где k_i – число вхождений элемента a_i в выборку, $k_1 + \cdots + k_n = m$.

Выборку можно закодировать булевым вектором

$$(\underbrace{1, \ldots, 1}_{k_1}, 0, \underbrace{1, \ldots, 1}_{k_2}, 0, \ldots, \underbrace{1, \ldots, 1}_{k_n}).$$

где 0 выполняет роль разделителя.
Таким образом, число выборок равно числу булевых векторов длины $n+m-1$, содержащих ровно m единиц, и равно

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

□

Для факториала справедлива формула Стирлинга

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

которая находит применение в оценке сложности алгоритмов.

Из формулы Стирлинга следует, что $n!$ растет быстрее, чем 2^n

$$\lim_{n\to\infty} \frac{n!}{2^n} = \infty.$$

Пример

Сколько различных пятизначных чисел можно составить из цифр 1, 2, 3, 4, 5, если все цифры в этих числах различны?
Составим первое число 12345. Все остальные числа получим перестановкой цифр этого числа.
Всего будет 5!=120 различных чисел.

Пример

В студенческой группе из 25 человек необходимо выбрать старосту и профорга. Сколькими способами можно сделать этот выбор?
Задача заключается в размещении без повторения 2-х элементов из 25. Число размещений равно

$$A_{25}^2 = \frac{25!}{23!} = 600.$$

Пример

Сколько существует различных булевых векторов длины 8, содержащих ровно 3 единицы?
Ответом является число сочетаний из 8 по 3 без повторений

$$C_8^3 = \frac{8!}{5!3!} = 56.$$

Пример

Сколькими способами можно распределить k одинаковых предметов по n различным корзинам?
Для каждого предмета выбираем корзину. Таким образом, формируем неупорядоченные выборки из n по k с повторениями. Число таких выборок равно $\overline{C}_n^k$.

Пусть множество A с n элементами содержит повторяющиеся элементы m типов. Например, множество цифр числа 732773 содержит элементы трёх типов $\{7; 3; 2\}$. Обозначим через k_i число элементов i-го типа, $i = 1, \ldots, m$, $k_1 + \cdots + k_m = n$. Сколько можно получить различных перестановок элементов множества A?

Перестановка повторяющихся элементов не приводит к новым перестановкам. Поэтому число перестановок элементов множества с повторяющимися элементами будет равно

$$P_{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\cdots k_m!}.$$

Пример

Сколько различных слов можно получить из слова «информатика», переставляя буквы в этом слове?
Всего букв в слове 11. Буквы «и, а» встречаются дважды.
Следовательно, число различных слов будет равно

$$\frac{11!}{2!2!} = 9979200.$$

Пусть A конечное множество, $|A| = n$. Зададим целые положительные числа $k_1, \ldots, k_m$ такие, что

$$k_1 + \cdots + k_m = n.$$

Теорема

Число разбиений множества A на m непересекающихся подмножеств

$$A = \bigcup_{i=1}^{m} A_i, \quad A_i \cap A_j = \emptyset, \quad i \neq j, \quad |A_i| = k_i$$

равно

$$C_n^{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\cdots k_m!}.$$

Доказательство.

Сначала построим первое подмножество как неупорядоченную (n, k_1)-выборку без повторений. Это можно сделать $C_n^{k_1}$ способами.
Затем построим второе подмножество. Для этого необходимо выбрать k_2 элементов из оставшихся $n - k_1$. Это можно сделать $C_{n-k_1}^{k_2}$ способами.
И так далее, пока не останутся последние k_m элементов. По правилу произведения получим

$$C_n^{k_1,k_2,\ldots,k_m} = C_n^{k_1} C_{n-k_1}^{k_2} \cdots C_{n-k_1-\cdots-k_{m-2}}^{k_{m-1}} =$$
$$= \frac{n!}{(n-k_1)!k_1!} \cdot \frac{(n-k_1)!}{(n-k_1-k_2)!k_2!} \cdots \frac{(n-k_1-\cdots-k_{m-2})!}{(n-k_1-\cdots-k_{m-1})!k_{m-1}!} =$$
$$= \frac{n!}{k_1!k_2!\ldots k_m!}.$$

□

Пример

Сколькими способами можно сформировать две подгруппы из группы студентов в 25 человек, если в одной подгруппе будет 12 студентов, во второй – 13?
Это можно сделать

$$C_{25}^{12,13} = \frac{25!}{12!13!} = 5200300$$

способами.

2.3 Биномиальные коэффициенты

Определение

Числа

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

называются биномиальными коэффициентами.

Теорема

Справедливы формулы:

1) $C_n^0 = C_n^n = 1$,
2) $C_n^m = C_n^{n-m}$,
3) $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$,
4) $C_n^m C_m^k = C_n^k C_{n-k}^{m-k}$.

Доказательство.

Докажем, например, 3. Сумма коэффициентов C_{n-1}^m и C_{n-1}^{m-1} равна

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

□

Формулу

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

можно использовать для последовательного вычисления биномиальных коэффициентов.

Результаты вычислений образуют треугольник Паскаля

$$\begin{array}{ccccccccc} & & & & C_0^0 & & & & \\ & & & C_1^0 & & C_1^1 & & & \\ & & C_2^0 & & C_2^1 & & C_2^2 & & \\ & C_3^0 & & C_3^1 & & C_3^2 & & C_3^3 & \\ C_4^0 & & C_4^1 & & C_4^2 & & C_4^3 & & C_4^4 \end{array}$$

Каждый из внутренних элементов треугольника равен сумме двух элементов, расположенных над ним

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

Биномиальные коэффициенты входят в формулу, которая получила название формулы бинома Ньютона.

Теорема (Формула бинома Ньютона)

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Формулу бинома Ньютона получим как следствие полиномиальной формулы.

Теорема (Полиномиальная формула)

$$(x_1 + \cdots + x_m)^n = \sum_{\substack{k_1+\cdots+k_m=n \\ k_1,\ldots,k_m \geq 0}} C_n^{k_1,\ldots,k_m} x_1^{k_1} \ldots x_m^{k_m}.$$

Доказательство.

Рассматриваемое выражение запишем в виде произведения n скобок

$$(x_1 + \cdots + x_m)^n = (x_1 + \cdots + x_m) \cdots (x_1 + \cdots + x_m).$$

При раскрытии скобок получим m^n слагаемых следующего вида $x_{i_1} \cdots x_{i_n}$, которые могут содержать повторяющиеся переменные. Пусть число повторений переменных $x_1, \ldots, x_m$ равно соответственно $k_1, \ldots, k_m$. Тогда

$$x_{i_1} \ldots x_{i_n} = x_1^{k_1} \ldots x_m^{k_m}, \quad k_1 + \cdots + k_m = n.$$

Число таких слагаемых равно числу перестановок с повторениями

$$P_{k_1,\ldots,k_m} = C_n^{k_1,\ldots,k_m}.$$

□

При $m = 2$ полиномиальная формула принимает вид формулы бинома Ньютона.

Как следствие формулы бинома Ньютона получим

$$2^n = (1+1)^n = \sum_{k=0}^{n} C_n^k, \quad 0 = (-1+1)^n = \sum_{k=0}^{n} (-1)^k C_n^k.$$

Пример

Записать функцию $(x+1)^5$ в виде полинома. Применим формулу бинома Ньютона. Получим

$$(x+1)^5 = \sum_{k=0}^{5} C_n^k x^k = 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5.$$

2.4 Метод включений и исключений

Теорема

Пусть A конечное множество и $|A| = n$. Пусть заданы некоторые свойства $p_1, \ldots, p_m$ элементов множества A. Обозначим число элементов множества A, обладающих свойствами $p_{i_1}, \ldots, p_{i_k}$, через $N(p_{i_1}, \ldots, p_{i_k})$. Тогда число элементов множества A, не обладающих ни одним из свойств $p_1, \ldots, p_m$, равно

$$N(\overline{p}_1, \ldots, \overline{p}_m) = n - \left(\sum_{1 \le i \le m} N(p_i) - \sum_{1 \le i < j \le m} N(p_i, p_j) + \cdots + (-1)^{m-1} N(p_1, \ldots, p_m) \right).$$

Доказательство.

Обозначим через A_i подмножество элементов множества A, обладающих свойством p_i.
Тогда $\overline{A}_i = A \setminus A_i$ есть подмножество элементов, которые не обладают свойством p_i.
Пересечение этих подмножеств

$$\bigcap_{i=1}^{m} \overline{A}_i$$

есть подмножество элементов, которые не обладают ни одним из свойств $p_1, \ldots, p_m$.

Из формулы включения-исключения следует

$$\left| \bigcap_{i=1}^{m} \overline{A}_i \right| = |A| - \left(\sum_{1 \le i \le m} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{m-1} |A_1 \cap \cdots \cap A_m| \right).$$

В этом соотношении

$$\left| \bigcap_{i=1}^{m} \overline{A}_i \right| = N(\overline{p}_1, \ldots, \overline{p}_m), \quad |A| = n, \quad |A_i| = N(p_i),$$
$$|A_i \cap A_j| = N(p_i, p_j), \quad \ldots, \quad |A_1 \cap \cdots \cap A_m| = N(p_1, \ldots, p_m).$$

□

Пример

В компании производителя программного обеспечения работают 50 человек.
Из числа сотрудников компании 20 ведут разработки на языке программирования C++,
19 – на языке Java,
16 – на языке PHP,
12 – на C++ и Java,
8 – на C++ и PHP,
10 – на Java и PHP,
5 – на C++, Java и PHP.
Сколько сотрудников не используют в своей работе ни один из указанных языков программирования?

Обозначим свойства сотрудников:

- p_1 – сотрудник использует в своей работе язык программирования C++;
- p_2 – сотрудник использует в своей работе язык программирования Java;
- p_3 – сотрудник использует в своей работе язык программирования PHP.

По методу включений и исключений

$$\begin{aligned} N(\overline{p}_1, \overline{p}_2, \overline{p}_3) =& n - (N(p_1) + N(p_2) + N(p_3) - \\ & - N(p_1, p_2) - N(p_1, p_3) - N(p_2, p_3) + N(p_1, p_2, p_3)) = \\ =& 50 - (20 + 19 + 16 - 12 - 8 - 10 + 5) = 20. \end{aligned}$$

Пример

Сколько натуральных чисел от 1 до 100 не делятся ни на 2, ни на 3, ни на 5?
Обозначим свойства чисел:

- p_1 – число делится на 2;
- p_2 – число делится на 3;
- p_3 – число делится на 5.

Пусть $[a]$ есть целая часть числа. Тогда

$$N(p_1) = \frac{100}{2} = 50, \quad N(p_2) = \left[\frac{100}{3}\right] = 33, \quad N(p_3) = \frac{100}{5} = 20,$$
$$N(p_1, p_2) = \left[\frac{100}{2 \cdot 3}\right] = 16, \quad N(p_1, p_3) = \frac{100}{2 \cdot 5} = 10,$$
$$N(p_2, p_3) = \left[\frac{100}{3 \cdot 5}\right] = 6, \quad N(p_1, p_2, p_3) = \left[\frac{100}{2 \cdot 3 \cdot 5}\right] = 3.$$

Следовательно,

$$\begin{aligned} N(\overline{p}_1, \overline{p}_2, \overline{p}_3) =& n - (N(p_1) + N(p_2) + N(p_3) - \\ & - N(p_1, p_2) - N(p_1, p_3) - N(p_2, p_3) + N(p_1, p_2, p_3)) = \\ =& 100 - (50 + 33 + 20 - 16 - 10 - 6 + 3) = 26. \end{aligned}$$

2.5 Число беспорядков

Определение

Рассмотрим множество $A = \{a_1; \ldots; a_n\}$. Беспорядком называется любая перестановка элементов множества A

$$(a_{i_1}, \ldots, a_{i_n}),$$

в которой ни какой из элементов не находится на своем месте, $i_j \neq j$. Число беспорядков называют субфакториалом и обозначают $!n$.

Пример

Беспорядки множества $\{1; 2; 3\}$ имеют вид

$$(2, 3, 1), \quad (3; 1; 2).$$

Теорема

Число беспорядков множества из n элементов равно

$$!n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right).$$

Доказательство.

Число беспорядков можно определить, применяя метод включений и исключений. Обозначим через p_i свойство перестановки – элемент a_i расположен на своем месте. Тогда

$$N(p_i) = (n-1)!, \quad N(p_i, p_j) = (n-2)!, \quad \ldots, \quad N(p_1, \ldots, p_n) = 0! = 1.$$

Следовательно,

$$\sum_{1 \leq i \leq n} N(p_i) = C_n^1 (n-1)!, \quad \sum_{1 \leq i < j \leq n} N(p_i, p_j) = C_n^2 (n-2)!, \quad \ldots$$

Искомое значение субфакториала

$$!n = N(\overline{p}_1, \ldots, \overline{p}_n).$$

Всего различных перестановок $n!$. Согласно методу включений и исключений

$$\begin{aligned} !n &= n! - C_n^1 (n-1)! + C_n^2 (n-2)! - \cdots + (-1)^n C_n^n 0! = \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!} = \\ &= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right). \end{aligned}$$

□

Для субфакториала справедливо рекуррентное соотношение

$$!n = !(n-1)n + (-1)^n, \quad !1 = 0.$$

На основе методов математического анализа доказывается, что $!n$ есть ближайшее целое к числу $n!/e$ или целая часть числа $(n! + 1)/e$.

Пример

Есть n писем и n конвертов. Письма случайным образом размещаются в конверты. Какова вероятность, что по крайней мере одно письмо попадёт в свой конверт?
Эта вероятность равна

$$1 - \frac{!n}{n!} \approx 1 - \frac{1}{e} \approx 0,63212.$$

2.6 Число функций

Теорема

Пусть $|A| = m$, $|B| = n$. Число всех функций $f : A \to B$ равно n^m.

Доказательство.

Каждая функция есть упорядоченная (n, m)-выборка с повторениями из элементов множества B. Следовательно, число функций равно числу размещений с повторениями

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

□

Теорема

Пусть $|A| = |B| = n$. Число всех биекций $f : A \leftrightarrow B$ равно $n!$.

Доказательство.

Каждая биекция есть перестановка элементов множества B. Следовательно, число биекций равно $n!$. □

Теорема

Пусть $|A| = m$, $|B| = n$, $m \le n$. Число всех инъекций $f : A \to B$ равно A_n^m.

Доказательство.

Каждая инъекция есть упорядоченная (n, m)-выборка без повторений из элементов множества B. Следовательно, число инъекций равно числу размещений без повторений

$$A_n^m = \frac{n!}{(n-m)!}.$$

□

Теорема

Пусть $|A| = m$, $|B| = n$, $m \ge n$. Число всех сюръекций $f : A \to B$ равно

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

Доказательство.

