



Уральский
федеральный
университет

имени первого Президента
России Б.Н. Ельцина

Уральский
энергетический
институт

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Учебное пособие



Министерство образования и науки Российской Федерации
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Рекомендовано
методическим советом УрФУ
в качестве **учебного пособия** для студентов,
обучающихся по направлениям подготовки
231300 — Прикладная математика
141100 — Энергетическое машиностроение
140400 — Электроэнергетика и электротехника
140100 — Теплоэнергетика и теплотехника
141403 — Атомные станции: проектирование,
эксплуатация и инжиниринг
280700 — Техносферная безопасность

Екатеринбург
Издательство Уральского университета
2015

УДК 519.1(075.8)

ББК 22.176я73

Э45

Рецензенты:

кафедра высшей и прикладной математики Уральского государственного университета путей сообщения (завкафедрой, д-р физ.-мат. наук проф. **Г. А. Тимофеева**);

д-р физ.-мат. наук, зам. директора ИММ УрО РАН **В. Т. Шевалдин**

Научный редактор — д-р физ.-мат. наук проф. **А. Н. Сесекин**

Элементы дискретной математики : учебное пособие / Д. С. Ананичев, Э45 И. Ю. Андреева, Н. В. Гредасова, К. В. Костоусов. — Екатеринбург : Изд-во Уральского университета, 2015. — 108 с.

ISBN 978-5-7996-1387-7

В учебном пособии рассматриваются элементы дискретной математики: логические исчисления, предикаты, булевы функции, комбинаторика, теория графов, автоматы и алгоритмы. Приведено решение типовых задач.

Предназначается для студентов всех форм обучения всех специальностей.

УДК 519.1(075.8)

ББК 22.176я73

ISBN 978-5-7996-1387-7

© Уральский федеральный
университет, 2015

1. Логические исчисления

Множество, отношения, функции

Множества

Множество — совокупность объектов (элементов).

Множества A, B, \dots

Элементы a, b, c, \dots

$a \in A$ a — элемент A (a принадлежит A).

$a \notin A$ a — не элемент A (a не принадлежит A).

Основное свойство множеств

Для любых a и A выполняется ровно одно из двух условий: $a \in A$, $a \notin A$.

Способы задания множеств

1. Перечисление элементов:

$A = \{0, 1, 2, 3, \dots, 9\}$.

$B = \{\text{красный, синий, зеленый}\}$.

$C = \{\text{борода, шляпа, очки}\}$.

Можно задать лишь конечные множества.

2. Определяющие свойства:

$A = \{x \mid x \text{ — десятичная цифра}\}$.

$N = \{x \mid x \text{ — натуральное число}\}$.

$Z = \{x \mid x \text{ — целое}\}$.

$N_0 = \{x \mid x \in Z, x \geq 0\}$.

$Q = \{\frac{m}{n} \mid m \in Z, n \in N\}$.

$R = \{x \mid x \text{ — действительное число}\}$.

$C = \{x \mid x \text{ — комплексное число}\}$.

$(2,3) = \{x \mid x \in R, x^2 - 5x + 6 < 0\}$.

Пример

$1 \in \{1, 2, 3\}$ — верно.

$1 \in \{\{1\}, \{2\}, \{3\}\}$ — не верно.

Элементы множества $\{\{1\}, \{2\}, \{3\}\}$ — это множества (а не числа).

Пример

Рассмотрим $S = \{X \mid X \notin X\}$.

Допустим, что $S \notin S$, тогда элемент S удовлетворяет определяющему свойству множества S , следовательно, $S \in S$. Противоречие. Допустим, что $S \in S$, тогда элемент S не удовлетворяет определяющему свойству множества S , следовательно, $S \notin S$. Опять противоречие. Таким образом, S не удовлетворяет основному свойству множества.

Проблема записи определяющим свойством — это чрезмерная сила.

$\emptyset = \{x \mid x \neq x\}$ — *пустое множество* — множество без элементов. $\forall a$

U — *универсальное множество* — множество, содержащее все интересующие нас в данный момент элементы. $\forall a \quad a \in U$.

$A \subseteq B$ — A подмножество B ; B надмножество A , если $\forall a$

$A \not\subseteq B \quad \exists a \quad a \in A \text{ и } a \notin B$.

Лемма 1

$\forall A$ 1) $\emptyset \subseteq A$.

2) $A \subseteq A$.

3) $A \subseteq U$.

Доказательство:

1) от противного (о/п).

$\emptyset \not\subseteq A \rightarrow \exists a \quad a \in \emptyset, a \notin A$.

2) очевидно.

3) по определению U .

$A = B$ (A равно B), если множества A и B состоят из одних и тех же элементов.

Замечание

$$A = B \Leftrightarrow \begin{cases} A \subseteq B \\ B \subseteq A \end{cases}$$

Операции с множествами

A, B — множества.

$A \cap B = \{x \mid x \in A, x \in B\}$ — пересечение множеств A и B .

$A \cup B = \{x \mid x \in A \text{ или } x \in B\}$ — объединение множеств A и B .

$x \in A$ или $x \in B$ означает, что выполняется хотя бы одно из двух.

$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$ — разность множеств A и B .

$\bar{A} = U \setminus A = \{x \mid x \notin A\}$ — дополнение до A .

Свойства $\forall A, B, C$

Коммутативности

$$1) A \cup B = B \cup A$$

$$1') A \cap B = B \cap A$$

Ассоциативности

$$2) (A \cup B) \cup C = A \cup (B \cup C)$$

$$2') (A \cap B) \cap C = A \cap (B \cap C)$$

Дистрибутивности

$$3) (A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

$$3') (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

Идемпотентности

$$4) A \cup A = A$$

$$4') A \cap A = A$$

Свойства нуля

$$5) A \cup \emptyset = A$$

$$5') A \cap \emptyset = \emptyset$$

Свойства единицы

$$6) A \cup U = U$$

$$6') A \cap U = A$$

Свойства дополнения

$$7) A \cup \bar{A} = U$$

$$7') A \cap \bar{A} = \emptyset$$

Свойство двойного дополнения

$$8) \bar{\bar{A}} = A$$

Тождества поглощения

$$9) A \cup (A \cap B) = A$$

$$9') A \cap (A \cup B) = A$$

Законы де Моргана

$$10) \overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$10') \overline{A \cap B} = \bar{A} \cup \bar{B}$$

Доказательство 2':

Докажем \subseteq : $\forall x \ x \in (A \cap B) \cap C$

$$(\text{по определению } \cap) \rightarrow \begin{cases} x \in A \cap B \\ x \in C \end{cases}$$

$$(\text{по определению } \cap) \rightarrow \begin{cases} x \in A \\ x \in B \\ x \in C \end{cases}$$

$$(\text{по определению } \cap) \rightarrow \begin{cases} x \in A \\ x \in B \cap C \end{cases}$$

$$(\text{по определению } \cap) \rightarrow x \in A \cap (B \cap C).$$

Докажем \supseteq : нужно развернуть стрелки.

Лемма 2

$$\forall A, B \text{ и } A \cap B \subseteq A \subseteq A \cup B.$$

Доказательство: непосредственно следует из определения.

Лемма 3

$$1) A \subseteq B.$$

$$2) A \cap B = A.$$

$$3) A \cup B = B.$$

Данные условия эквивалентны.