Пусть F – множество всех функций $f : A \to B$. Множество сюръекций

$$F_s = \{f \in F | \ \forall y \in B \ \exists x \in A : y = f(x)\}.$$

Обозначим

$$B = \{y_1; \ldots; y_n\}, \quad F_i = \{f \in F |\ y_i \notin f(A)\}.$$

Тогда

$$F_s = \bigcap_{i=1}^{n} \overline{F_i}, \quad \overline{F_i} = F \setminus F_i.$$

Следовательно, по методу включений и исключений

$$|F_s| = \left|\bigcap_{i=1}^{n} \overline{F_i}\right| = |F| - \left(\sum_{1 \le i \le n} |F_i| - \sum_{1 \le i < j \le n} |F_i \cap F_j| + \right.$$
$$\left. + \sum_{1 \le i < j < k \le n} |F_i \cap F_j \cap F_k| - \cdots + (-1)^{n-1} |F_1 \cap \cdots \cap F_n| \right).$$

Учитывая, что

$$|F| = n^m, \quad |F_i| = (n-1)^m, \quad |F_i \cap F_j| = (n-2)^m, \quad \ldots,$$

получим

$$|F_s| = C_n^0 n^m - C_n^1 (n-1)^m + C_n^2 (n-2)^m - \cdots =$$
$$= \sum_{k=0}^{n-1} (-1)^k C_n^k (n-k)^m.$$

□

Пример

Сколькими способами можно разместить 5 различных марок в 3 различных конверта, если в каждом конверте должна быть по крайне мере одна марка?
Для решения этой задачи применим теорему о числе сюръекций. В данном случае $m = 5$, $n = 3$. Следовательно, число способов размещения марок равно

$$C_3^0 3^5 - C_3^1 2^5 + C_3^2 1^5 = 150.$$

Тема 3. Алгебра логики

3.1 Логические операции

Определение

Высказывание – это повествовательное утверждение, относительно которого можно однозначно сказать, что оно является истинным или ложным.

Пример

Утверждение «Площадь круга равна πR^2, где R – радиус круга» является высказыванием.
Утверждение «Это утверждение ложно» высказыванием не является, т.к. оно логически противоречиво. Относительно данного утверждения нельзя сказать, что оно является истинным или ложным.

Из заданного множества высказываний можно получить новые высказывания, применяя логические связки – логические операции: «и», «или», «если, то», «тогда и только тогда, когда» и др.

Множество высказываний и множество логических операций над высказываниями образуют алгебру высказываний – алгебру логики.

Пусть A и B два произвольных высказывания.

Определение

Операция «и», логическое умножение, конъюнкция, обозначается: AB, $A \wedge B$, $A\&B$. Высказывание $A \wedge B$ является истинным тогда и только тогда, когда истинными являются высказывания A и B.

Определение

Операция «или», логическое сложение, дизъюнкция, обозначается: $A + B$, $A \vee B$, $A!B$. Высказывание $A \vee B$ является ложным тогда и только тогда, когда оба высказывания A и B являются ложными.

Определение

Операция «отрицание», «не», «инверсия», обозначается $\neg A$, $\bar{B}$. Высказывание $\bar{A}$ является истинным, если A ложно, и является ложным, если A истинно.

Определение

Операция «следование», «импликация», обозначается $A \to B$, $A \Rightarrow B$. Высказывание $A \to B$ является ложным тогда и только тогда, когда A истинно, а B ложно.

Определение

Операция «эквивалентность», обозначается $A \sim B$, $A \Leftrightarrow B$. Высказывание $A \sim B$ является истинным тогда и только тогда, когда A и B оба истинны или оба ложны.

Таблицы истинности основных логических операций:

A	B	$A \wedge B$
и	и	и
и	л	л
л	и	л
л	л	л

A	B	$A \vee B$
и	и	и
и	л	и
л	и	и
л	л	л

A	B	$A \to B$
и	и	и
и	л	л
л	и	и
л	л	и

A	B	$A \sim B$
и	и	и
и	л	л
л	и	л
л	л	и

A	$\bar{A}$
и	л
л	и

Соответствие логических операций и теоретико-множественных операций:

Высказывания	Множества
$A \wedge B$	$A \cap B$
$A \vee B$	$A \cup B$
$A \to B$	$A \subseteq B$
$A \sim B$	$A = B$
$\bar{A}$	$\bar{A}$

3.2 Булевы функции

Сложные высказывания записываются в виде формул алгебры высказываний. Например,

$$A \vee B \to C, \quad \overline{(A \to B) \vee C} \sim (A \wedge B).$$

Пример

Определим высказывания:

$$A : x < y, \quad B : y < z, \quad C : x < z.$$

Тогда сложное высказывание «Если $x < y$ и $y < z$, то $x < z$» можно записать в виде формулы алгебры высказываний

$$A \wedge B \to C.$$

Формулы алгебры высказываний есть логические (булевы) функции. Значения и аргументы этих функций принимают только два значения: «и» и «л». Эти логические константы обозначают соответственно 1 и 0.

Определение

Булева функция n аргументов $f(x_1, x_2, \ldots, x_n)$ есть функция

$$f : E^n \to E,$$

где $E = \{0; 1\}$.

Существует 2^n различных булевых векторов размера n. Булева функция каждому булеву вектору ставит в соответствие 0 или 1. Поэтому существует

$$2^{2^n}$$

различных булевых функций. При $n = 2$ число различных булевых функций равно 16.

Основные булевы функции двух аргументов:

$x_1 \wedge x_2$ – конъюнкция

$x_1 \vee x_2$ – дизъюнкция

$x_1 \to x_2$ – импликация

$x_1 \leftarrow x_2$ – обратная импликация

$x_1 \sim x_2$ – эквивалентность

$x_1 \oplus x_2$ – сумма по модулю 2 (отрицание эквивалентности, исключающее или)

$x_1|x_2$ – штрих Шеффера (отрицание конъюнкции, «не-и»)

$x_1 \downarrow x_2$ – стрелка Пирса (отрицание дизъюнкции, «не-или»)

Таблицы истинности основных булевых функций двух аргументов:

x_1	x_2	$x_1 \to x_2$	$x_1 \leftarrow x_2$	$x_1 \sim x_2$	$x_1 \oplus x_2$	$x_1 \mid x_2$	$x_1 \downarrow x_2$
0	0	1	1	1	0	1	1
0	1	1	0	0	1	1	0
1	0	0	1	0	1	1	0
1	1	1	1	1	0	0	0

Булеву функцию можно задать:

1) в виде формулы;
2) в виде таблицы значений;
3) в виде вектора значений;
4) в виде множества номеров наборов значений переменных, на которых функция принимает значение 1.

При заполнении таблицы значений булевой функции наборы значений переменных пронумеруем от 0 до $2^n - 1$. Значения переменных есть цифры двоичной записи этих номеров.

Пример

Мажоритарная функция (функция голосования) принимает значение 1, если более половины переменных имеют значение 1, иначе значение функции равно 0.
Мажоритарную функцию можно записать в виде формулы. При $n = 3$ получим

$$f(x_1, x_2, x_3) = x_1 \wedge x_2 \vee x_1 \wedge x_3 \vee x_2 \wedge x_3,$$
$$f(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3.$$

Таблица значений мажоритарной функции

	x_1	x_2	x_3	f
0	0	0	0	0
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	1
6	1	1	0	1
7	1	1	1	1

Вектор значений мажоритарной функции

$$f = (00010111).$$

Множество номеров наборов переменных, на которых мажоритарная функция принимает значение 1,

$$f = \{3; 5; 6; 7\}$$

Определение

Переменная x_i называется фиктивной переменной булевой функции $f(x_1, \ldots, x_n)$, если

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

для всех наборов значений переменных $\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\}$.
Иначе переменная называется существенной.

Фиктивные переменные можно удалить из булевой функции и тем самым уменьшить число переменных.

Пример

Рассмотрим булеву функцию трёх переменных

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Переменные x, z являются существенными. Переменная y фиктивная.

Удалим переменную y из таблицы. Получим функцию $g(x,z)$ с таблицей значений

x	z	$g(x,z)$
0	0	0
0	1	1
1	0	1
1	1	0

Отметим, что $g(x,z) = x \oplus z$.

Определение

Две формулы алгебры высказываний называются равносильными, если соответствующие булевы функции совпадают.

Равносильные формулы (законы алгебры логики):

$\bar{\bar{x}} = x$	Снятие двойного отрицания
$x \wedge y = y \wedge x$	Коммутативность конъюнкции
$x \vee y = y \vee x$	Коммутативность дизъюнкции
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	Ассоциативность конъюнкции
$(x \vee y) \vee z = x \vee (y \vee z)$	Ассоциативность дизъюнкции
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	Дистрибутивность конъюнкции относительно дизъюнкции
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	Дистрибутивность дизъюнкции относительно конъюнкции
$x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$	Законы поглощения
$\overline{x \vee y} = \bar{x} \wedge \bar{y}$, $\overline{x \wedge y} = \bar{x} \vee \bar{y}$	Законы де Моргана
$x \vee \bar{x} = 1$	Закон исключенного третьего
$x \wedge \bar{x} = 0$	Закон противоречия
$x \wedge x = x, \quad x \vee x = x$	Идемпотентность
$x \wedge 1 = x, \quad x \vee 0 = x$	Свойства констант

Доказать справедливость законов алгебры логики можно на основе таблиц истинности соответствующих функций.

Например, для закона де Моргана

$$\overline{x \vee y} = \bar{x} \wedge \bar{y}$$

получим следующую таблицу

x	y	$x \vee y$	$\overline{x \vee y}$	$\bar{x}$	$\bar{y}$	$\bar{x} \wedge \bar{y}$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

С помощью законов алгебры логики можно выполнять преобразования булевых функций.

Пример

Рассмотрим булеву функцию $f(x,y) = \overline{x \vee \bar{y}} \vee x$. Применяя законы де Моргана, дистрибутивности, исключенного третьего, коммутативности, получим

$$f(x,y) = (\bar{x} \wedge y) \vee x = (\bar{x} \vee x) \wedge (y \vee x) = 1 \wedge (x \vee y) = x \vee y.$$

3.3 Классы булевых функций

Все множество булевых функций $f(x_1, \ldots, x_n)$ обозначим через P_2. Число переменных может быть любым.

Определение

Суперпозицией двух булевых функций

$$f(x_1, \ldots, x_k, \ldots, x_n), \quad g(y_1, \ldots, y_m)$$

называется булева функция

$$f(x_1, \ldots, x_{k-1}, g(y_1, \ldots, y_m), x_{k+1}, \ldots, x_n).$$

Пример

Пусть $f(x_1, x_2) = x_1 \wedge x_2$, $g(x_1, x_2) = x_1 \oplus x_2$. Тогда

$$f(g(x_1, x_2), x_2) = (x_1 \oplus x_2) \wedge x_2, \quad g(f(x_1, x_2), x_2) = (x_1 \wedge x_2) \oplus x_2.$$

Определение

Замыканием множества булевых функций $F \subseteq P_2$ называется множество $[F]$ всех булевых функций, получаемых из F с помощью операции суперпозиции.

Определение

Множество булевых функций F называется замкнутым, если $[F] = F$.

Определение

Система булевых функций

$$F = \{f_1; \ldots; f_m\}$$

называется функционально полной, если $[F] = P_2$.

Следующие классы булевых функций будем называть основными.

Определение

Булева функция f сохраняет константу 0, если

$$f(0, \ldots, 0) = 0.$$

Класс булевых функций, сохраняющих константу 0, обозначим через K_0.

Определение

Булева функция f сохраняет константу 1, если

$$f(1, \ldots, 1) = 1.$$

Класс булевых функций, сохраняющих константу 1, обозначим через K_1.

Определение

Функция $\overline{f(\bar{x}_1, \ldots, \bar{x}_n)}$ называется двойственной к функции f и обозначается f^*.

Пример

Двойственной для конъюнкции является дизъюнкция

$$\overline{\bar{x}_1 \wedge \bar{x}_2} = x_1 \vee x_2.$$

Определение

Булева функция f называется самодвойственной, если $f = f^*$. Класс самодвойственных функций обозначим через S.

Определение

Булева функция f называется линейной, если она может быть записана в следующем виде

$$f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus c_2 x_2 \oplus \cdots \oplus c_n x_n,$$

где $c_i \in \{0; 1\}$. Множество всех линейных функций обозначим через L.

Пример

Эквивалентность является линейной функцией

$$x_1 \sim x_2 = 1 \oplus x_1 \oplus x_2.$$

Пусть $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ – два булевых вектора длины n. Будем говорить, что $x \geq y$, если $x_i \geq y_i$, $i = 1, \ldots, n$. В противном случае x и y несравнимы.

Определение

Булева функция f называется монотонной, если для любых $x \geq y$ выполняется неравенство $f(x) \geq f(y)$. Множество всех монотонных функций обозначим через M.

Теорема

Классы булевых функций K_0, K_1, S, L, M и все множество булевых функций P_2 замкнуты.

Доказательство.

Докажем $[S] = S$. Пусть $f, g \in S$. Тогда

$$\begin{aligned}
&\overline{f(\bar{x}_1, \ldots, g(\bar{y}_1, \ldots, \bar{y}_m), \ldots, \bar{x}_n)} = \\
&f(x_1, \ldots, \overline{g(\bar{y}_1, \ldots, \bar{y}_m)}, \ldots, x_n) = \\
&f(x_1, \ldots, g(y_1, \ldots, y_m), \ldots, x_n).
\end{aligned}$$

□

Теорема (теорема Поста)

Система булевых функций F является функционально полной тогда и только тогда, когда для любого класса $K \in \{K_0; K_1; S; L; M\}$ найдется функция $f \in F$ такая, что $f \notin K$.

Таблица принадлежности булевых функций классам K_0, K_1, S, L, M

Функция	K_0	K_1	S	L	M
$\bar{x}$	−	−	+	+	−
$x_1 \wedge x_2$	+	+	−	−	+
$x_1 \vee x_2$	+	+	−	−	+
$x_1 \to x_2$	−	+	−	−	−
$x_1 \sim x_2$	−	+	−	+	−
$x_1 \oplus x_2$	+	−	−	+	−

Из таблицы видно, что системы булевых функций: $\{\bar{x}, x_1 \wedge x_2\}$, $\{\bar{x}, x_1 \vee x_2\}$ являются функционально полными.

3.4 Нормальные формы булевых функций

Рассмотрим множество булевых функций n переменных $x_1, \ldots, x_n$.

Обозначим: $x_i \wedge x_j = x_i x_j$, $x_i^1 = x_i$, $x_i^0 = \bar{x}_i$.

Под литералом будем понимать x_i или $\bar{x}_i$.

Определение

Элементарной конъюнкцией называется конъюнкция литералов

$$x_{i_1}^{\sigma_1} \ldots x_{i_m}^{\sigma_m}, \quad m \leq n,$$

где $\sigma_i \in \{0; 1\}$.

Например, элементарными конъюнкциями являются

$$x_1 x_3, \quad x_2 x_3 \bar{x}_4.$$

Элементарная конъюнкция равна 1 только на наборе значений аргументов $x_{i_1} = \sigma_1, \ldots, x_{i_m} = \sigma_m$.

Определение

При $m = n$ элементарная конъюнкция называется конституентой единицы.

Определение

Дизъюнкция элементарных конъюнкций называется дизъюнктивной нормальной формой (ДНФ).

Определение

Дизъюнкция конституент единицы называется совершенной дизъюнктивной нормальной формой (СДНФ).

Теорема

Любую булеву функцию, кроме константы 0, можно записать в виде ДНФ.

Доказательство.

Справедливо представление булевой функции в виде СДНФ

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

□

Пример

Функция задана таблицей значений

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

Запишем СДНФ

$$f(x_1,x_2,x_3) = \bar{x}_1x_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1\bar{x}_2x_3 \vee x_1x_2x_3.$$

Применяя законы алгебры логики, получим ДНФ

$$f(x_1,x_2,x_3) = \bar{x}_1x_2 \vee x_1x_3.$$

Определение

Элементарной дизъюнкцией называется дизъюнкция

$$x_{i_1}^{\sigma_1} \vee \cdots \vee x_{i_m}^{\sigma_m}, \quad m \le n$$

где $\sigma_i \in \{0;1\}$.

Элементарная дизъюнкция равна 0 только на наборе значений аргументов $x_{i_1} = \bar{\sigma}_1, \ldots, x_{i_m} = \bar{\sigma}_m$.

Определение

При $m = n$ элементарная дизъюнкция называется конституентой нуля.

Определение

Конъюнкция элементарных дизъюнкций называется конъюнктивной нормальной формой (КНФ).

Определение

Конъюнкция конституент нуля называется совершенной конъюнктивной нормальной формой (СКНФ).

Теорема

Любую булеву функцию, кроме константы 1, можно записать в виде КНФ.

Доказательство.

Справедливо представление в виде СКНФ

$$f(x_1,\dots,x_n) = \bigwedge_{f(\sigma_1,\dots,\sigma_n)=0} x_1^{\bar{\sigma}_1} \vee \dots \vee x_n^{\bar{\sigma}_n}.$$

□

Пример

$$f(x_1,x_2,x_3) = (x_1 \vee x_2 \vee x_3)(x_1 \vee x_2 \vee \bar{x}_3)(\bar{x}_1 \vee x_2 \vee x_3)(\bar{x}_1 \vee \bar{x}_2 \vee x_3).$$

Определение

Сумма по модулю два элементарных конъюнкций называется бисуммарной нормальной формой (БНФ).

Определение

Сумма по модулю два конституент единицы называется совершенной бисуммарной нормальной формой (СБНФ).

Теорема

Любую булеву функцию, кроме константы 0, можно записать в виде БНФ

Доказательство.

Справедливо представление в виде СБНФ

$$f(x_1,\dots,x_n) = \bigoplus_{f(\sigma_1,\dots,\sigma_n)=1} x_1^{\sigma_1}\dots x_n^{\sigma_n}.$$

□

Пример

$$f(x_1,x_2,x_3) = \bar{x}_1x_2\bar{x}_3 \oplus \bar{x}_1x_2x_3 \oplus x_1\bar{x}_2x_3 \oplus x_1x_2x_3.$$

Функции $\{\oplus; \wedge; 0; 1\}$ образуют функционально полную систему функций.

Алгебра на множестве булевых переменных с операциями сложения по модулю два и конъюнкцией называют алгеброй Жегалкина.

Справедливы соотношения

$$x_1 \oplus x_2 = x_2 \oplus x_1, \quad x_1(x_2 \oplus x_3) = x_1x_2 \oplus x_1x_3$$
$$x \oplus x = 0, \quad x \oplus 0 = x, \quad \bar{x} = 1 \oplus x.$$

Любую булеву функцию можно представить в виде полинома Жегалкина. Для этого в СДНФ достаточно заменить $\bar{x}$ на $1 \oplus x$, операцию $\vee$ на $\oplus$.

Пример

$$f(x_1, x_2, x_3) = (1 \oplus x_1)x_2(1 \oplus x_3) \oplus (1 \oplus x_1)x_2x_3 \oplus x_1(1 \oplus x_2)x_3 \oplus x_1x_2x_3 =$$
$$= x_2 \oplus x_1x_2 \oplus x_1x_3.$$

3.5 Построение минимальных ДНФ

Определение

ДНФ булевой функции называется минимальной, если общее количество литералов в ней минимально.

Метод Квайна построения минимальной ДНФ.

Пусть булева функция задана в виде СДНФ. На первом этапе выполняем операции склеивания и поглощения

$$xy \vee \bar{x}y = (x \vee \bar{x})y = 1y = y,$$
$$x \vee xy = x(1 \vee y) = x1 = x.$$

В результате получаем сокращённую ДНФ. Элементарные конъюнкции сокращённой ДНФ называются импликантами.

На втором этапе составляем таблицу импликантов. Столбцы таблицы соответствуют конституентам единицы СДНФ, строки – импликантам сокращённой ДНФ.

Отмечаем вхождения импликантов в конституенты единицы. Выбираем наименьшее число импликант, дизъюнкция которых сохраняет все конституенты единицы. Получаем тупиковые ДНФ. Минимальная ДНФ выбирается из тупиковых ДНФ.

Пример

Пусть булева функция задана СДНФ

$$f(x_1, x_2, x_3) = x_1\bar{x}_2x_3 \vee \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2\bar{x}_3 \vee x_1x_2\bar{x}_3 \vee x_1x_2x_3 \vee \bar{x}_1\bar{x}_2x_3.$$

Построим таблицу склеивания

	$x_1\bar{x}_2x_3$	$\bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{x}_1x_2\bar{x}_3$	$x_1x_2\bar{x}_3$	$x_1x_2x_3$	$\bar{x}_1\bar{x}_2x_3$
$x_1\bar{x}_2x_3$	–				x_1x_3	$\bar{x}_2x_3$
$\bar{x}_1\bar{x}_2\bar{x}_3$		–	$\bar{x}_1\bar{x}_3$			$\bar{x}_1\bar{x}_2$
$\bar{x}_1x_2\bar{x}_3$			–	$x_2\bar{x}_3$		
$x_1x_2\bar{x}_3$				–	x_1x_2	
$x_1x_2x_3$					–	
$\bar{x}_1\bar{x}_2x_3$						–

Сокращённая ДНФ

$$f(x_1, x_2, x_3) = x_1x_3 \vee \bar{x}_2x_3 \vee \bar{x}_1\bar{x}_3 \vee \bar{x}_1\bar{x}_2 \vee x_2\bar{x}_3 \vee x_1x_2.$$

Построим таблицу импликантов

	$x_1\bar{x}_2x_3$	$\bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{x}_1x_2\bar{x}_3$	$x_1x_2\bar{x}_3$	$x_1x_2x_3$	$\bar{x}_1\bar{x}_2x_3$
x_1x_3	⊛				⊛	
$\bar{x}_2x_3$	*					*
$\bar{x}_1\bar{x}_3$		*	*			
$\bar{x}_1\bar{x}_2$		⊛				⊛
$x_2\bar{x}_3$			⊛	⊛		
x_1x_2				*	*	

Тупиковые ДНФ

$$f(x_1, x_2, x_3) = x_1x_3 \vee \bar{x}_1\bar{x}_2 \vee x_2\bar{x}_3,$$
$$f(x_1, x_2, x_3) = \bar{x}_2x_3 \vee \bar{x}_1\bar{x}_3 \vee x_1x_2$$

являются минимальными.

Метод карт Карно построения минимальной ДНФ.

Карта Карно – это преобразованная таблица значений булевой функции. Карта Карно для функции трёх переменных имеет следующий вид

$x_1 \diagdown x_2x_3$	11	10	00	01
1				
0				

Карта Карно для функции четырёх переменных

$x_1x_2 \diagdown x_3x_4$	10	11	01	00
10				
11				
01				
00				

В клетках ставятся 0 и 1, соответствующие значениям функции.

Единицы, расположенные в соседних клетках (по горизонтали и вертикали) могут склеиваться.

При этом карту можно свернуть по горизонтали и вертикали.

Для построения минимальной ДНФ необходимо найти наиболее рациональное покрытие единиц карты Карно.

Пример

Для функции

$$f(x_1, x_2, x_3) = x_1\bar{x}_2x_3 \vee \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2\bar{x}_3 \vee x_1x_2\bar{x}_3 \vee x_1x_2x_3 \vee \bar{x}_1\bar{x}_2x_3.$$

карта Карно имеет вид

$x_1 \diagdown x_2x_3$	11	10	00	01
1	1	1	0	1
0	0	1	1	1

Минимальные покрытия

$$f(x_1, x_2, x_3) = x_1x_2 \vee \bar{x}_1\bar{x}_3 \vee \bar{x}_2x_3,$$
$$f(x_1, x_2, x_3) = x_1x_3 \vee x_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2,$$

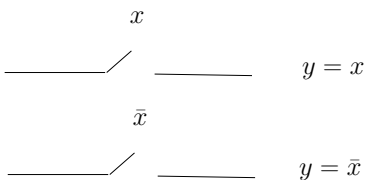
показаны на рисунке

$x_1 \diagdown x_2x_3$	11	10	00	01
1	1	1	0	1
0	0	1	1	1

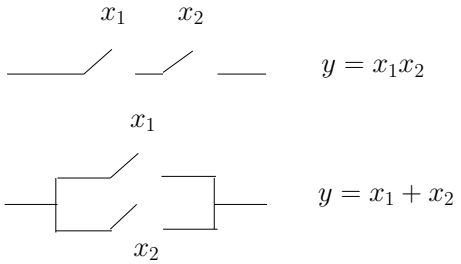
$x_1 \diagdown x_2x_3$	11	10	00	01
1	1	1	0	1
0	0	1	1	1

3.6 Контактные и функциональные схемы

Контактная схема представляет собой электрическую цепь, содержащую контакты двух типов: замыкающие и размыкающие.



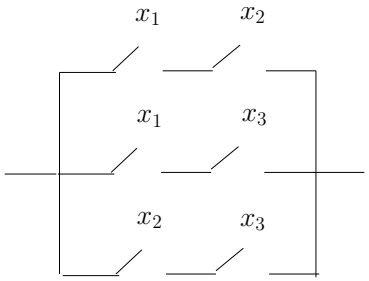
Последовательное соединение контактов описывается конъюнкцией, параллельное соединение – дизъюнкцией.



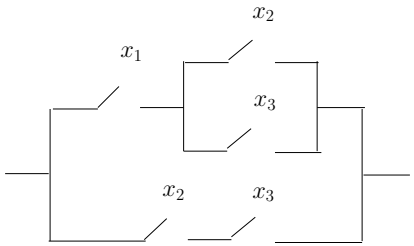
Любую контактную схему можно представить в виде последовательного и параллельного соединения контактов. Таким образом, любую контактную схему можно задать в виде ДНФ некоторой булевой функции.

Пример

Контактная схема мажоритарной функции $y = x_1x_2 + x_1x_3 + x_2x_3$.



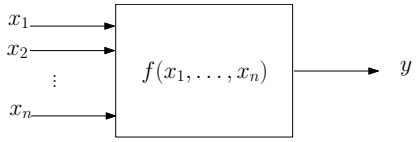
Эквивалентная схема



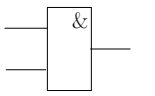
Этой схеме соответствует форма записи мажоритарной функции

$$y = x_1(x_2 + x_3) + x_2x_3.$$

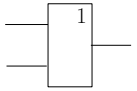
Функциональные (логические) схемы – это электронные устройства, поведение которых описывается булевыми функциями.



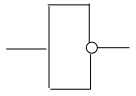
Основные логические элементы функциональных схем: конъюнктор, дизъюнктор, инвертор, штрих Шеффера, стрелка Пирса



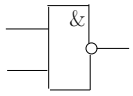
$y = x_1x_2$



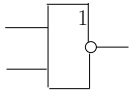
$y = x_1 + x_2$



$y = \bar{x}$

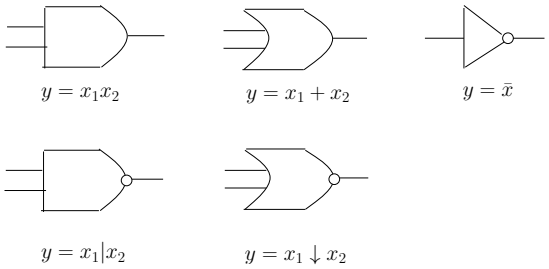


$y = x_1|x_2$



$y = x_1 \downarrow x_2$

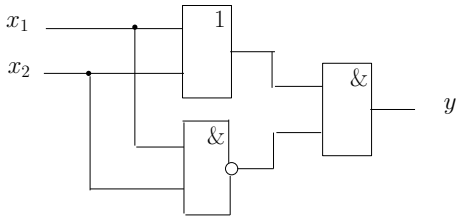
Международный стандарт обозначений логических элементов функциональных схем



Пример

Функциональная схема полусумматора

$$y = x_1 \oplus x_2 = (x_1 + x_2)\overline{x_1 x_2}$$



Тема 4. Алгебраические структуры

4.1 Основные понятия

Определение

Отображение

$$\alpha : A^n \to A$$

называется n-арной алгебраической операцией на множестве A.

Далее будем рассматривать бинарные алгебраические операции

$$\alpha : A^2 \to A.$$

Бинарную алгебраическую операцию будем обозначать:

$$a * b, \quad ab, \quad a + b, \quad a, b \in A.$$

Пример

Бинарными алгебраическими операциями являются:

- операции сложения $x + y$ и умножения xy на множестве действительных чисел R;
- операции объединения $A \cup B$ и пересечения $A \cap B$ множеств ;
- операции дизъюнкции $x \vee y$ и конъюнкции $x \wedge y$ на множестве $B = \{0; 1\}$;
- операция сложения векторов на плоскости $\vec{v} + \vec{u}$;
- операции сложения $a(x) + b(x)$ и умножения $a(x)b(x)$ полиномов с действительными коэффициентами

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$
$$b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m.$$

Определение

Множество A с заданными на нём алгебраическими операциями $\alpha_1, \ldots, \alpha_n$ называется алгебраической структурой и обозначается

$$\langle A; \alpha_1, \ldots, \alpha_n \rangle.$$

Пример

Множество квадратных матриц M_n заданной размерности n с операциями сложения и умножения образуют алгебраическую структуру $\langle M_n; +, \cdot \rangle$ с двумя алгебраическими операциями.