Доказательство:

$$1) \rightarrow 2):$$

докажем \subseteq : по Лемме 2,

$$\text{докажем } \supseteq : \left. \begin{matrix} a \in A \\ A \subseteq B \end{matrix} \right\} \rightarrow a \in B \rightarrow a \in A \cap B.$$

$$2) \rightarrow 1): A = A \cap B \text{ (по Лемме 2)} \subseteq B \text{ (по свойству 1')}. \quad \square$$

Лемма 4

$$\forall A, B, C \text{ и } A \subseteq B \Rightarrow \begin{cases} A \cap C \subseteq B \cap C \\ A \cup C \subseteq B \cup C \end{cases} \text{ (стабильность } \subseteq \text{ относительно } \cap \text{ и } \cup).$$

Доказательство:

$$\forall x \ x \in A \cap C \text{ (по определению } \cap)$$

$$\rightarrow \begin{cases} x \in A \text{ (по определению } \subseteq) \\ x \in C \end{cases} \rightarrow \begin{cases} x \in B \\ x \in C \end{cases} \rightarrow x \in B \cap C$$

$\forall x \ x \in A \cup C \ x \in A \rightarrow A \subseteq B \rightarrow x \in B$ (по Лемме 2) $\subseteq B \cup C$ или $x \in C$ (по Лемме 2) $\subseteq B \cup C$.

Следствие из Леммы 4

$$\begin{cases} A \subseteq B \\ C \subseteq D \end{cases} \rightarrow \begin{cases} A \cap C \subseteq B \cap D \\ A \cup C \subseteq B \cup D \end{cases}$$

Доказательство:

$$A \cap C \text{ (по Лемме 4)} \subseteq B \cap C \text{ (по Лемме 4)} \subseteq B \cap D.$$

Доказательство свойства 4:

По Лемме 1 $A \subseteq A$ вместе с Леммой 3 получаем $A \cup A = A$.

Доказательство свойства 6:

По Лемме 1 $\emptyset \subseteq A$ вместе с Леммой 3 получаем $A \cup \emptyset = A$.

Доказательство свойства 9':

По Лемме 2 $A \subseteq A \cup B$ вместе с Леммой 3 $A \cap (A \cup B) = A$.

Доказательство свойства 3:

Сначала докажем \supseteq :

$$A \cap C \text{ (по Лемме 2)} \subseteq C.$$

$$B \cap C \subseteq C$$

$$(A \cap C) \cup (B \cap C) \text{ (последствию из Леммы 4)} \subseteq C \cup C \text{ (по свойству 4)} = C.$$

$$A \cap C \text{ (по Лемме 2)} \subseteq A \text{ (по Лемме 2)} \subseteq A \cup B.$$

$$B \cap C \text{ (по Лемме 2)} \subseteq B \text{ (по Лемме 2)} \subseteq A \cup B.$$

$$\begin{aligned} (A \cap C) \cup (B \cap C) \text{ (по следствию из Леммы 4)} &\subseteq (A \cup B) \cup (A \cup B) \\ \text{(по свойству 4)} &= (A \cup B). \end{aligned}$$

$$Z = (A \cap C) \cup (B \cap C).$$

$$\left. \begin{array}{l} Z \subseteq C \\ Z \subseteq (A \cup B) \end{array} \right\} \Rightarrow Z \text{ (по свойству 4')} = Z \cap Z$$

$$\text{(последствию из Леммы 4)} \subseteq (A \cup B) \cap C.$$

Теперь докажем \subseteq :

$$\forall x \ x \in (A \cup B) \cap C \Rightarrow \begin{cases} x \in A \cup B \\ x \in C \end{cases}$$

$$\begin{cases} x \in A \\ x \in C \end{cases} \rightarrow x \in A \cap C \subseteq Z.$$

Или

$$\begin{cases} x \in B \\ x \in C \end{cases} \rightarrow x \in B \cap C \subseteq Z.$$

Булеан $B(A)$ множества A — это множество всех его подмножеств.

Отношения

Упорядоченная пара элементов $x, y: (x, y) = \{\{x, y\}, \{x\}\}$.

Основное свойство

$$(x, y) = (z, t) \Leftrightarrow \begin{cases} x = z \\ y = t \end{cases}$$

Доказательство

1-й случай:

$$x = y$$

$$(x, y) = (x, x) = \{\{x\}\} = \{\{z, t\}, \{z\}\} \rightarrow \{z, t\} \text{ —}$$

одноэлементное множество $z = t = \{\{z\}\}$, значит $x = z$, $y = t$.

2-й случай:

$$x \neq y$$

$$\{\{x, y\}, \{x\}\} = \{\{z, t\}, \{z\}\} \Rightarrow \{x, y\} = \{z, t\}$$

Отсюда $\{z, t\}$ —

2-элементное множество

$$\Rightarrow \{x\} \neq \{z, t\} \rightarrow \{x\} = \{z\} \rightarrow x = z; y \neq x \Rightarrow y = t.$$

Отождествим $(x_1, (x_2, x_3))$ и $((x_1, x_2), x_3)$.

Упорядоченная цепочка элементов $x_1, x_2, x_3, \dots, x_n$ — это

$$(x_1, x_2, x_3, \dots, x_n) = ((x_1, x_2, \dots, x_{n-1}), x_n).$$

Прямое произведение A и B

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid \forall i \in \{1 \dots n\} a_i \in A_i\}.$$

Чтобы задать отношение, достаточно указать все пары объектов, которые оно связывает.

Бинарное отношение ρ на множествах A и B — это $\rho \subseteq A \times B$.

N -арное отношение ρ — это $\rho \subseteq A_1 \times A_2 \times \dots \times A_n$.

Если $A_1 = A_2 = A_3 = \dots = A_n = A$, то $A_1 \times A_2 \times \dots \times A_n = A^n$ и $\rho \subseteq A^n$ ρ — n -местное отношение на A .

Отношение ρ на A :

рефлексивное, если $\forall x \in A \ x \rho x$;

симметричное, если $\forall x, y \in A \ x \rho y \rightarrow y \rho x$;

антисимметричное, если $\forall x, y \in A \begin{cases} x \rho y \\ y \rho x \end{cases} \rightarrow x = y$;

транзитивное, если $\forall x, y, z \in A \begin{cases} x \rho y \\ y \rho z \end{cases} \rightarrow x \rho z$.

Примеры

1) « $=$ » на \mathbf{Z} .

2) « \leq » на \mathbf{Z} .

3) « \subseteq » на $\mathbf{B}(A)$.

4) ρ соответствует фразе «...учится в одной группе с...» на множестве всех студентов университета.

5) ρ соответствует фразе «...одного года рождения с...» на множестве всех людей.

6) « \parallel » на \mathbf{Z} .

7) «сравнимо по модулю n » на \mathbf{Z} .

8) « $<$ » на \mathbf{Z} .

$\rho \subseteq A^2$ — эквивалентность, если ρ — рефлексивно, транзитивно, симметрично.

9) A — множество всех направленных отрезков на плоскости.

$$\overrightarrow{AB} \rho \overrightarrow{CD} \Leftarrow \begin{cases} \overrightarrow{AB} \uparrow \uparrow \overrightarrow{CD} \\ |\overrightarrow{AB}| = |\overrightarrow{CD}| \end{cases} \text{ — это эквивалентность.}$$

Вектор — множество всех сонаправленных отрезков одинаковой длины.

$$\vec{a} = [\overrightarrow{AB}] = \{\overrightarrow{xy} \mid \overrightarrow{xy} \overrightarrow{AB}\}.$$

$\rho \subseteq A^2$ — порядок, если ρ — рефлексивно, антисимметрично.