Определение

Алгебраическая структура называется конечной, если число её элементов конечно.

Конечную алгебраическую структуру

$$\langle A; * \rangle, \quad A = \{a_1; a_2; \ldots; a_n\},$$

с бинарной алгебраической операцией $*$ можно задать таблицей Кэли

$*$	a_1	$\ldots$	a_n
a_1	b_{11}	$\ldots$	b_{1n}
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	b_{n1}	$\ldots$	b_{nn}

где $b_{ij} = a_i * a_j \in A$.

Пример

На множестве $A = \{0; 1; 2\}$ задана бинарная алгебраическая операция $a + b \pmod 3$. Таблица Кэли для этой алгебраической структуры имеет следующий вид

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Определение

Бинарная алгебраическая операция, заданная на множестве A, называется коммутативной, если

$$\forall a, b \in A : ab = ba.$$

Называется ассоциативной, если

$$\forall a, b, c \in A : (ab)c = a(bc).$$

Пример

Операция сложения матриц коммутативна.
Операция умножения матриц не коммутативна.
Обе эти операции ассоциативные.

Под a^n понимается

$$a^n = \underbrace{aa \ldots a}_{n}.$$

Справедливы соотношения

$$a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}.$$

Если $ab = ba$, то $(ab)^n = a^n b^n$.

Определение

Элемент $e \in A$ такой, что

$$\forall a \in A : ae = ea = a$$

называется единичным (нейтральным). Единичный элемент будем также обозначать a^0.

Пример

В алгебраической структуре $\langle M_n; +, \cdot \rangle$ по отношению к операции сложения нейтральным элементом является нулевая матрица, по отношению к операции умножения нейтральным элементом является единичная матрица.

Единичный элемент, если существует, всегда единственный.

Пусть существуют два единичных элемента e_1 и e_2.

По определению единичного элемента

$$e_1 e_2 = e_1, \quad e_1 e_2 = e_2.$$

Следовательно, $e_1 = e_2 = e$.

Определение

Обратным для a называется элемент a^{-1} такой, что

$$aa^{-1} = a^{-1}a = e.$$

Пусть для элемента a существует обратный a^{-1}. Тогда

$$(a^n)^{-1} = (a^{-1})^n, \quad n \in N.$$

В дальнейшем $(a^{-1})^n$ будем обозначать a^{-n}.

Определение

Две алгебраические структуры

$$\langle A; \alpha_1, \ldots, \alpha_n \rangle \quad \text{и} \quad \langle B; \beta_1, \ldots, \beta_n \rangle$$

с бинарными алгебраическими операциями называются изоморфными, если существует биекция $f: A \leftrightarrow B$ такая, что

$$\forall a_1, a_2 \in A \; \forall \alpha_i : \; f(a_1 \alpha_i a_2) = f(a_1) \beta_i f(a_2).$$

Пример

Алгебраические структуры: $\langle B; \wedge \rangle$, $\langle B; \vee \rangle$, $B = \{0; 1\}$ изоморфны.
Биекцию $f: B \leftrightarrow B$ установим по правилу $f(x) = \bar{x}$.
Это означает, что $f(0) = 1, \quad f(1) = 0$.
Применяя закон де Моргана, получим

$$\forall x, y \in B : f(x \vee y) = \overline{x \vee y} = \bar{x} \wedge \bar{y} = f(x) \wedge f(y).$$

Следовательно, рассматриваемые алгебраические структуры изоморфны.

4.2 Группы

Определение

Алгебраическая структура $G = \langle A; \cdot \rangle$ с бинарной ассоциативной операцией называется полугруппой.

Определение

Алгебраическая структура $G = \langle A; \cdot \rangle$ с бинарной ассоциативной операцией называется группой, если в G существует единичный элемент и для для каждого элемента G существует обратный.

Коммутативную группу принято называть абелевой группой.

Определение

Группа называется конечной порядка n, если она содержит ровно n различных элементов.

Пример

Множество целых чисел относительно операции умножения образует полугруппу, относительно операции сложения образует абелеву группу.

Пример

Множество невырожденных квадратных матриц одной размерности образует группу относительно операции умножения.
Произведение двух невырожденных матриц AB – невырожденная матрица.
Единичным элементом является единичная матрица E.
Для каждой невырожденной матрицы существует обратная матрица A^{-1} такая, что $A^{-1}A = E$, $AA^{-1} = E$.
Данная группа не является абелевой. В общем случае, $AB \neq BA$.

Определение

Группа называется мультипликативной, если алгебраическая операция имеет смысл произведения. В мультипликативной группе алгебраическая операция обозначается «$\cdot$». Нейтральный элемент обозначается «1». Обратный элемент обозначается «a^{-1}».
Произведение n элементов $a \dots a$ обозначается «a^n ».

Определение

Группа называется аддитивной, если алгебраическая операция имеет смысл сложения. В аддитивной группе алгебраическая операция обозначается «$+$». Нейтральный элемент обозначается «0».
Обратный элемент называется противоположным и обозначается «$-a$». Сумма n элементов $a + \dots + a$ обозначается «na».

Теорема (Свойства группы)

Пусть G – группа. Тогда

1) *Для любого $a \in G$ обратный элемент a^{-1} является единственным.*
2) *Для любых $a, b \in G$ уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$.*
   Для любых $a, b \in G$ уравнение $xa = b$ имеет единственное решение $x = ba^{-1}$.
3) *Для любых $a, b \in G$ справедливо равенство $(ab)^{-1} = b^{-1}a^{-1}$.*

Доказательство.

Предположим, что для элемента a существуют два обратных элемента a_1 и a_2. Тогда

$$a_1 a a_2 = a_1(a a_2) = a_1 e = a_1,$$
$$a_1 a a_2 = (a_1 a)a_2 = e a_2 = a_2.$$

Следовательно, $a_1 = a_2$.
Подставим $x = a^{-1}b$ в уравнение $ax = b$. Получим

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Следовательно, $x = a^{-1}b$ является решением уравнения $ax = b$.

Пусть существуют два решения x_1 и x_2. Тогда из равенств $ax_1 = b$, $ax_2 = b$ следует, что $ax_1 = ax_2$. Умножим левую и правую часть последнего равенства на a^{-1}. Получим

$$(a^{-1}a)x_1 = (a^{-1}a)x_2, \quad ex_1 = ex_2, \quad x_1 = x_2.$$

Аналогично можно показать, что уравнение $xa = b$ имеет единственное решение $x = ba^{-1}$.

Докажем третью часть теоремы. Для любых $a, b \in G$ справедливы равенства

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$
$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Следовательно, $(ab)^{-1} = b^{-1}a^{-1}$.

Определение

Пусть G – группа. Подмножество $H \subseteq G$ называется подгруппой G, если H само является группой.

Теорема

Пересечение двух подгрупп является подгруппой.

Доказательство.

Пусть H и P подгруппы группы G. Обозначим $Q = H \cap P$. Пусть $a, b \in Q$. Необходимо показать, что $ab \in Q$, $e \in Q$, $a^{-1} \in Q$.
Из условия $a, b \in Q$ следует, что $a, b \in H$ и $a, b \in P$. Следовательно, $ab \in H$ и $ab \in P$. Таким образом, $ab \in Q$.
Единичный элемент является единственным, при этом $e \in H$ и $e \in P$. Следовательно, $e \in Q$.
Пусть $a \in Q$. Тогда $a \in H$ и $a \in P$. Обратный элемент $a^{-1} \in H$ и $a^{-1} \in P$. Следовательно, $a^{-1} \in Q$. □

Теорема

Для любого элемента a группы G множество

$$\{a\} = \left\{a^k \mid k \in Z\right\} \subseteq G$$

является абелевой подгруппой.

Доказательство.

Для любых $k, j \in Z$ произведение

$$a^k a^j = a^j a^k = a^{k+j} \in \{a\}.$$

Единичный элемент $e = a^0 \in \{a\}$.
Для любого $a^k \in \{a\}$ существует обратный $(a^k)^{-1} = a^{-k} \in \{a\}$.
Следовательно, $\{a\}$ является абелевой подгруппой G. □

Определение

Подгруппа $\{a\}$ называется циклической подгруппой, порождённой элементом a.

Пример

Пусть $G = \langle Z; + \rangle$ – группа целых чисел относительно операции сложения.
Подмножество чётных чисел является подгруппой G.
Сумма двух чётных чисел является чётным числом.
Противоположное число к чётному числу является чётным числом.
Нейтральный элемент, число 0, является чётным числом.
Подгруппа чётных чисел является циклической подгруппой $\{2\}$, поскольку любое четное число записывается в виде $2k$, $k \in Z$.

4.3 Циклические группы

Определение

Группа G называется циклической, если она совпадает с одной из своих циклических подгрупп, т.е. её можно представить в виде

$$G = \{a\}, \quad a \in G.$$

Теорема

Любая подгруппа циклической группы является циклической.

Доказательство.

Пусть H есть подгруппа циклической группы $G = \{a\}$.
Если $a^k \in H$, то и $(a^k)^{-1} = a^{-k} \in H$.
Пусть k – минимальное положительное число такое, что $a^k \in H$.
Покажем, что любой элемент H может быт записан в виде $(a^k)^p = a^{pk}$. Докажем от противного.
Пусть $a^n \in H$, $n > k$ и n не делится на k. Тогда $n = pk + r$, где $0 < r < k$.
Следовательно, $a^r = a^n a^{-pk} \in H$, что противоречит выбору k.
Таким образом, мы показали, что a^k является порождающим элементом подгруппы $H = \{a^k\}$. □

Определение

Порядком элемента a группы G называется наименьшее положительное число n такое, что $a^n = e$.

Теорема

Пусть G – группа и $a \in G$ имеет порядок n. Тогда циклическая подгруппа $\{a\}$ является конечной порядка n и состоит из элементов

$$\{a\} = \{e; a; a^2; \ldots; a^{n-1}\}.$$

Доказательство.

Все элементы последовательности $e, a, a^2, \ldots, a^{n-1}$ различны. Докажем от противного. Пусть

$$a^k = a^r, \quad k, r < n, \quad k > r.$$

Тогда $a^{k-r} = e$, $k - r < n$. Следовательно, порядок элемента a меньше n, что противоречит исходному предположению.
Любая другая степень a, положительная или отрицательная, совпадает с одним из элементов этой последовательности.
Пусть $|k| \geq n$. Тогда k можно записать в виде $k = np + r$, $0 \leq r < n$. Следовательно,

$$a^k = (a^n)^p a^r = e^p a^r = a^r \in \{e, a, a^2, \ldots, a^{n-1}\}.$$

Таким образом,

$$\{a\} = \{e, a, a^2, \ldots, a^{n-1}\}.$$

□

Определение

Пусть G – группа. Подмножество $H \subset G$ называется системой образующих группы G, если любой элемент G есть произведение конечного числа элементов, каждый из которых является элементом H или обратным к элементу H.

Пример

Для циклической группы $G = \{a\}$ система образующих состоит из одного элемента a.

Пример

Множество $A = \{(x, y) \mid x, y \in Z\}$ с операцией сложения

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

образует абелеву группу. Система образующих этой группы состоит из двух элементов: $(0, 1)$ и $(1, 0)$.

4.4 Симметрическая группа

Пусть задано множество A. Обозначим через F множество биекций

$$f : A \leftrightarrow A.$$

Рассмотрим операцию композиции биекций $f \circ g$.

Для любого $x \in A$ значение композиции определяется по правилу

$$(f \circ g)(x) = g(f(x)).$$

Операция композиции биекций является алгебраической операцией, поскольку композиция биекций также является биекцией.

Эта операция является ассоциативной

$$\forall f, g, h \in F : (f \circ g) \circ h = f \circ (g \circ h).$$

Действительно,

$$((f \circ g) \circ h)(x) = h((f \circ g)(x)) = h(g(f(x))),$$
$$(f \circ (g \circ h))(x) = (g \circ h)(f(x)) = h(g(f(x))).$$

Рассмотрим биекцию $e : A \leftrightarrow A$, заданную правилом

$$e(x) = x, \quad x \in A.$$

Справедливы равенства

$$(e \circ f)(x) = f(e(x)) = f(x), \quad (f \circ e)(x) = e(f(x)) = f(x).$$

Следовательно, e является нейтральным элементом по отношению к операции композиции.

Обратным элементом для $f \in F$ является обратная функция

$$f^{-1} : A \leftrightarrow A, \quad x = f^{-1}(y), \quad y = f(x),$$

которая также является биекцией. Справедливы соотношения

$$f \circ f^{-1} = e, \quad f^{-1} \circ f = e.$$

Таким образом, множество F относительно операции композиции образует группу.

Определение

Симметрической группой множества A называется группа биекций $f : A \leftrightarrow A$ относительно операции композиции. Симметрическую группу обозначают $S(A)$.

Теорема (Теорема Кэли)

Пусть $G = \langle A; \cdot \rangle$ – группа. Существует подгруппа H группы $S(A)$, такая, что G изоморфна H.

Доказательство.

Пусть $a \in A$. Построим функцию $f_a : A \to A$ по правилу

$$\forall x \in A : f(x) = ax.$$

Эта функция является биекцией.
Для любого $y \in A$ уравнение $ax = y$ имеет единственное решение $x = a^{-1}y$.
Следовательно, f_a является сюръекцией и инъекцией, то есть биекцией.

Обозначим через $F_A = \{f_a | \ a \in A\}$ множество таких биекций. Пусть $a, b \in A$. Тогда

$$\forall x \in A : (f_a \circ f_b)(x) = f_b(f_a(x)) = f_b(ax) = bax = f_{ba}(x).$$

Следовательно, $f_a \circ f_b = f_{ba} \in F_A$.
Обозначим через 1 нейтральный элемент группы G. Нейтральный элемент группы $S(A)$ равен $e = f_1 \in F_A$. Обратный элемент $f_a^{-1} = f_{a^{-1}} \in F_A$.