$R = \{A_i \mid i \in I\}$ — разбиение множества A , если:

$$1) \bigcup_{i \in I} A_i = A;$$

$$2) \forall i, j, i \neq j \rightarrow A_i \cap A_j = \emptyset.$$

$a \in A \ [a_\rho] = \{x \mid x \rho a\}$ — класс эквивалентности ρ (класс по порядку ρ элемента a).

$$A/\rho = \{[a]_\rho \mid a \in A\} \text{ — фактор множества } A \text{ по порядку } \rho.$$

Теорема (об отношениях эквивалентности)

1) ρ — эквивалентность на $A \Rightarrow \{[a]_\rho \mid a \in A\}$ — разбиение A .

2) $R = \{A_i \mid i \in I\}$ — разбиение $A \Rightarrow \rho: [x \rho y \Leftrightarrow \exists i \in I \ x \in A_i \text{ и } y \in A_i]$ — эквивалентности и $A/\rho = R$.

Доказательство

1) $\bigcup_{a \in A} [a]_\rho = A$ очевидно $\forall a \in A \ [a]_\rho \subseteq A$.

$$\bigcup_{a \in A} [a]_\rho \subseteq \bigcup_{a \in A} A = A \quad x \in A, \rho \text{ рефлексивно.}$$

$$x \rho x \Rightarrow x \in [x]_\rho \Rightarrow x \in \bigcup_{a \in A} [a]_\rho$$

Разные классы не пересекаются.

$$[a]_\rho \neq [b]_\rho.$$

О/П.

$$[a]_\rho \cap [b]_\rho \neq \emptyset \Rightarrow \exists c \in [a]_\rho \cap [b]_\rho \rightarrow \begin{cases} c \in [a] \rightarrow \{c \rho a \rightarrow \{a \rho c \rightarrow a \rho b\} \\ c \in [b] \rightarrow \{c \rho b \rightarrow \{b \rho c \rightarrow a \rho b\} \end{cases}$$

$$\forall x: x \in [a] \rightarrow \begin{cases} x \rho a \rightarrow x \rho b \rightarrow x \in [b], \text{ то есть } [a]_\rho \subseteq [b]_\rho. \\ a \rho b \end{cases}$$

Симметрично $[b]_\rho \subseteq [a]_\rho \Rightarrow [a]_\rho = [b]_\rho$ — противоречие.

2) $\forall x \in A \bigcup_{i \in j} A_i \Rightarrow \exists i \in I \ x \in A_i$ и $x \in A_i \Rightarrow x\rho x \Rightarrow \rho$ рефлексивно.

ρ очевидно симметрично.

$$\forall x, y, z \in A \begin{cases} x\rho y \\ y\rho z \end{cases} \rightarrow \begin{cases} \exists i \in I \ x \in A_i \text{ и } y \in A_i \\ \exists j \in I \ y \in A_j \text{ и } z \in A_j \end{cases} \rightarrow i \neq j \Rightarrow A_i \cap A_j = \emptyset,$$

но $y \in A_i \cap A_j \Rightarrow i = j \rightarrow \exists x \in A_i$ и $z \in A_i \rightarrow x\rho z$.

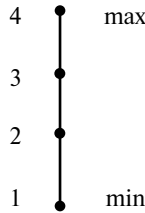
$A/\rho = R \subseteq \forall a \in A$ (надо показать, что $[a] \in R$) $A = \bigcup_{i \in I} A_i \Rightarrow \exists i \in I \ a \in A_i$
 $x \in [a] \rightarrow x\rho a \rightarrow \exists j \ x \in A_j$ и $a \in A_j \Rightarrow [i = j]$.

$$\begin{aligned} \exists i \quad & x \in A_i \Rightarrow [a] \subseteq A_i \\ & x \in A_i \rightarrow x\rho a \rightarrow x \in [a] \Rightarrow A_i = [a] \Rightarrow [a] = A_i, \end{aligned} \quad \text{то есть } [a] \in R.$$

$\supseteq \forall i \in I$ (надо $A_i \in A/\rho$) $a \in A_i \Rightarrow [a] = A_i$.

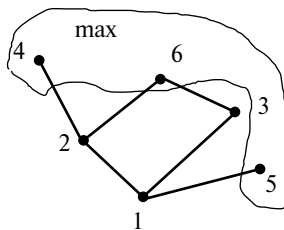
Структуры порядка

1) \leq на $\{1, 2, 3, 4\}$



Будем изображать элементы A точками на плоскости. Пусть они соответствуют элементу x , можно добраться по линиям снизу вверх до точки соответствует $y \Leftrightarrow x\rho y$, полученное изображение и есть структура порядка.

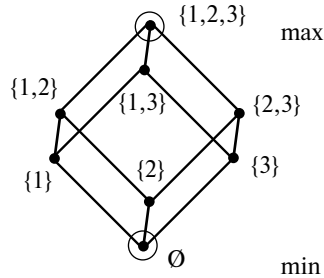
2) $|$ на $\{1, 2, 3, 4, 5, 6\}$



2,3 — несравнимы.

Наибольшего нет.

3) \subseteq на $\beta(\{1,2,3\})$:



Элемент $x \in A$ наибольший, если $\forall y \in A$ $y \leq x$ (x больше всех).

$x \in A$ наименьший, если $\forall y \in A$ $x \leq y$.

Элемент $x \in A$ максимальный, если $\forall y \in A$ $x \leq y \rightarrow x = y$ (нет элемента, $>$ чем x).

$x \in A$ минимальный, если $\forall y \in A$ $y \leq x \rightarrow x = y$.

Замечание 1

Наибольший — максимальный $\forall b \in P \begin{cases} a \leq b \\ b \leq a \end{cases} \rightarrow a = b$.

Замечание 2

Наибольший единственный a_1, a_2 — наибольший $\begin{cases} a_2 \leq a_1 \\ a_1 \leq a_2 \end{cases} \rightarrow a_1 = a_2$.

Операции с отношениями

1) $\cup, \cap, \setminus, -$

Пример

" $<$ " \cup " $=$ " " \leq "

" \leq " \cap " \geq " " $=$ " " $=$ "

" $<$ " \cup " $>$ " " $=$ " " \neq "

2) $\rho^{-1} = \{(x, y) \mid y \leq x\}$ — обратное к ρ отношение.

$\rho \subseteq A \times B \Rightarrow \rho^{-1} \subseteq B \times A$

Пример

$$" <^{-1} = " > "$$

$$" |^{-1} = " : "$$

$$x : y \Leftrightarrow \frac{x}{y} \in Z$$

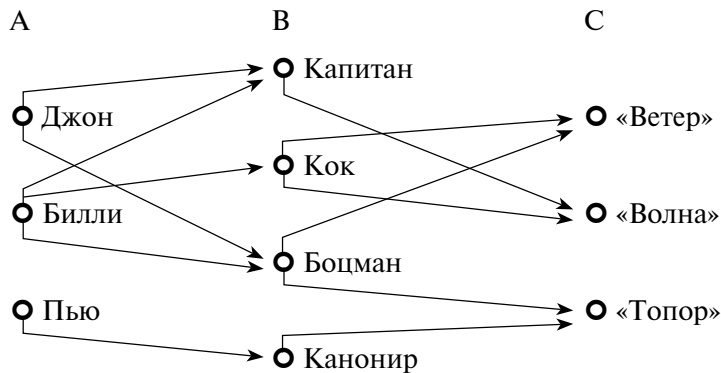
$$" =^{-1} = " = "$$
Замечание

$$(\rho^{-1})^{-1} = \rho$$

$$3) \rho \leq A \times B \quad \sigma \subseteq B \times C$$

$$\rho \cdot \sigma = \{(x, y) \mid \exists z \in B \quad x \rho z, z \sigma y\} \text{ — произведение отношений } \rho \text{ и } \sigma.$$

Пусть A — люди, B — должности, C — предприятия. Если ρ соответствует фразе «...способен быть...», σ соответствует фразе «...требуется на...», тогда ρ и σ соответствует фразе «...может наняться на...».

**Теорема (о связи свойств и операций)**

$$\rho \in A \times A.$$

1) ρ — рефлексивное $\Leftrightarrow \langle = \rangle \subseteq \rho$.

2) ρ — симметричное $\Leftrightarrow \rho^{-1} \subseteq \rho \Leftrightarrow \rho^{-1} = \rho$.

3) ρ — антисимметричное $\Leftrightarrow \rho \cap \rho^{-1} \subseteq \langle = \rangle$.

4) ρ — транзитивное $\Leftrightarrow \rho \cdot \rho \subseteq \rho$.

Доказательство:

2) $3 \rightarrow 2$ очевидно.

$2 \rightarrow 1 \quad \forall x, y \in A \quad x \rho y \text{ (по определению } \rho^{-1}) \rightarrow y \rho^{-1} x \rightarrow y \rho x.$

$1 \rightarrow 3$

докажем \subseteq : $(x, y) \in \rho^{-1} \rightarrow (y, x) \in \rho \rightarrow (x, y) \in \rho$.

докажем \supseteq : $(x, y) \in \rho \rightarrow (y, x) \in \rho \rightarrow (x, y) \in \rho^{-1}$.

$$3) \Rightarrow (x, y) \in \rho \cap \rho^{-1} \rightarrow \begin{cases} (x, y) \in \rho \\ (x, y) \in \rho^{-1} \end{cases} \rightarrow \begin{cases} xpy \\ ypx \end{cases} \rightarrow x = y \rightarrow (x, y) \in " = " .$$

$$\Leftarrow \forall x, y \begin{cases} xpy \\ ypx \end{cases} \rightarrow \begin{cases} xpy \\ x\rho^{-1}y \end{cases} \rightarrow (x, y) \in \rho \cap \rho^{-1} \rightarrow x = y .$$

$$4) \Rightarrow (x, y) \in \rho \cdot \rho \rightarrow \exists z \begin{cases} x\rho z \\ z\rho y \end{cases} \rightarrow xpy \rightarrow (x, y) \in \rho .$$

$$\Leftarrow \forall x, y, z \begin{cases} xpy \\ ypz \end{cases} \rightarrow x\rho \cdot \rho z \rightarrow x\rho z .$$

Функции

$$\rho \subseteq A \times B .$$

Область определения $\rho : D_\rho = \{a \in A \mid \exists b \in B, a\rho b\}$.

Область значений $\rho : E_\rho = \{b \in B \mid \exists a \in A, a\rho b\}$.

ρ — всюду определено, если $D_\rho = A$;

ρ — сюръективно, если $E_\rho = B$;

ρ — всюду определено $\forall a \in A \exists b \in B, a\rho b$.

Утверждение 1

$$D_\rho = E^{\rho^{-1}} = D_{\rho^{-1}} .$$

ρ — всюду определено $\Rightarrow \rho^{-1}$ сюръективно.

ρ — сюръективно $\Rightarrow \rho^{-1}$ всюду определено.

Доказательство очевидно.

Утверждение 2

$$\rho \subseteq A \times B, \quad \sigma \subseteq B \times C .$$

ρ, σ — всюду определено $\Rightarrow \rho \cdot \sigma$ — всюду определено.

ρ, σ — сюръективно $\Rightarrow \rho \cdot \sigma$ — сюръективно.

Доказательство:

$$\forall c \in C \xrightarrow{\sigma - \text{сюръективно}} \exists b \in B \text{ в } \sigma c \xrightarrow{\rho - \text{сюръективно}} \exists a \in A \text{ } a\rho b \Rightarrow a\rho\sigma c$$

$$\rho \subseteq A \times B.$$

$$\rho - \text{однозначное } \forall a \in A, b_1, b_2 \in B \begin{cases} a\rho b_1 \\ a\rho b_2 \end{cases} \rightarrow b_1 = b_2$$

$$\rho - \text{инъективное } \forall b \in B, a_1, a_2 \in A \begin{cases} a_1\rho b \\ a_2\rho b \end{cases} \rightarrow a_1 = a_2.$$

Утверждение 3

$$\rho - \text{однозначно} \rightarrow \rho^{-1} - \text{инъективно.}$$

$$\rho - \text{инъективно} \rightarrow \rho^{-1} - \text{однозначно.}$$

Утверждение 4

$$\rho, \sigma - \text{однозначно} \Rightarrow \rho \cdot \sigma - \text{однозначно.}$$

$$\rho, \sigma - \text{инъективно} \Rightarrow \rho \cdot \sigma - \text{инъективно.}$$

Доказательство:

$$\forall a \in A, c_1, c_2 \in C.$$

$$\begin{cases} a\rho\sigma c_1 \rightarrow \exists b_1 \begin{cases} a\rho b_1, b_1\sigma c_1 \end{cases} \\ a\rho\sigma c_2 \rightarrow \exists b_2 \begin{cases} a\rho b_2, b_2\sigma c_2 \end{cases} \end{cases} \xrightarrow{\rho - \text{однозначно}} b_1 = b_2 = b$$

$$\text{и } \begin{cases} b\sigma c_1 \\ b\sigma c_2 \end{cases} \xrightarrow{\sigma - \text{однозначно}} c_1 = c_2.$$

$\rho \subseteq A \times B$ — функция, если ρ — однозначно и всюду определено.

$\rho: A \rightarrow B$ (ρ — это функция, действующая из множества A в множество B).

$$(a, b) \in \rho \Leftrightarrow a\rho b \Leftrightarrow b = \rho(a).$$

ρ — инъективно — функция вложена.

$$\rho: A \rightarrow B.$$

ρ — сюръективно — функция « отображение на ».

$$\rho: A \rightarrow \succ B.$$

Биекция.

$$\rho: A \rightarrow \succ \rightarrow \succ B.$$

Теорема 1

$$f: A \rightarrow B, g: B \rightarrow C.$$

f, g — инъективные $\Rightarrow f \cdot g$ — инъективно.

f, g — сюръективные $\Rightarrow f \cdot g$ — сюръективно.

f, g — биекция $\Rightarrow f \cdot g$ — биекция.

Это следует из утверждений 2 и 4.

Теорема 2

$f: A \rightarrow B, f^{-1}: B \rightarrow A \Rightarrow f$ — биекция.

f — биекция $\Rightarrow f^{-1}$ — биекция.

Это следует из утверждений 1 и 3.

Замечание

Пусть множества A и B — конечные, $\varphi: A \rightarrow B$, тогда в множествах A и B будет одинаковое количество элементов.