Таким образом, относительно операции композиции множество F_A образует подгруппу $H = \langle F_A; \circ \rangle$ группы $S(A)$.
Установим биекцию $g : A \leftrightarrow F_A$ по правилу

$$\forall a \in A : g(a) = f_a.$$

Эта биекция порождает изоморфизм групп G и H. □

Определение

Симметрическая группа $S(A)$ конечного множества A с n элементами называется группой симметрий и обозначается S_n.

Группа симметрий S_n является конечной. Порядок группы симметрий S_n равен числу биекций $n!$.

Теорема Кэли справедлива и для группы симметрий. Это означает, что любая конечная группа порядка n изоморфна некоторой подгруппе группы симметрий S_n.

Группу симметрий называют также группой подстановок. Это название происходит от формы записи биекции в виде подстановки.

Определение

Подстановкой порядка n называется таблица

$$P_k = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

где нижняя строка есть перестановка элементов верхней строки.

Каждая подстановка есть биекция $f : A \leftrightarrow A$, где $A = \{1; 2; \dots; n\}$.
Всего различных подстановок $n!$

Под произведением подстановок

$$P_i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

понимается подстановка

$$P_i P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}.$$

Произведение подстановок есть композиция соответствующих подстановкам биекций.

Пример

При $n = 3$ подстановки можно записать в следующем виде

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$
$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Пример произведения подстановок

$$P_4 P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_6.$$

Множество подстановок порядка n относительно операции умножения образуют группу. В этой группе единичным элементом является подстановка

$$P_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Для каждой подстановки P_i существует обратная P_j такая, что

$$P_i P_j = P_1, \quad P_j P_i = P_1.$$

Обратной для

$$P_i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

является подстановка P_j, которая может быть построена следующим образом. Сначала составим таблицу

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Затем переставим столбцы этой таблицы так, чтобы она приняла вид подстановки

$$P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Это и будет, обратная для P_i подстановка.

Пример

Таблица Кэли для группы подстановок S_3 имеет следующий вид

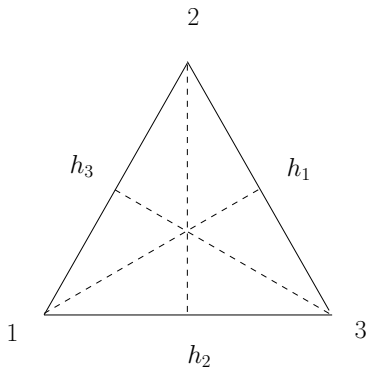
$*$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_6	P_4	P_5
P_3	P_3	P_1	P_2	P_5	P_6	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_6	P_4	P_3	P_1	P_2
P_6	P_6	P_4	P_5	P_2	P_3	P_1

Группа подстановок не является абелевой. В общем случае $P_iP_j \neq P_jP_i$. Например,

$$P_2P_4 = P_6, \quad P_4P_2 = P_5.$$

Пример

Группа симметрий правильного треугольника



Будем рассматривать самосовмещения треугольника, то есть такие перемещения треугольника, при которых изображение треугольника на плоскости не меняется.

Такие самосовмещения возможны при повороте треугольника относительно центра против часовой стрелки на на углы 0^0, 120^0, 240^0, а также при повороте треугольника относительно трёх высот h_1, h_2, h_3.

Алгебраической операцией в данном случае является операция последовательного перемещения треугольника.

Операции поворота треугольника можно описать в виде подстановок:

- P_1 – поворот на 0^0;
- P_2 – поворот на 120^0;
- P_3 – поворот на 240^0;
- P_4 – поворот относительно высоты h_1;
- P_5 – поворот относительно высоты h_2;
- P_6 – поворот относительно высоты h_3;

Например, последовательное выполнение поворотов треугольника относительно высоты h_1 и против часовой стрелки на 240^0 описывается подстановкой $P_4P_3 = P_6$.

Группа симметрий правильного треугольника является группой симметрий S_3.

4.5 Разложение группы по подгруппе

Пусть H есть подгруппа группы G. Рассмотрим бинарное отношение на множестве G

$$R_H = \{(a, b) |\ a^{-1}b \in H\}.$$

Теорема

Отношение R_H является отношением эквивалентности.

Доказательство.

Необходимо показать, что отношение R_H является рефлексивным, симметричным и транзитивным.

Рефлексивность

$$a^{-1}a = e \in H \ \Rightarrow\ (a, a) \in R_H.$$

Симметричность

$$(a, b) \in R_H \ \Rightarrow\ a^{-1}b = h \in H \Rightarrow\ b^{-1}a = h^{-1} \in H \ \Rightarrow\ (b, a) \in R_H.$$

Транзитивность

$$(a, b) \in R_H,\ (b, c) \in R_H \ \Rightarrow\ a^{-1}b = h_1 \in H,\ b^{-1}c = h_2 \in H \ \Rightarrow$$
$$a^{-1}c = h_1h_2 \in H \ \Rightarrow\ (a, c) \in R_H.$$

□

Отношение эквивалентности порождает разбиение группы на классы эквивалентности

$$[a] = \{b \mid a \sim b\}.$$

Определение

Левые смежные классы группы G по подгруппе H есть множества

$$aH = \{ah \mid h \in H\}.$$

Теорема

Классы эквивалентности отношения R_H есть левые смежные классы G по H

$$[a] = aH.$$

Доказательство.

Докажем методом включения

$$b \in [a] \ \Leftrightarrow\ a^{-1}b = h \in H \ \Leftrightarrow\ b = ah \in aH$$

□

Левые смежные классы образуют разбиение группы. Это означает, что

$$G = \bigcup_{a \in G} aH$$

и любые два смежных класса aH, bH либо совпадают, либо не пересекаются.

Аналогично определяются правые смежные классы Ha.

Если группа G абелева, то левые и правые смежные классы совпадают, $aH = Ha$.

Теорема (Теорема Лагранжа)

Пусть G конечная группа порядка n, H – подгруппа G порядка k. Тогда n делится на k.

Доказательство.

Все левые смежные классы содержат ровно k элементов, т.к. из равенства $ah_1 = ah_2$, $h_1, h_2 \in H$ следует $h_1 = h_2$.
Пусть p есть число различных смежных классов. Тогда $n = kp$. □

Пример

Рассмотрим группу подстановок S_3. Порядок этой группы равен 6. По теореме Лагранжа в группе S_3 могут быть подгруппы порядка 1,2,3. Запишем эти подгруппы

$$\{P_1\}, \quad \{P_1; P_4\}, \quad \{P_1; P_5\}, \quad \{P_1; P_6\}, \quad \{P_1; P_2; P_3\}.$$

4.6 Определение и свойства колец

Определение

Кольцом называется алгебраическая структура $\langle K; +, \cdot \rangle$ с двумя алгебраическими операциями: сложение «$+$» и умножение «$\cdot$», в которой выполняются следующие условия:

1) $\langle K; + \rangle$ является аддитивной абелевой группой;
2) $\langle K; \cdot \rangle$ является полугруппой;
3) выполняется закон дистрибутивности

$$\forall a, b, c \in K: \ (a + b)c = ac + bc, \quad c(a + b) = ca + cb.$$

Пример

Множество целых чисел с операциями сложения и умножения $\langle Z; +, \cdot \rangle$ является кольцом.

Множество $F(x)$ многочленов

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

с действительными коэффициентами образует кольцо $\langle F(x); +, \cdot \rangle$.

Определение

Кольцо $\langle K; +, \cdot \rangle$ называется коммутативным, если умножение коммутативная операция.
Кольцо $\langle K; +, \cdot \rangle$ называется кольцом с единицей, если в полугруппе $\langle K; \cdot \rangle$ существует единица 1.

Теорема (Свойства кольца)

Пусть $\langle K; +, \cdot \rangle$ *– кольцо. Тогда*

1) $\forall a \in K \ : \ a0 = 0a = 0$
2) $\forall a, b \in K \ : \ (-a)b = a(-b) = -ab$

Доказательство.

Для любых $a, b \in K$ справедливы утверждения:

$$\begin{aligned} a(a+0) = aa + a0, \ a(a+0) = aa \ &\Rightarrow \ a0 = 0, \\ (a+0)a = aa + 0a, \ (a+0)a = aa \ &\Rightarrow \ 0a = 0, \\ 0 = 0b = (a-a)b = ab + (-a)b \ &\Rightarrow \ (-a)b = -ab, \\ 0 = a0 = a(b-b) = ab + a(-b) \ &\Rightarrow \ a(-b) = -ab. \end{aligned}$$

Здесь мы применили закон дистрибутивности и определение нулевого и противоположного элемента аддитивной группы. □

Определение

Элементы $a, b \neq 0$ кольца $\langle K; +, \cdot \rangle$ называются делителями нуля, если $ab = 0$.

Пример

Множество квадратных матриц с действительными элементами размерности n образуют кольцо $\langle M_n; +, \cdot \rangle$. В этом кольце существуют делители нуля. Например, при $n = 2$

$$\begin{bmatrix} 1 & 2 \\ -2 & -4 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ -1,5 & -2,5 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Определение

Подмножество L кольца $\langle K; +, \cdot \rangle$ является подкольцом, если L само является кольцом $\langle L; +, \cdot \rangle$.

Теорема

Подмножество L кольца $\langle K; +, \cdot \rangle$ является подкольцом тогда и только тогда, когда

$$\forall a, b \in L \ : a - b \in L \quad \text{и} \quad ab \in L.$$

Доказательство.

Необходимость очевидна. Докажем достаточность. Пусть $a, b \in L$. Тогда

$$0 = a - a \in L, \quad 0 - a = -a \in L, \quad a - (-b) = a + b \in L,$$
$$a + b = b + a, \quad ab \in L.$$

Следовательно, $\langle L; + \rangle$ – абелева группа, $\langle L; \cdot \rangle$ – полугруппа. Также выполняется закон дистрибутивности

$$\forall a, b, c \in L : a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

Тем самым мы показали, что $\langle L; +, \cdot \rangle$ является кольцом. □

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$. Множество целых чисел $L = \{pn | \ n \in Z\}$, кратных заданному натуральному числу p, является подкольцом кольца Z.
Действительно, пусть $a, b \in L$. Тогда $a = pn$, $b = pm$ и $a - b = p(n - m) \in L$, $ab = p(npm) \in L$. Следовательно, L есть подкольцо кольца $\langle Z; +, \cdot \rangle$.

Пример

Рассмотрим кольцо многочленов $\langle F(x); +, \cdot \rangle$ и множество $L(x)$ многочленов $f(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n$ с нулевым коэффициентом a_0. Пусть $f(x), g(x) \in L(x)$. Тогда $f(x) - g(x) \in L(x)$, $f(x)g(x) \in L(x)$. Следовательно, $L(x)$ является подкольцом кольца $\langle F(x); +, \cdot \rangle$.

4.6 Идеалы, классы вычетов, фактор-кольца

Пусть $\langle K; +, \cdot \rangle$ – коммутативное кольцо.

Определение

Идеалом кольца K называется подкольцо L такое, что для любого $a \in L$ и любого $b \in K$ произведение $ab \in L$.

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$. Множество целых чисел $L = \{pn | \ n \in Z\}$, кратных заданному натуральному числу p, является идеалом кольца Z.
Действительно, множество L является подкольцом кольца $\langle Z; +, \cdot \rangle$ и для любых $a = pn \in L$, $b \in Z$ произведение $ab = pnb \in L$.

Теорема

Для любого $a \in K$ множество $aK = \{ab \mid b \in K\}$ является идеалом кольца K. Этот идеал называется главным.

Доказательство.

Пусть $a, b, c \in K$. Тогда $ab \in aK$, $ac \in aK$. При этом

$$ab - ac = a(b - c) \in aK, \quad (ab)(ac) = a(bac) \in aK.$$

Следовательно, множество aK является подкольцом K.
Подкольцо aK является идеалом, поскольку $(ab)c = a(bc) \in aK$. □

Определение

Кольцо называется кольцом главных идеалов, если в этом кольце других идеалов кроме главных нет.

Пример

Кольцо целых чисел $\langle Z; +, \cdot \rangle$ является кольцом главных идеалов. Действительно, пусть L есть идеал кольца Z. Обозначим через a наименьшее натуральное число в L. Покажем, что $L = aZ$. По определению идеала $aZ \subseteq L$. Пусть $b \in L$ и $b \notin aZ$. Существуют $q, r \in N$ такие, что $b = aq + r$ и $0 < r < a$. Тогда $r = b - aq \in L$, что противоречит выбору a. Следовательно, $L = aZ$.

Пусть L – идеал кольца $\langle K; +, \cdot \rangle$. Рассмотрим аддитивную коммутативную группу $\langle K; + \rangle$. Подкольцо L также является и подгруппой $\langle L; + \rangle$ группы $\langle K; + \rangle$. Рассмотрим смежные классы

$$[a] = a + L = \{a + b \mid b \in L\}$$

группы $\langle K; + \rangle$ по подгруппе $\langle L; + \rangle$. В теории колец эти смежные классы называют классами вычетов и обозначают C_a.

На множестве классов вычетов определим операции сложения и умножения

$$C_a + C_b = C_{a+b},$$
$$C_a C_b = C_{ab}.$$

Теорема

Множество классов вычетов образуют коммутативное кольцо относительно операций сложения и умножения. Это кольцо называется факторкольцом и обозначается K/L.

Доказательство.

Справедливы равенства:

$$C_a + C_b = C_{a+b} = C_{b+a} = C_a + C_b,$$
$$C_a + C_0 = C_a, \quad C_a + C_{-a} = C_0,$$
$$C_a C_b = C_{ab} = C_{ba} = C_b C_a.$$

Следовательно, K/L есть коммутативное кольцо. □

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$ и идеал $\langle L; +, \cdot \rangle$ чисел, кратных натуральному числу p.
Обозначим Z_p кольцо классов вычетов, порождённое идеалом L.
Элементы кольца классов вычетов имеют следующий вид

$$C_a = \{a + pn \mid n \in Z\}.$$

В этом кольце существует единичный элемент C_1. Для любого $n \in Z$ класс вычетов $C_{pn} = C_0$.

Кольцо Z_p является конечным и состоит из элементов

$$Z_p = \{C_0, C_1, \ldots, C_{p-1}\}.$$

Действительно, пусть $a \in Z$. Тогда $a = pn + r$, $0 \le r < p$ и, следовательно,

$$C_a = C_{pn+r} = C_p C_n + C_r = C_0 + C_r = C_r.$$

Противоположный к классу C_m есть класс C_{p-m}, поскольку

$$C_m + C_{p-m} = C_p = C_0.$$

Операции сложения и умножения в кольце Z_p выполняются по следующим правилам

$$C_m + C_n = \begin{cases} C_{m+n}, & m+n < p \\ C_{m+n-p}, & m+n \ge p \end{cases},$$

$$C_m C_n = C_r, \quad mn = pk + r, \quad 0 \le r < p.$$

4.7 Определение и свойства полей

Определение

Коммутативное кольцо $\langle P; +, \cdot \rangle$ называется полем, если в P существует 1 и для любого $a \in P$, $a \ne 0$, существует a^{-1}.