Доказательство

$$\forall a \in A \exists! \alpha \in \varphi \alpha = (a, b).$$

В A и φ одинаковое количество элементов.

$$\forall b \in B \exists! \alpha \in \varphi \alpha = (x, b).$$

В B и φ одинаковое количество элементов.

$|A|$ — количество элементов в A .

$$\varphi: A \rightarrow B \Rightarrow |A| = |B|.$$

Пример

$M_{m,n}$ — множество кратчайших маршрутов между противоположными концами города размером m на n кварталов. Легко проверить, что

$$|M_{1,n}| = n+1 \quad |M_{2,2}| = 6 \quad |M_{m,n}| = ?$$

Анаграмма слова — это слово, полученное перестановкой букв.

ПОП \rightarrow ПОП

ОПП

ППО

$$A_{m,n} = \left\{ \omega \mid \omega - \text{анаграмма слова } \underbrace{\text{ПП} \dots \text{П}}_n \underbrace{\text{ВВ} \dots \text{В}}_m \right\}.$$

Легко проверить, что $|A_{1,n}| = n+1, |A_{2,2}| = 6, |A_{m,n}| = ?$

φ — правило:

идем вправо — пишем П;

идем вверх — пишем В.

$$\varphi: M_{m,n} \rightarrow A_{m,n}.$$

$$\varphi^{-1}: A_{m,n} \rightarrow M_{m,n}.$$

По Т2 φ — биекция.

$$|A_{m,n}| = |M_{m,n}|.$$

Пусть $\varphi: A \rightarrowtail B$, тогда мощность A равна мощности B . ($|A| = |B|$).

Лемма

$R = \{x_i \mid i \in N\}$ — разбиение X . $\forall i \in N \ |x_i| < \infty$. Тогда $|X| = |N|$.

Доказательство

Занумеруем X_i по очереди, тогда, поскольку $\left| \bigcup_{k=1}^{i-1} X_k \right| < \infty$, процесс дойдет

до X_i на конечном шаге для любого i .

Пример (Диагональ Кантора)

$$|N| = |R|: a_i \in Z, a_{i,j} \in \{0, 1, 2, \dots, 9\}.$$

Доказательство:

$$\text{о/п: } |N| \neq |R| \Rightarrow \exists \varphi: R \rightarrowtail R.$$

$$1) \xrightarrow{\varphi} a_1, a_{11}, a_{12}, a_{13} \dots$$

$$2) \xrightarrow{\varphi} a_2, a_{21}, a_{22} \dots$$

$$3) \xrightarrow{\varphi} a_3, a_{31}, a_{32} \dots$$

$$n) \xrightarrow{\varphi} a_n, a_{n1}, a_{n2}, a_{n3} \dots$$

$$Z = 0, b_1, b_2, b_3.$$

$$b_i \in \{0, 1, \dots, 9\} \setminus \{a_{ii}\}.$$

φ — сюръективно:

$\exists n \ Z = \varphi(n)$, но $a_{nn} \neq b_n$ — противоречие.

$$|A| \leq |B| \Leftrightarrow \exists \varphi: A \rightarrowtail B \text{ (или } \exists B' \subseteq B \ \varphi: A \rightarrowtail B').$$

Теорема

$|A| \leq |B|$ — порядок на множестве мощностей.

Доказательство:

\leq — рефлексивно $|A| \leq |A| \quad \exists A' = A \quad \varepsilon : A \succ \rightarrow \succ A' \quad \forall a \in A \quad \varepsilon(a) = a$.

\leq — транзитивно $|A| \leq |B|, |B| \leq |C|$.

$\begin{cases} \varphi : A \succ \rightarrow B \\ \exists \psi : B \succ \rightarrow C \end{cases} \Rightarrow \varphi_0 \psi : A \succ \rightarrow C \Rightarrow |A| \leq |C|$.

\leq — антисимметрично.

Предложение (Теорема Кантора-Бернштейна)

$\varphi : A \succ \rightarrow B, \psi : B \succ \rightarrow A \Rightarrow \exists \beta : A \succ \rightarrow \succ B$.

Доказательство:

$\alpha = \varphi_0 \psi : A \succ \rightarrow A \quad E_\alpha = \alpha(A)$

Строим цепочку множеств A_0, A_1, A_2, \dots

$A_0 = A_1 \quad A_1 = \psi(B), \quad A_2 = \alpha(A_0), \quad A_3 = \alpha(A_1)$.

$A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq A_4 \supseteq \dots \supseteq D \dots A_k = \alpha(A_{k-2})$.

$A_1 = \psi(B) \supseteq A_2 = \psi(\varphi(A)) \quad B \supseteq \varphi(A)$.

$A_3 = \alpha(\psi(B)) = \psi(\varphi(\psi(B))) \quad A \supseteq \psi(B)$.

$D = \bigcap_{i=0}^{\infty} A_i \alpha(A_{2i} \setminus A_{2i+1}) \subseteq A_{2i+2} \setminus A_{2i+3}$.

Допустим: $x \leftarrow A_{2i} \setminus A_{2i+1} \quad \alpha(x) \in A_{2i+3} = \alpha(A_{2i+1}) \Rightarrow \exists y \in A_{2i+1} \quad \alpha(y) = \alpha(x)$

$x \neq y$, это противоречит инъективности α .

$y \in A_{2i+2} \setminus A_{2i+3} \Rightarrow \exists x \in A_{2i} \quad \alpha(x) = y$.

Если $x \in A_{2i+1}$, то $y = \alpha(x) \in A_{2i+3}$.

Значит $x \notin A_{2i+1}$, то есть $x \in A_{2i} \setminus A_{2i+1}$.

Следовательно, $\alpha(A_{2i} \setminus A_{2i+1}) = A_{2i+2} \setminus A_{2i+3} \quad \alpha : A_{2i} \setminus A_{2i+1} \succ \rightarrow \succ A_{2i+2} \setminus A_{2i+3}$ что

$\forall i \in N_0$.

$\beta(a) = \begin{cases} \alpha(a), & \text{если } \exists i \in N_0 \quad a \in A_{2i} \setminus A_{2i+1}, \\ a, & \text{иначе } a \in A_{2i+1} \setminus A_{2i+2} \text{ или } a \in D. \end{cases}$

Убедимся, что $\beta : A \succ \rightarrow \succ A_1$.

Сюръективность: $\forall y \in A$ либо $y \in D \rightarrow y = \beta(y)$.

$y = \beta(y) \leftarrow$ либо $y \in A_{2i+1} \setminus A_{2i} \setminus A_{2i} \in N_0$.

$\exists x \in A_{2i-2} \setminus A_{2i-1} \leftarrow$ либо $y \in A_{2i} \setminus A_{2i+1} \in N$.

$\alpha(x) = y$.

Инъективность: $x, y \in A$ $\beta(x) = \beta(y)$.

Либо $\beta(x) \in D \rightarrow \beta(y) \in D \Rightarrow x = \beta(x) = \beta(y) = y$,

либо $\exists i \in N_0 \rightarrow \beta(x) \in A_{2i+1} \setminus A_{2i} \Rightarrow x = \beta(x) = \beta(y) = y$,

либо $\exists i \in N \rightarrow \beta(x) \in A_{2i} \setminus A_{2i+1} \Rightarrow \beta(x) = \alpha(x) = \alpha(y) =$
 $= \beta(y) \xrightarrow{\alpha - \text{инъективно}} x = y$.