Алгебраическая структура $\langle P \setminus \{0\}; \cdot \rangle$ является коммутативной группой. Таким образом, поле состоит из двух коммутативных групп, объединённых законом дистрибутивности.

Пример

Множество целых чисел $\langle Z; +, \cdot \rangle$ полем не является. Множество рациональных чисел $\langle Q; +, \cdot \rangle$, множество действительных чисел $\langle R; +, \cdot \rangle$ и множество комплексных чисел $\langle C; +, \cdot \rangle$ являются полями относительно операций сложения и умножения.

В поле нет делителей нуля. Действительно, пусть $ab = 0$, $a \neq 0$, $b \neq 0$. Тогда $a^{-1}(ab) = (a^{-1}a)b = 1b = b = 0$. Что противоречит исходному предположению.

Теорема

Конечное коммутативное кольцо с единицей является полем тогда и только тогда, когда в этом кольце нет делителей нуля.

Доказательство.

Необходимость мы уже доказали. Докажем достаточность. Обозначим элементы кольца

$$K = \{a_1; a_2; \ldots; a_n\}.$$

Среди этих элементов есть нулевой элемент – 0 и единичный – 1.

Пусть $a \in K$ и $a \neq 0$. Рассмотрим последовательность элементов

$$aa_1,\ aa_2,\ \ldots,\ aa_n.$$

Все элементы этой последовательности различны. Действительно, пусть $aa_i = aa_j$, $a_i \neq a_j$. Тогда $a(a_i - a_j) = 0$. Поскольку $a \neq 0$ и в кольце нет делителей нуля, то $a_i - a_j = 0$. То есть, $a_i = a_j$. Получили противоречие.
Таким образом,

$$\{a_1; a_2; \ldots; a_n\} = \{aa_1; aa_2; \ldots; aa_n\}.$$

Следовательно, $aa_i = 1$ некоторого $1 \leq i \leq n$. В силу коммутативности $a_i a = 1$. Это означает, что для каждого элемента $a \in K$ существует обратный a^{-1}. Тем самым мы доказали, что рассматриваемое кольцо является полем. □

Пример

Рассмотрим кольцо вычетов Z_p. Это конечное коммутативное кольцо, состоящее из элементов

$$Z_p = \{C_0; C_1; \ldots; C_{p-1}\}.$$

В этом кольце есть единичный элемент C_1.
Пусть p составное число, $p = mn$. Тогда

$$C_m C_n = C_p = C_0.$$

Следовательно, в кольце Z_p есть делители нуля и поэтому Z_p не является полем.

Пусть p простое число. В этом случае в кольце Z_p делителей нуля нет. Докажем от противного.
Пусть $C_m C_n = C_0$. Тогда $mn = kp$. Число p простое. Следовательно, k делится на m.
Мы можем записать $k = ml$. После деления на m левой и правой равенства $mn = kp$ получим $n = lp$. Что невозможно, поскольку $n < p$.
Таким образом, при простом p кольцо вычетов Z_p является полем.

Определение

Подкольцо L поля $\langle P; +, \cdot \rangle$ называется подполем, если L само является полем.

Определение

Поле P называется расширением поля L, если L является подполем P.

Пример

Поле действительных чисел $\langle R; +, \cdot \rangle$ является расширением поля рациональных чисел $\langle Q; +, \cdot \rangle$. Поле комплексных чисел $\langle C; +, \cdot \rangle$ является расширением поля действительных чисел $\langle R; +, \cdot \rangle$.

Конечные поля называют полями Галуа и обозначают F_q или $GF(q)$, где q – число элементов поля.

Конечное поле с числом элементов q существует тогда и только тогда, когда $q = p^m$,где p – простое число, m – любое натуральное число.

Мултипликативная группа конечного поля $GF(q)$ является циклической. Это означает, что существует элемент поля $a \neq 0$ такой, что все остальные элементы поля, за исключением 0, являются степенями этого элемента. Таким образом

$$GF(q) = \{0; 1; a; a^2; \ldots; a^{q-2}\}.$$

Пример

Простейшим примером конечного поля F_2 является поле $\langle E; \oplus, \cdot \rangle$, где $E = \{0; 1\}$, $\oplus, \cdot$ – логические операции сумма по модулю два и конъюнкция. Это поле изоморфно полю классов вычетов $\langle Z_2; +, \cdot \rangle$.

В общем случае кольцо классов вычетов $\langle Z_p; +, \cdot \rangle$ является полем тогда и только тогда, когда p – простое число.

Все остальные конечные поля можно построить как расширение полей классов вычетов.

Обозначим через $GF(q)[x]$ кольцо многочленов с коэффициентами из поля $GF(q)$. Элементы $GF(q)[x]$ есть многочлены следующего вида

$$f(x) = f_0 + f_1 x + \cdots + f_n x^n, f_i \in GF(q).$$

Многочлен $f(x) \in GF(q)[x]$ называется нормированным, если коэффициент при старшей степени равен $f_n = 1$.

Многочлен $f(x) \in GF(q)[x]$ называется примитивным, если его нельзя представить в виде произведения двух многочленов из $GF(q)[x]$ ненулевой степени.

В кольце $GF(q)[x]$ для любого натурального m всегда существует по крайней мере один примитивный многочлен степени m.

Например в кольце $GF(2)[x]$ примитивными многочленами являются

$$1 + x + x^2, \quad 1 + x + x^3, \quad 1 + x + x^4,$$
$$1 + x^2 + x^5, \quad 1 + x + x^6, \quad 1 + x^3 + x^7.$$

Примитивными многочленами второй степени в кольце $GF(3)[x]$ являются

$$1 + x^2, \quad 2 + x + x^2, \quad 2 + 2x + x^2.$$

Алгоритм построения конечного поля $GF(p^m)$ удобно описать с использованием кольца многочленов $GF(p)[x]$.

Пусть $f(x)$ есть примитивный нормированный многочлен степени m в кольце $GF(p)[x]$.

Элементы поля $GF(p^m)$ есть многочлены $g(x) \in GF(p)[x]$ степени не выше $m - 1$. Число таких многочленов равно p^m.

Элементы поля $GF(p^m)$ можно также рассматривать как векторы

$$g = [g_0, g_1, \ldots, g_{m-1}],$$

составленные из коэффициентов многочленов

$$g(x) = g_0 + g_1 x + \cdots + g_{m-1} x^{m-1} \in GF(p)[x].$$

В случае $p = 2$ это будут двоичные векторы.

Операции сложения и умножения элементов поля $GF(p^m)$ выполняются как операции сложения и умножения соответствующих многочленов в кольце $GF(p)[x]$.

При этом результат произведения двух многочленов $g(x)$ и $h(x)$ есть остаток от деления $g(x)h(x)$ на $f(x)$.

Другими словами, произведение $g(x)$ и $h(x)$ в поле $GF(p^m)$ есть $g(x)h(x) \pmod{f(x)}$ в кольце $GF(p)[x]$.

Организовать вычисления в конечном поле можно с использованием порождающего элемента мультипликативной группы поля.

Сумма элементов поля a^i и a^j есть сумма соответствующих векторов с элементами из поля $GF(p)$.

Произведение определяется по правилу

$$a^i a^j = a^{i+j} \pmod{q-1}.$$

Рассмотрим пример построения поля $GF(2^3)$ с использованием примитивного многочлена третьей степени $f(x) = 1 + x + x^3$.

Элементы поля – это все многочлены с двоичными коэффициентами не выше второй степени:

$$0; \quad 1; \quad x; \quad 1+x; \quad x^2; \quad 1+x^2; \quad x+x^2; \quad 1+x+x^2.$$

Можно построить таблицы сложения и умножения элементов поля. Пусть, например,

$$g(x) = 1 + x^2, \quad h(x) = 1 + x + x^2.$$

Тогда

$$g(x) + h(x) = x,$$
$$g(x)h(x) = (1+x^2)(1+x+x^2) \pmod{f(x)} =$$
$$= (1 + x + x^3 + x^4) \pmod{f(x)} = x + x^2.$$

Элемент поля $a = x$ является порождающим элементом мультипликативной группы поля. Это означает, что элементы поля можно записать в следующем виде:

$$0; \quad 1; \quad a; \quad a^2; \quad a^3; \quad a^4; \quad a^5; \quad a^6.$$

Здесь

$$\begin{aligned}
&a = x,\\
&a^2 = x^2 \pmod{f(x)} = x^2;\\
&a^3 = x^3 \pmod{f(x)} = 1 + x,\\
&a^4 = x^4 \pmod{f(x)} = x + x^2,\\
&a^5 = x^5 \pmod{f(x)} = 1 + x + x^2,\\
&a^6 = x^6 \pmod{f(x)} = 1 + x^2.
\end{aligned}$$

Заметим, что

$$a^7 = x^7 \pmod{f(x)} = 1.$$

Таким образом мы получаем три эквивалентных представления элементов поля: в виде степени порождающего элемента мультипликативной группы поля, в виде многочлена и в виде двоичного вектора

0	0	[000]
1	1	[100]
a	x	[010]
a^2	x^2	[001]
a^3	$1+x$	[110]
a^4	$x+x^2$	[011]
a^5	$1+x+x^2$	[111]
a^6	$1+x^2$	[101]

Пусть, например, необходимо вычислить сумму и произведение элементов поля a^4 и a^6. Значение суммы можно вычислить как значение суммы соответствующих двоичных векторов в поле $GF(2)$. Получим

$$a^4 + a^6 \equiv [011] + [101] = [110] \equiv a^3.$$

Значение произведения вычисляется по правилу

$$a^4 a^6 = a^{10} \pmod 7 = a^3.$$

При этом не требуется умножать и делить соответствующие элементам a^4 и a^6 многочлены.

4.8 Булева алгебра

Рассмотрим алгебраическую структуру с тремя алгебраическими операциями $\langle B; +, \cdot, ^- \rangle$. Две из них бинарные: «$+$»,«$\cdot$», одна унарная: «$^-$». Элемент $\overline{a}$ будем называть дополнением элемента a.

Определение

Алгебраическая структура $\langle B; +, \cdot, ^- \rangle$ называется булевой алгеброй, если

1) $\langle B; + \rangle$ есть коммутативная полугруппа с нулевым элементом 0;
2) $\langle B; \cdot \rangle$ есть коммутативная полугруппа с единичным элементом 1;
3) выполняются законы дистрибутивности

$$\forall a, b, c \in B: \ a(b+c) = ab + bc, \ a + bc = (a+b)(a+c);$$

4) выполняются законы дополнения

$$\forall a \in B: \ a + \overline{a} = 1, \ a\overline{a} = 0.$$

Пример

Булеан 2^A множества A образует булеву алгебру $\langle 2^A; \cup, \cap, ^- \rangle$ относительно операций объединения, пересечения и дополнения множеств. Роль нуля здесь выполняет пустое множество $\emptyset$, роль единицы само множество A.

Пример

Согласно законам алгебры логики множество $B = \{0; 1\}$ образует булеву алгебру $\langle B; \vee, \wedge, ^- \rangle$ относительно логических операций дизъюнкции, конъюнкции и отрицания.

Рассмотрим следствия, которые вытекают из аксиом булевой алгебры. Сначала заметим, что для любого элемента a, элемент, удовлетворяющий законам дополнения, является единственным и равен $\overline{a}$. Действительно, пусть для некоторого элемента b выполняются равенства

$$a + b = 1, \quad ab = 0.$$

Применяя законы дистрибутивности и дополнения, получим

$$b = b + 0 = b + a\overline{a} = (b + a)(b + \overline{a}) = 1(b + \overline{a}) = (a + \overline{a})(b + \overline{a}) = ab + \overline{a} = 0 + \overline{a} = \overline{a}.$$

Заметим также, что $1 + 0 = 1$, $1 \cdot 0 = 0$. Следовательно, $\overline{1} = 0$, $\overline{0} = 1$.

Теорема

Пусть $\langle B; +, \cdot, {}^{-} \rangle$ есть булева алгебра. Тогда для любых $a, b \in B$ справедливы тождества:

1) *идемпотентность*
$$2a = a, \quad a^2 = a;$$
2) *свойства констант*
$$a + 1 = 1, \quad a0 = 0.$$
3) *поглощение*
$$a + ab = a, \quad a(a + b) = a;$$

4) двойное дополнение
$$\overline{\overline{a}} = a;$$
5) законы де Моргана
$$\overline{a + b} = \overline{a}\,\overline{b}, \quad \overline{ab} = \overline{a} + \overline{b};$$
6) склеивание
$$\overline{a}b + ab = b, \quad (\overline{a} + b)(a + b) = b;$$

Доказательство.

Идемпотентность.
Из законов дистрибутивности и дополнения получим

$$2a = (a + a)1 = (a + a)(a + \overline{a}) = a + a\overline{a} = a + 0 = a,$$
$$a^2 = a^2 + 0 = a^2 + a\overline{a} = a(a + \overline{a}) = a1 = a.$$

Свойства констант.
Из идемпотентности и законов дополнения следует

$$a + 1 = a + (a + \overline{a}) = (a + a) + \overline{a} = a + \overline{a} = 1,$$
$$a0 = a(a\overline{a}) = a^2\overline{a} = a\overline{a} = 0.$$

Поглощение.
Из законов дистрибутивности и свойств констант следует

$$a + ab = a1 + ab = a(1 + b) = a1 = a,$$
$$a(a + b) = (a + 0)(a + b) = a + 0b = a + 0 = a.$$

Двойное дополнение.
По законам дополнения

$$\overline{a} + \overline{\overline{a}} = 1, \quad \overline{a}\,\overline{\overline{a}} = 0,$$
$$\overline{a} + a = 1, \quad \overline{a}a = 0.$$

В силу единственности дополнения $\overline{\overline{a}} = a$.