Итак, $\beta: A \rightarrow A_1$, но $\psi: B \rightarrow A_1 \Rightarrow \psi^{-1}: A_1 \rightarrow B$ $\beta \cdot \psi^{-1}: A \rightarrow \beta$,
 что и требовалось доказать.

2. Предикаты

Операции над предикатами

Предикат — функция P типа: $M^n \rightarrow B$, где $B = \{0, 1\}$, M — произвольное множество, то есть функция P , сопоставляющая вектору (m_1, m_2, \dots, m_n) значение 0 или 1.

При этом множество M называется предметной областью предиката P (m_1, m_2, \dots, m_n) ; m_1, m_2, \dots, m_n — предметными переменными, P — предикатным символом.

Используется выражение: n -местный предикат на множестве M ; число n называется местностью предиката.

В общем смысле предикатом называется отображение

$$P: M_1 \times M_2 \times \dots \times M_n \rightarrow B,$$

где M_i есть некоторые множества. Прямое произведение $M_1 \times M_2 \times \dots \times M_n$ будем называть областью определения предиката P .

Область истинности предиката P — подмножество $I_P \subseteq M^n$ предметной области предиката P , на элементах которого значения предиката равны 1.

Пример

Одноместный предикат $P(X)$ на множестве натуральных чисел: «при делении на 3 число X даёт остаток 2». Область истинности — множество чисел вида $3n + 2$ ($n = 0, 1, 2, \dots$).

Пример

Двуместный предикат $Q(X, Y)$: «при делении на 3 число X даёт остаток Y ». Предметная область для $Q(X, Y)$ — множество пар (a, b) , где a и b — натуральные числа, причём $b \in \{0, 1, 2\}$.

Пример

Трёхместный предикат $R(X, Y, Z)$: «при делении на Z число X даёт остаток Y ». Предметная область — множество троек (X, Y, Z) , где $X, Y, Z \in \mathbb{N}$, $Z \neq 0$, $0 \leq Y < Z$.

Пример

Четырехместный предикат $P(\lambda, L, M, N)$: «плоскость λ содержит точки L, M, N ». Для плоскости $\lambda: 3X - 2Y + 4Z + 7 = 0$ и точек $L(-3, -5, -2)$, $M(5, 13, 1)$, $N(7, -4, -9)$ предикат P равен 1. Если же вместо точки M взять точку $M(2, 6, 0)$, $P = 0$.

Любому n -арному отношению $R(m_1, m_2, \dots, m_n)$ можно взаимно однозначно сопоставить n -местный предикат, который 1 для тех и только тех наборов (m_1, m_2, \dots, m_n) , для которых выполнено $R(m_1, m_2, \dots, m_n)$.

Кванторы

Над предикатами на M можно производить логические операции и получать новые предикаты. Операции над предикатами есть операции над соответствующими отношениями: конъюнкция, дизъюнкция, отрицание, импликация и другие. Состав переменных и предметная область предиката, полученного в результате операции, определяются при этом естественным образом.

Например, $P(X_1, X_2, \dots, X_n) \& Q(Y_1, Y_2, \dots, Y_n) = R(X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_n)$, где $X_1 \in M_1, X_2 \in M_2, \dots, X_n \in M_n$, $Y_1 \in N_1, Y_2 \in N_2, \dots, Y_n \in N_n$; среди переменных X_i, Y_j могут быть совпадающие переменные так же, как и среди множеств M_i и N_j .

Примеры

1. $R(X, Y) = P(X) \& Q(Y)$, $X \in M, Y \in M$, X и Y — разные предметные переменные. Область определения двухместного предиката $R(X, Y)$ — множество $S = M^2$.

2. $R(X) = P(X) \& Q(X)$: у предикатов $P(X) \& Q(X)$ — общая предметная область и одинаковая переменная; $R(X)$ — одноместный предикат на M .

3. $P(X) \rightarrow Q(X)$. Это означает: «если выполнено $P(X)$, то выполнено $Q(X)$ », т.е. «если $(X > 2)$, то $(X < 5)$ » или, выражая импликацию через дизъюнкцию « $(X > 2) \vee X < 5$ ». Можно устранить отрицание « $(X \leq 2) \vee (X < 5)$ ». Отсюда получаем окончательно: « $(X < 5)$ ».

Если $P(X, Y)$ — двухместный предикат, то фиксирование или конкретизация одной переменной превращает его в одноместный. Пусть, например, $P(X, Y)$ — «число X делится на число Y », определённый на множестве пар

натуральных чисел N , кроме пар $(X, 0)$. Тогда $P(X, 5)$ — одноместный предикат на N , истинный для всех чисел, кратных 5.

Для предикатов определяются две специфические операции, называемые навешиванием кванторов, которые превращают одноместный предикат $P(X)$ в 0-местный:

Квантор всеобщности — высказывание: «для всех X выполнено $P(X)$ », обозначение $\forall X : P(X)$.

Квантор существования — высказывание: «существует X , для которого выполнено $P(X)$ », обозначение $\exists X : P(X)$.

Процедура навешивания кванторов на предикат применима к любым предикатам.

Рассмотрим трёхместный предикат $P(X, Y, Z)$, который является истинным для некоторых троек (X, Y, Z) . Предикату P можно сопоставить выражения с кванторами $\exists X : P(X, Y, Z)$ и $\exists X : P(X, Y, Z)$; первое означает: «для всякого X выполнено $P(X, Y, Z)$ », второе — «существует X такой, что выполнено $P(X, Y, Z)$ ».

Пусть, например, $P(X, Y, Z) = 3X - 2Y > Z$ с предметной областью — множеством действительных чисел R , область истинности предиката P — полупространство по одну сторону от плоскости $3X - 2Y = Z$. Ему можно сопоставить выражения

$$Q_1(X, Y) = \forall X : 3X - 2Y > Z \text{ и } Q_2(X, Y) = \exists X : 3X - 2Y > Z.$$

Полученные двуместные предикаты зависят от Y и Z , но не зависят от X . Этот факт выражается так: переменная X в указанных предикатах связана квантором, а переменные Y, Z — свободные.

Связанные (свободные) переменные — это переменные, на которые навешены (соответственно — не навешены) кванторы $\forall X$ или $\exists X$.

Смысл связанных и свободных переменных в предикатных выражениях различен. Свободные переменные — это обычные переменные; они могут принимать значения из предметной области; выражение $P(X)$ — переменное высказывание, зависящее от значения X . В то же время выражение $\forall X : P(X)$ не зависит от X и при фиксированном предикате P и предметной области имеет вполне определённое значение: 0 или 1. Это, в частности, означает, что переименование связанной переменной не меняет истинности выражения.

Переменные, являющиеся по существу связанными, встречаются не только в логике. Например, в выражениях $\sum_{X=1}^{10} f(X)$ или $\int_a^b f(X) dX$ переменная X

связана, то есть при фиксированной f первое выражение равно определённому числу $f(1)+f(2)+\dots+f(10)$, а второе является функцией от a и b .

На предикат с навешенным квантором можно снова навешивать квантор, если у него есть свободные переменные. Если кванторы навешены на все переменные, предикат становится 0-местным, то есть высказыванием.