Законы де Моргана.
Из законов дистрибутивности и свойств констант получим

$$(a + b)\overline{a}\,\overline{b} = (a\overline{a})\overline{b} + (b\overline{b})\overline{a} = 0\overline{b} + 0\overline{a} = 0,$$
$$(a + b) + \overline{a}\,\overline{b} = (a + b + \overline{a})(a + b + \overline{b}) = (1 + b)(1 + a) = 1.$$

Элемент $\overline{a}\,\overline{b}$ удовлетворяет законам дополнения для элемента $a + b$.
Следовательно,

$$\overline{a + b} = \overline{a}\,\overline{b}.$$

Применяя доказанный закон и двойное дополнение, получим

$$\overline{a} + \overline{b} = \overline{\overline{\overline{a} + \overline{b}}} = \overline{\overline{\overline{a}}\,\overline{\overline{b}}} = \overline{ab}.$$

Склеивание.
По законам дистрибутивности и дополнения

$$\overline{a}b + ab = (\overline{a} + a)b = 1b = b,$$
$$(\overline{a} + b)(a + b) = \overline{a}a + b = 0 + b = b.$$

□

Тема 5. Теория графов

5.1 Основные определения

Определение

Графом называется совокупность двух конечных множеств – множества вершин V и множества ребер E, соединяющих вершины

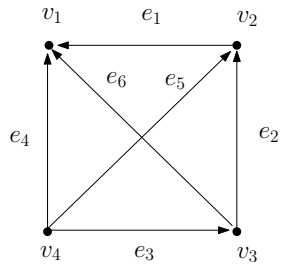
$$G = \langle V, E \rangle,$$

$$V = \{v_1; v_2; \ldots; v_n\}, \quad E = \{e_1; e_2; \ldots; e_m\}, \quad e_k = (v_i, v_j).$$

Ребра могут быть направленные и ненаправленные. Направленные ребра называются дугами.

Пример

Бинарное отношение $x > y$ на множестве чисел $V = \{1; 2; 3; 4\}$ описывается графом

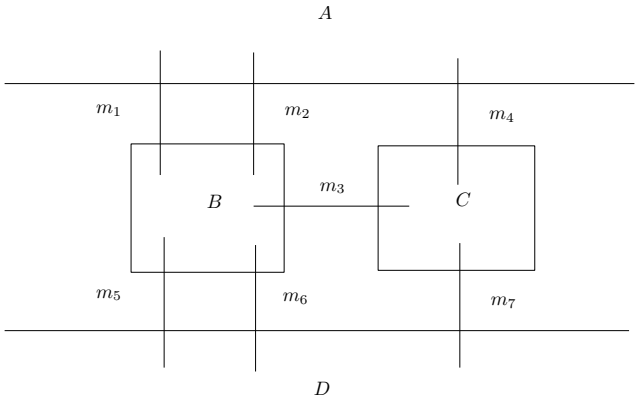


Здесь:

$$v_1 = 1, \quad v_2 = 2, \quad v_3 = 3, \quad v_4 = 4,$$
$$e_1 = (2, 1) \quad e_2 = (3, 2), \quad e_3 = (4, 3),$$
$$e_4 = (4, 1), \quad e_5 = (4, 2), \quad e_6 = (3, 1).$$

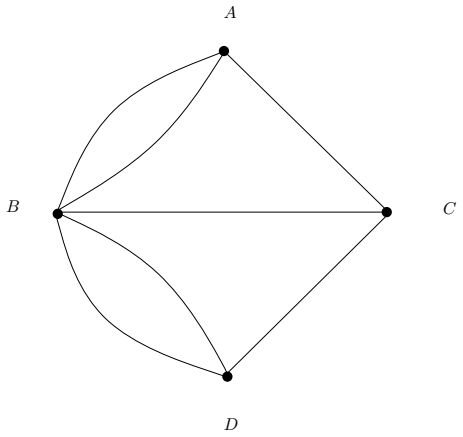
Пример (Задача Эйлера о кёнигсбергских мостах, 1736 год)

Четыре части суши соединяют семь мостов.



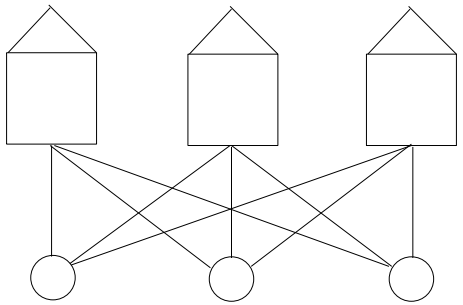
Необходимо обойти все части суши, пройдя по каждому мосту один раз, и вернуться в исходную точку.

Граф задачи Эйлера



Пример (Задача о трёх домах и трёх колодцах)

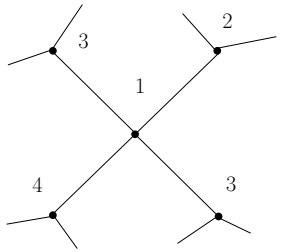
Необходимо провести от каждого дома к каждому колодцу тропинку так, чтобы тропинки не пересекались.



Решение для более общей задачи о планарности графа было получено независимо Понтрягиным в 1927 и Куратовским в 1930 году.

Пример (Задача о четырёх красках)

Необходимо раскрасить карту, используя четыре краски, так, чтобы никакие две соседние области не были закрашены одним цветом. Вершины графа – области, ребра – границы. Необходимо расставить в вершинах графа цифры 1,2,3,4 так, чтобы рядом не было двух одинаковых цифр



Решение было получено в 1976 году с применением компьютера. Авторы: Аппель, Хакен.

Определение

Ребро $e = (v, v)$ называется петлей.

Определение

Граф без петель и кратных ребер называется простым.

Определение

Граф без петель, но с кратными ребрами называется мультиграфом.

Определение

Граф с петлями и кратными ребрами называется псевдографом.

Определение

Если множество ребер состоит из упорядоченных пар, то граф называется ориентированным (орграфом). Ребра орграфа называются дугами.

Ориентированный граф без кратных рёбер задаёт бинарное отношение на множестве вершин графа.

Определение

Если каждому ребру приписано некоторое неотрицательное число, то граф называется взвешенным (нагруженным).

Весом или стоимостью графа называется сумма весов его ребер.

Определение

Две вершины называются смежными, если существует ребро, соединяющее эти вершины.
Два ребра, примыкающие к одной вершине, называются смежными.
Вершина и примыкающее к ней ребро называются инцидентными.

Определение

Число ребер, инцидентных вершине v, называется степенью вершины и обозначается $d(v)$.

Определение

Для ориентированного графа число дуг, исходящих из вершины v, называется полустепенью исхода, а входящих – полустепенью захода. Эти числа обозначаются соответственно $d^-(v)$ и $d^+(v)$.

Определение

Маршрутом в графе называется чередующаяся последовательность вершин и ребер.

$$v_1 e_1 v_2 e_2 v_3 \dots e_{k-1} v_k,$$

в которой любые два соседних элемента инцидентны.

Определение

Цепью называется маршрут, в котором все ребра различны.

Определение

Цепь называется простой, если все вершины в этой цепи различны. Простую цепь можно описать в виде последовательности вершин

$$v_1 v_2 \dots v_k.$$

Определение

Замкнутая цепь называется циклом.
Замкнутая простая цепь называется простым циклом.
Цикл, который содержит все ребра графа, называется эйлеровым.
Простой цикл, который проходит через все вершины графа, называется гамильтоновым.

Определение

Граф без циклов называется ациклическим.

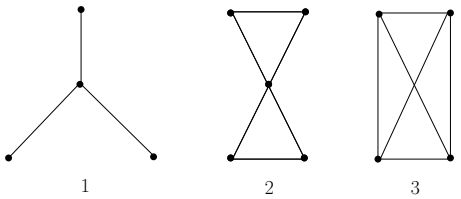
Определение

Граф с эйлеровым циклом называется эйлеровым.

Определение

Граф с гамильтоновым циклом называется гамильтоновым.

Пример



1 – ациклический граф; 2 – эйлеров граф; 3 – гамильтонов граф

Определение

Длиной маршрута называется количество ребер в нём с учётом повторений.
Расстоянием между двумя вершинами называется длина кратчайшей цепи, связывающей эти вершины.

Для нагруженного графа длина маршрута равна сумме весов ребер, составляющих маршрут.

Определение

Диаметром графа называется максимальное расстояние между вершинами графа.

Определение

Две вершины связаны, если существует соединяющая их цепь. Граф, в котором все вершины связаны, называется связным.

Определение

Компонентой связности графа называется множество вершин графа таких, что любые две вершины из этого множества связаны и никакая из этих вершин не связана с оставшимися вершинами графа.

Определение

Путь в ориентированном графе есть ориентированная цепь.
В простом ориентированном графе вершина u называется достижимой из вершины v, если существует путь, ведущий из v в u.

Определение

Граф, в котором каждые две вершины смежны, называется полным. Полный граф с n вершинами обозначают K_n.

Число рёбер в простом полном графе равно $n(n-1)/2$.

Определение

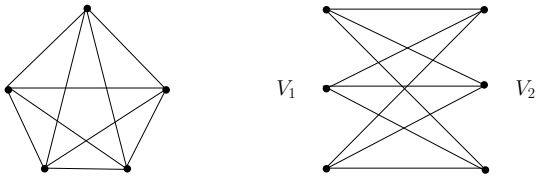
Двудольный граф $G = \langle V, E \rangle$ содержит два подмножества вершин V_1 и V_2 такие, что $V = V_1 \bigcup V_2$, $V_1 \bigcap V_2 = \emptyset$. При этом каждое ребро $e \in E$ инцидентно вершине из V_1 и вершине из V_2.

Определение

Двудольный граф $G = \langle V_1, V_2, E \rangle$ называется полным, если любые две вершины из множеств V_1 и V_2 смежны. Полный двудольный граф обозначают $K_{n,m}$, где n число вершин в V_1, m – число вершин в V_2.

Число рёбер в полном двудольном графе равно nm.

Пример



1 2

1 – полный граф K_5; 2 – полный двудольный двудольный граф $K_{3,3}$.

Определение

Неориентированный граф без циклов называется деревом.

Дерево с n вершинами всегда содержит $n-1$ ребро.

Определение

Несвязный неориентированный граф без циклов называется лесом.

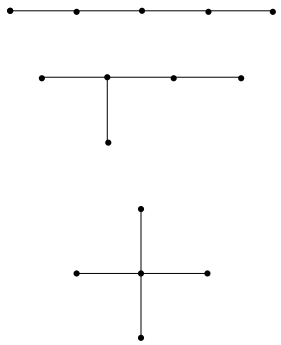
Определение

Дерево с выделенным корнем называется ориентированным.

Определение

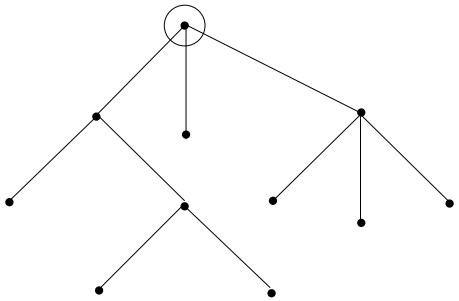
Бинарное (двоичное) дерево – это дерево с корнем, которое можно разбить на три части: корень, левое бинарное дерево и правое бинарное дерево, каждое из которых может быть пустым.

Пример



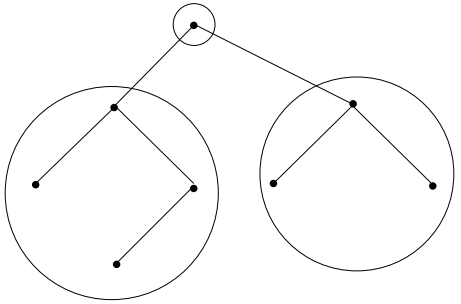
Деревья с пятью вершинами

Пример



Ориентированное дерево

Пример



Бинарное дерево

Определение

Подграфом графа $G = \langle V, E \rangle$ называется граф $G' = \langle V', E' \rangle$ такой, что $V' \subseteq V$, $E' \subseteq E$.

Определение

Полный подграф некоторого графа называется кликой этого графа.

Определение

Максимальная клика графа – это клика с максимально возможным числом вершин.

Определение

Подграф $G' = \langle V', E' \rangle$ графа $G = \langle V, E \rangle$ называется остовным деревом графа, если он содержит все вершины графа $V' = V$ и является деревом.

Если n – число вершин, а m – число ребер графа G, то любое его остовное дерево имеет n вершин и $n - 1$ ребер.

Число $\gamma = m - n + 1$ называется цикломатическим числом графа G.

Определение

Графы $G_1 = \langle V_1, E_1 \rangle$ и $G_2 = \langle V_2, E_2 \rangle$ называются изоморфными, если существуют биекции

$$f : V_1 \leftrightarrow V_2, \; g : E_1 \leftrightarrow E_2$$

такие, что $G_2 = \langle f(V_1), g(E_1) \rangle$.

Два графа различны, если они не изоморфны.

5.2 Представления графов

1) Матрица смежности
2) Матрица инцидентности
3) Список ребер
4) Список смежности

Пусть $G = \langle V, E \rangle$ – граф с n вершинами и m ребрами

Матрица смежности графа

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix},$$

$$a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ 0, & (v_i, v_j) \notin E \end{cases}$$

Матрица инцидентности

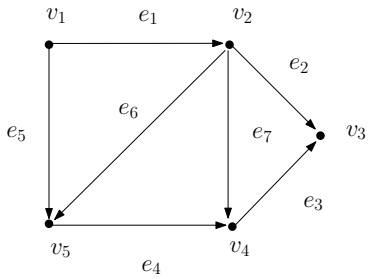
$$B = \begin{bmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nm} \end{bmatrix}$$

Для неориентированного графа $b_{ij} = 1$, если вершина v_i и ребро e_j инцидентны. Иначе $b_{ij} = 0$.

Для ориентированного графа:

$b_{ij} = -1$, если вершина v_i и ребро $e_j = (v_i, v_k)$ инцидентны;
$b_{ij} = 1$, если вершина v_i и ребро $e_j = (v_k, v_i)$ инцидентны;
$b_{ij} = 0$, если вершина v_i и ребро e_j не инцидентны.

Пример



Матрица смежности

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Матрица инцидентности

$$B = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{bmatrix} -1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Список рёбер

$$R = \begin{bmatrix} 1 & 1 & 2 & 2 & 2 & 4 & 5 \\ 2 & 5 & 5 & 3 & 4 & 3 & 4 \end{bmatrix}$$

Список смежности (массив связанных списков)

начало 1 $\to$ 2 $\to$ 5 конец
начало 2 $\to$ 3 $\to$ 4 $\to$ 5 конец
начало 3 конец
начало 4 $\to$ 3 конец
начало 5 $\to$ 4 конец

5.3 Основные теоремы

Теорема (Эйлер)

Сумма степеней вершин графа равна удвоенному числу рёбер

$$\sum_{v \in V} d(v) = 2|E|.$$

Теорема

В любом графе число вершин нечётной степени чётно.