Пример

Для рассмотренного выше предиката $P(\lambda, L, M, N)$ предикат $\exists \lambda: P(\lambda, L, M, N)$ означает, что существует плоскость, содержащая 3 данные точки: L, M, N . Двуместный предикат $\forall L: (\exists \lambda: P(\lambda, L, M, N))$ можно записать короче: $\forall L \exists \lambda: P(\lambda, L, M, N)$, что означает: для любой точки L существует плоскость λ , содержащая эту точку и 2 данные точки: M, N . Наконец, предикат $\forall L: (\forall M: (\forall N: (\exists \lambda: P(\lambda, L, M, N))))$, или $\forall L: \forall M: \forall N: \exists \lambda: P(\lambda, L, M, N)$, выражает истинное высказывание о том, что для любых трёх точек существует содержащая их плоскость.

Область действия квантора — выражение, на которое навешивается квантор. Для устранения разночтений оно может быть заключено в скобки.

Примеры

1. $(\forall X: P(X, Y)) \vee Q(X)$.
2. $(\forall X: ((P(X, Y)) \vee Q(X)))$.

Предикатные формулы. Тавтологии

Предикатная формула (формула логики предикатов) — формула, содержащая знаки булевых операций и кванторов.

Более точно, в формулах участвуют: символы предметных переменных X, Y, Z, \dots ; символы предикатов; логические символы $\neg, \&, \vee, \rightarrow, \sim$; символы кванторов.

Предикатной формулой (одновременно определяются понятия свободных и связанных переменных) называется выражение, построенное по следующим правилам.

1. Если P — символ предиката, X_1, X_2, \dots, X_i — символы переменных (необязательно различных), то $P(X_1, X_2, \dots, X_i)$ — предикатная формула; все её переменные свободные.

2. Если A — формула, то A — тоже формула с теми же свободными и связанными переменными.

3. Если A, B — формулы и нет переменных, свободных в одной из них и связанных в другой, то $A \& B, A \vee B, A \rightarrow B, A \sim B$ тоже формулы с теми же свободными и связанными переменными.

4. Если A — формула, содержащая свободную переменную X (и, быть может, другие переменные — свободные и связанные), то выражения $\forall X : A(X)$ и $\exists X : A(X)$ — предикатные формулы; в каждой из них переменная X переходит из множества свободных в множество связанных, т. е. число свободных переменных уменьшается, а число связанных увеличивается на 1. При этом формула A называется областью действия квантора.

В формуле должны быть правильным образом расставлены скобки, определяющие области действия кванторов и порядок выполнения логических и кванторных операций. Однако для сокращения записи могут быть удалены излишние скобки (считается, что знак квантора связывает сильнее, чем знак логической операции), также можно записывать кванторные формулы без знака «:».

Пример

Пусть $P(X, Y) = X \leq Y$ для действительных чисел $X, Y \in R$. Это 2-местный предикат с предметной областью на числовой плоскости. Область истинности — полуплоскость, ограниченная биссектрисой I и III координатных углов, включающая точки границы. Формулы $\forall X : P(X, Y)$ и $\forall Y : P(X, Y)$ — одноместные предикаты со свободными переменными Y и, соответственно, X . Область истинности — пустое множество, так как не существует ни наибольшего, ни наименьшего среди действительных чисел. Предикат $\exists X : P(X, Y)$ — одноместный со свободной переменной Y . Его область истинности — вся числовая ось, так как какое бы ни было Y , существует меньшее число X .

Рассмотрим тот же предикат $P(X, Y) = X \leq Y$ на предметной области натуральных чисел: $X, Y \in N = \{0, 1, 2, \dots\}$. Область истинности предиката — целочисленные точки I-го координатного угла, включая точки оси абсцисс, расположенные над биссектрисой и на ней. Область истинности для предиката $\forall X : P(X, Y)$ — пустое множество, для $\forall Y : P(X, Y)$ область истинности состоит из одного числа 0. Отсюда можно заключить, что предикат $\exists X : (\forall Y : P(X, Y))$ есть истинное высказывание (обе переменные — связанные), поскольку существует наименьшее натуральное число — 0.

Пример

1. Для предиката $P(X, Y) = X \leq Y$ формула $P(X, Y) \& P(Y, X)$ выражает предикат $X = Y$. Тот же предикат $P(X, Y)$ может быть выражен через

3-местный предикат на множестве натуральных чисел $Q(S, T, U) = S + T = U$ следующим образом: $P(X, Y) = \exists S : Q(S, X, Y)$, т.е. существует такое S , что $X + S = Y$, или $Y - X = S \geq 0$. Формула $\exists S : Q(S, X, Y)$ означает, что X — чётное число ($X = S + S$). Наконец, формула $P(X, Y) \& P(Y, X)$ выражает условие $X < Y$.

2. Предикат $R(X, Y, Z)$: «при делении на Z число X даёт остаток Y » может быть выражен предикатной формулой $\exists k (X = kZ + Y), k \in N$.

Область истинности предиката, выраженного предикатной формулой, определяется областями истинности составляющих и применяемыми в формуле операциями:

$$I_{P \vee Q} = I_P \cup I_Q; I_{P \& Q} = I_P \cap I_Q; I_{\neg P} = \bar{I}_P; I_{P \rightarrow Q} = \bar{I}_P \cup I_Q.$$

Интерпретация — это сопоставление каждому предикатному символу в формуле определённого предиката.

Пусть две формулы F и G содержат одно и то же множество свободных переменных (может быть пустое).

Формулы F и G равносильны в данной интерпретации, если они выражают один и тот же предикат (то есть при одинаковых значениях предметных переменных они принимают одинаковые значения).

Пример

Если $P(X, Y) = X > Y$, $Q(X, Y) = X > Y$, то $\bar{P}(X, Y)$ и $Q(X, Y)$ — равносильные формулы; при других интерпретациях P и Q эти формулы могут не быть равносильными.

Формулы F и G равносильны на множестве M , если они равносильны во всех интерпретациях на этом множестве.

Пример

$\exists X : P(X)$ и $\forall X : P(X)$ будут равносильны на одноэлементном множестве M : если существует подходящий X , то поскольку других значений нет, истинно и второе суждение. На множестве, содержащем более одного элемента, это уже не так.

Формулы F и G равносильны в логике предикатов, если они равносильны на всех множествах.

В этом случае можно назвать эту равносильность тождеством в логике предикатов, или законом логики предикатов и обозначать $F \equiv G$.

Для предикатных формул сохраняются все равносильности логики высказываний. Кроме того, справедливы такие эквивалентности для кванторных формул.

1. Перенос квантора через отрицание (законы де Моргана для предикатов): $\neg \forall X : A(X) \equiv \exists X : \neg A(X)$; $\neg \exists X : A(X) \equiv \forall X : \neg A(X)$.

2. Вынесение квантора за скобки.

Если формула $A(X)$ содержит свободную переменную X , а формула B не содержит X и в них нет переменных, свободных в одной из формул и связанных в другой, то:

$$\exists X : (A(X) \& B) \equiv (\exists X : A(X)) \& B;$$

$$\forall X : (A(X) \& B) \equiv (\forall X : A(X)) \& B;$$

$$\exists X : (A(X) \vee B) \equiv (\exists X : A(X)) \vee B;$$

$$\forall X : (A(X) \vee B) \equiv (\forall X : A(X)) \vee B.$$

3. Законы коммутативности для одноимённых кванторов.

$$\forall X : (\forall Y : A(X, Y)) \equiv \forall Y : (\forall X : A(X, Y));$$

$$\exists X : (\exists Y : A(X, Y)) \equiv \exists Y : (\exists X : A(X, Y)).$$

Коммутативность даёт использовать более короткую запись: $\forall X, Y, Z : P(X, Y, Z)$ или $\exists X, Y : Q(X, Y, Z)$ и т. п.