Теорема

Граф является двудольным тогда и только тогда, когда все его простые циклы имеют чётную длину.

Теорема

Связный граф является эйлеровым тогда и только тогда, когда каждая вершина графа имеет чётную степень.

Рассмотрим простые графы с числом вершин $n \geq 3$.

Теорема (Дирак)

Если в графе степень любой вершины $d(v) \geq n/2$, то граф является гамильтоновым.

Теорема (Оре)

Если в графе для любых двух несмежных вершин $d(v_i) + d(v_j) \geq n$, то граф является гамильтоновым.

Определение

Граф называется планарным, если его можно изобразить на плоскости без пересечения рёбер.

Теорема (Формула Эйлера)

Число областей (граней), на которые планарный граф разбивает плоскость, равно

$$f = m - n + 2,$$

где n – число вершин, m – число рёбер.

Теорема

Полный граф с пятью вершинами K_5 и полный двудольный граф $K_{3,3}$ не являются планарными.

Определение

Два графа называются гомеоморфными, если они оба могут быть получены из одного графа, включением в его рёбра новых вершин степени 2.

Теорема (Понтрягин, 1927, Куратовский, 1930)

Граф является планарным тогда и только тогда, когда он не содержит подграфа, гомеоморфного графу K_5 или графу $K_{3,3}$.

Теорема

Граф является планарным тогда и только тогда, когда он не содержит подграфа, стягиваемого к графу K_5 или графу $K_{3,3}$.

5.4 Алгоритмы на графах

Задача обхода графа.

Задан простой неориентированнй граф. Необходимо обойти все вершины графа, начиная с заданной начальной вершины.

Метод поиска в глубину.

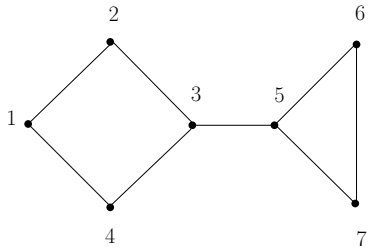
Начинаем с заданной вершины v. Переходим в любую вершину u, смежную с v. Из вершины u переходим в следующую вершину и т.д.

Если нет возможности перейти в новую вершину, то последнюю вершину отмечаем как использованную и возвращаемся на один шаг назад.

Продолжаем, пока не вернёмся в исходную вершину.

Рассматриваемые вершины образуют стек («последний пришёл – первый ушёл»). В начале стека находится вершина v.

Пример (Метод поиска в глубину)



Протокол работы алгоритма поиска в глубину оформим в виде таблицы. Обозначим: НВ – новая вершина, ИВ – использованная вершина, НН – новых вершин нет.
Начальная вершина – 3.

Стек	НВ	ИВ
3	5	
3,5	6	
3,5,6	7	
3,5,6,7	НН	7
3,5,6	НН	6
3,5	НН	5
3	2	
3,2	1	
3,2,1	4	
3,2,1,4	НН	4
3,2,1	НН	1
3,2	НН	2
3	НН	3

Метод поиска в ширину.

Пусть v – начальная вершина. Отметим все соседние с v вершины. Для каждой из этих вершин рассмотрим свои соседние вершины, которых ещё нет в списке отмеченных, и т.д. Продолжаем, пока не закончатся все вершины.

В методе поиска в ширину вершины образуют очередь («первый пришёл – первый ушёл»).

Пример

Очередь	НВ	ИВ
3	2,4,5	3
2,4,5	1	2
4,5,1	НН	4
5,1	6,7	5
1,6,7	НН	1
6,7	НН	6
7	НН	7

Задача о нахождении кратчайшего пути.

Пусть $G = \langle V, E \rangle$ – взвешенный ориентированный граф без петель. Заданы веса дуг $\rho(u, v) \geq 0$. Необходимо найти кратчайшие пути от заданной вершины s до всех вершины графа.

Алгоритм Дейкстры.

Алгоритм основан на свойстве кратчайшего пути. Обозначим через $d(u, v)$ длину кратчайшего пути из вершины u в вершину v. Пусть кратчайший путь из вершины s в вершину v проходит через вершину w. Тогда

$$d(s, v) = d(s, w) + d(w, v).$$

Каждой вершине присваиваются метки. Метка вершины $m(v)$ обозначает оценку длины пути от s до v. Метки пересчитываются по мере обхода графа в ширину. Окончательные значения меток будут равны кратчайшим расстояниям.

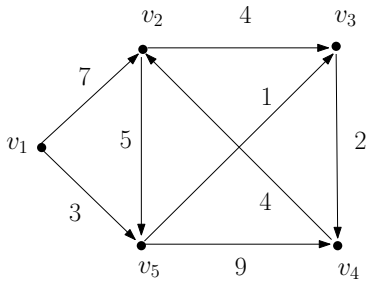
1) Присваиваем $m(s) = 0$ и $m(v) = \infty$ для всех остальных вершин.
2) Создаём множество вершин $S = \{\emptyset\}$. Во множестве S будут накапливаться вершины, для которых кратчайший путь определен.
3) Во множестве $V \setminus S$ определяем вершину w с минимальной меткой. Включаем её во множество S. На первом шаге это будет вершина s.
4) Пересчитываем метки тех вершин $v \in V \setminus S$, для которых существуют дуги (w, v), по правилу

$$m(v) = \min\{m(v), m(w) + \rho(w, v)\}$$

5) Повторяем п. 3. Останавливаемся, если множество S нельзя изменить.

Пример (Алгоритм Дейкстры)

Для графа



определим кратчайшие пути от вершины v_1 до всех остальных вершин графа. Протокол работы алгоритма Дейкстры оформим в виде таблицы.

Шаг	S	$V \setminus S$	$m(v_1)$	$m(v_2)$	$m(v_3)$	$m(v_4)$	$m(v_5)$
0	$\emptyset$	$v_1 v_2 v_3 v_4 v_5$	0	∞	∞	∞	∞
1	v_1	$v_2 v_3 v_4 v_5$	0	7	∞	∞	$\boxed{3}$
2	$v_1 v_5$	$v_2 v_3 v_4$	0	7	$\boxed{4}$	12	3
3	$v_1 v_5 v_3$	$v_2 v_4$	0	7	4	$\boxed{6}$	3
4	$v_1 v_5 v_3 v_4$	v_2	0	7	4	6	3
5	$v_1 v_5 v_3 v_4 v_2$	$\emptyset$	0	7	4	6	3

Последняя строка таблицы содержит значения длин кратчайших путей. Сами кратчайшие пути можно построить начиная с конечных вершин:

$$v_1 - v_2$$
$$v_1 - v_5 - v_3$$
$$v_1 - v_5 - v_3 - v_4$$
$$v_1 - v_5$$

Задача построения остовного дерева минимального веса.

Задан простой неориентированный взвешенный граф $\langle V, E \rangle$ с функцией весов ребер $f(v_i, v_j) > 0$, $(v_i, v_j) \in E$. Необходимо построить остовное дерево минимального веса.

Алгоритм Прима.

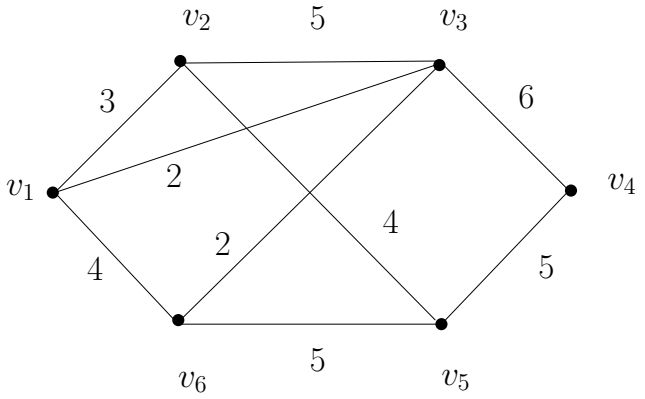
Выбираем одну из вершин графа в качестве корневой вершины дерева. Создаём дерево состоящее только из этой вершины.

На каждом шаге алгоритма к текущему дереву добавляем ребро наименьшего веса, соединяющее вершину из множества вершин дерева U и множества $V \setminus U$.

В процессе построения дерева образуется очередь рёбер с приоритетом, задаваемым весами рёбер.

Пример (Алгоритм Прима)

Для графа

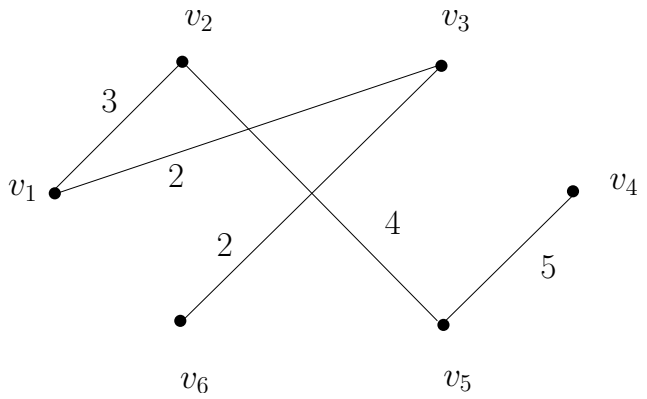


построить остовное дерево минимального веса.

Шаг	U	Очередь	$V \setminus U$
1	v_1	$f(v_1, v_3) = 2$ $f(v_1, v_2) = 3$ $f(v_1, v_6) = 4$	$v_2 v_3 v_4 v_5 v_6$
2	$v_1 v_3$	$f(v_3, v_6) = 2$ $f(v_1, v_2) = 3$ $f(v_1, v_6) = 4$ $f(v_3, v_2) = 5$ $f(v_3, v_4) = 6$	$v_2 v_4 v_5 v_6$

3	$v_1 v_3 v_6$	$f(v_1, v_2) = 3$ $f(v_3, v_2) = 5$ $f(v_6, v_5) = 5$ $f(v_3, v_4) = 6$	$v_2 v_4 v_5$
4	$v_1 v_3 v_6 v_2$	$f(v_2, v_5) = 4$ $f(v_6, v_5) = 5$ $f(v_3, v_4) = 6$	$v_4 v_5$
5	$v_1 v_3 v_6 v_2 v_5$	$f(v_5, v_4) = 5$ $f(v_3, v_4) = 6$	v_4
6	$v_1 v_3 v_6 v_2 v_5 v_4$		

Остовное дерево



Вес дерева равен 16.

5.5 Алгоритмы анализа графа Веб

Пусть дана коллекция гипертекстовых документов, например, веб-архив поисковой системы интернета.

Данную коллекцию документов представим в виде простого ориентированного графа $G = \langle V, E \rangle$. Вершинами графа являются документы (веб страницы), дугами – ссылки на документы.

Вершины графа обозначим номерами $i = 1, 2, \ldots, n$, дуги ссылками $i \to j$.

Необходимо определить ранги документов в виде неотрицательных чисел

$$p_i \geq 0, \quad \sum_{i=1}^{n} p_i = 1.$$

Алгоритм PageRank – алгоритм ранжирования графа Веб поисковой системы Google

Авторы – Сергей Брин, Ларри Пейдж, основатели компании Google, 1998 год.

Расчет рангов выполняется рекурсивно по правилу

$$p_i(k+1) = \alpha \sum_{j \to i} \frac{p_j(k)}{d_j^- + 1} + \frac{1-\alpha}{n}, \quad k = 0, 1, \ldots,$$

где d_j^- – полустепень исхода вершины j, $0 < \alpha < 1$ – параметр алгоритма.

Сумма вычисляется по всем ссылкам, ведущим на документ i. В том числе сумма содержит слагаемое

$$\frac{p_i(k)}{d_i^- + 1}.$$

Последнее требование необходимо для выполнения условия нормирования

$$\sum_{i=1}^{n} p_i = 1.$$

Начальные значения рангов

$$p_i(0) = \frac{1}{n}, \quad i = 1, 2, \ldots, n$$

Алгоритму PageRank можно дать следующую интерпретацию, основанную на модели случайного пользователя.

Пользователь начинает свое движение по Вебу со случайно выбранной страницы.

Ранг страницы интерпретируется как вероятность нахождения пользователя на данной странице.

Пользователь осуществляет свое движение по графу Веб согласно следующему правилу.

Пусть в момент времени k пользователь находится на странице j. Тогда в момент времени $k+1$ с вероятностью α он переходит на одну из d_j^- страниц, на которые ссылается страница j, или остается на странице j.

С вероятностью $1 - \alpha$ он начинает новое движение по Вебу, выбрав случайным образом начальную страницу. Выбор ссылки и выбор страницы для перехода осуществляется с равной вероятностью.

Векторно-матричная форма записи алгоритма PageRank.

Обозначим через L матрицу смежности графа. Составим матрицу $\bar{L} = L + E$, где E – единичная матрица.

Обозначим через A матрицу с элементами

$$a_{ij} = \frac{\bar{L}_{ji}}{d_j^- + 1}, \quad i = 1, \ldots, n, \quad j = 1, \ldots, n.$$

Составим векторы

$$p(k) = \begin{bmatrix} p_1(k) \\ p_2(k) \\ \vdots \\ p_n(k) \end{bmatrix}, \quad e = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}.$$

Алгоритм PageRank в векторно-матричной форме принимает следующий вид

$$p(k+1) = \alpha A p(k) + \frac{1-\alpha}{n} e, \quad k = 0, 1, \ldots$$

При $k \to \infty$ получим систему линейных алгебраических уравнений

$$p = \alpha A p + \frac{1-\alpha}{n} e,$$

или

$$(E - \alpha A) p = \frac{1-\alpha}{n} e.$$

Следовательно, ранги страниц равны

$$p = (E - \alpha A)^{-1} \frac{1-\alpha}{n} e.$$

Алгоритм HITS (Hyperlink Induced Topic Search).

Автор – Джон Клейнберг, 1999 г.

Для каждой страницы вычисляются два ранга:

- p_i – ранг лидера (authority);
- q_i – ранг посредника (hub).

Вычисляются ранги последовательно по формулам

$$p_i(k+1) = \sum_{j \to i} q_j(k), \quad q_i(k+1) = \sum_{i \to j} p_j(k), \quad k = 0, 1, \ldots.$$

В векторно-матричной форме

$$p(k+1) = L^T q(k), \quad q(k+1) = L p(k), \quad k = 0, 1, \ldots$$

На каждом шаге вычислений выполняется нормирование векторов p и q по следующему правилу

$$p(k) = p(k) \Big/ \sum_{i=1}^{n} p_i(k), \quad q(k) = q(k) \Big/ \sum_{i=1}^{n} q_i(k).$$