Отметим различие между логическими интерпретациями формул в логике высказываний и логике предикатов. Простое высказывание допускает два возможных значения, а сложное, составленное из n простых — 2^n . В отличие от высказываний предикат имеет, вообще говоря, бесконечное множество интерпретаций. Во-первых, может быть бесконечной область определения предиката, и предикатному символу можно сопоставить бесконечное множество различных функций. Во-вторых, предикат $P(m_1, m_2, \dots, m_n)$ можно рассматривать на различных множествах M .

Многие предикаты, например, выражающие часто встречающиеся отношения, такие как "=", ">", "<" и другие, имеют стандартные обозначения и вполне определенный (или оговорённый в пределах контекста) смысл. С точки зрения истинности для предикатных формул вводятся следующие понятия.

Формула F называется *выполнимой* (*непротиворечивой*), если существует интерпретация, в которой F имеет истинное значение, т. е. область истинности не пуста.

Тождественно истинная (*общезначимая*) *формула*, или *тавтология*, — формула, для которой при любой её интерпретации область истинности совпадает с областью определения.

Тождественно ложная (*противоречивая*) *формула* — это формула, для которой область истинности пуста.

Обозначение тавтологии: $\vdash F$, тождественно ложной — $\vdash \neg F$.

Формула F общезначима тогда и только тогда, когда формула $\neg F$ не является выполнимой; формула F выполнима тогда и только тогда, когда $\neg F$ не является общезначимой.

Некоторые общезначимые формулы:

1. Если F и G — равносильные в логике предикатов формулы, то $F \sim G$ — общезначимая формула. При этом $I_F = I_G$.

Если $F \rightarrow G$ — общезначимая формула, то $I_F \subseteq I_G$.

2. Если Y не входит в формулу $P(X)$, то $\forall X : P(X) \rightarrow P(Y)$ и $P(Y) \rightarrow \exists X : P(X)$ — общезначимые формулы.

3. Приведённые выше тождества для кванторных формул.

Квантор всеобщности есть обобщение операции конъюнкции, а квантор существования — обобщение дизъюнкции, и тем самым законы де Моргана для предикатов характеризуют взаимную двойственность кванторов $\forall X$ и $\exists X$.

4. $\forall X : (P(X) \& Q(X)) \equiv \forall X : P(X) \& \forall X : Q(X)$.

5. $\exists X : (P(X) \vee Q(X)) \equiv \exists X : P(X) \vee \exists X : Q(X)$.

6. Выше отмечена возможность перестановки одноимённых кванторов т.е. эти эквивалентности — общезначимые формулы.

7. Импликация $\exists X : (\forall Y : P(X, Y)) \rightarrow \forall Y : (\exists X : P(X, Y))$ является тавтологией. Однако сложная формула $\forall X : (\exists Y : P(X, Y)) \rightarrow \exists Y : (\forall X : P(X, Y))$ уже не является тавтологией.

Теорема о подстановке

Пусть F — тождественно истинная формула логики высказываний. Тогда подстановка вместо её переменных X_1, X_2, \dots, X_n предикатных формул B_1, B_2, \dots, B_n такая, что получается правильная предикатная формула, которая даёт общезначимую формулу логики предикатов.

Вопрос о распознавании общезначимости формул логики предикатов относится к предмету теории алгоритмов. Не уточняя пока соответствующих понятий, сформулируем важный результат.

Теорема Черча

Не существует алгоритма, который для любой формулы логики предикатов установил бы, общезначима она или нет.

Однако в некоторых частных случаях такой алгоритм существует, например, для формул, содержащих только одноместные предикатные символы.

Исчисление предикатов

Метод доказательства формул, содержащих переменные, путём непосредственной подстановки в них предметных констант называется методом интерпретаций, или методом моделей. Подстановка констант позволяет интерпретировать формулу как содержательное утверждение об элементах конкретного множества. Поэтому такой метод, апеллирующий к содержательному смыслу интерпретированной формулы называют семантическим, то есть смысловым. Это удобно при доказательстве выполнимости формул или их неэквивалентности, поскольку и в том, и в другом случае достаточно найти одну подходящую подстановку (интерпретацию).

Метод интерпретации можно применять и для исследования истинности формул на конечных предметных областях, так как если область M конечна, $M = \{m_1, m_2, \dots, m_n\}$, то кванторы выражают конечные формулы логики высказываний:

$$X : P(X, Y) \equiv P(m_1) \& P(m_2) \& \dots \& P(m_n),$$

$$X : P(X, Y) \equiv P(m_1) \vee P(m_2) \vee \dots \vee P(m_n).$$

В этом случае все кванторные формулы можно заменить указанным способом и получить, содержащие только символы предикатов и логических операций, после чего проверить истинность можно конечным числом подстановок констант.

Для большинства же предметных областей доказательство тождественной истинности формул методом интерпретаций связано с большими трудностями. Поэтому применяется другой приём — аксиоматизация, т. е. построение формальной системы и порождение исследуемых формул из аксиом с помощью процедур вывода.

Как и для исчисления высказываний, для предикатных формул построение исчисления проводится путём указания некоторой совокупности формул, которые называются аксиомами, и заданием правил вывода, позволяющих из общезначимых формул получать общезначимые. Часть аксиом исчисления предикатов совпадает с аксиомами исчисления высказываний.

Приведем две аксиомы исчисления предикатов:

1. $\forall X_i (P(X_i) \rightarrow P(X_j))$, где формула $P(X_i)$ не содержит переменной X_j .
2. $P(X_i) \rightarrow \exists X_j (P(X_j))$ с тем же условием, что и в 1.

Правила вывода (при этом не должны нарушаться требования к правильности формул):

1. Правило *modus ponens*:

$$\frac{A, (A \rightarrow B)}{B}.$$

2а. Правило связывания квантором \forall :

$$\frac{B \rightarrow A(X_i)}{B \rightarrow \forall X_i A(X_i)},$$

где формула B не содержит переменной X_i .

2б. Правило связывания квантором \exists :

$$\frac{A(X_i) \rightarrow B}{\exists X_i A(X_i) \rightarrow B},$$

где формула B не содержит переменной X_i .

3. Переименование связанной переменной: связанную переменную формулы A можно заменить в кванторе и во всех вхождениях в области действия квантора.

Понятия вывода, теоремы, вывода из системы гипотез определяются в исчислении предикатов так же, как в любой аксиоматической теории.

Приведём без доказательства несколько утверждений об исчислениях предикатов (A, B, \dots — формулы в исчислении).

Теорема 1

Если $A \vdash B$ и существует вывод формулы B из формулы A , использующий только правило *modus ponens*, то $\Gamma \vdash (A \rightarrow B)$.

Теорема 2

Аксиомы исчисления предикатов — общезначимые формулы.

Теорема 3

Формула, получаемая из общезначимой по любому правилу выхода 1–3, является общезначимой.

Теорема 4

Любая выводимая в исчислении предикатов формула — общезначима.

Теорема 5

Исчисление предикатов непротиворечиво, так как в силу теоремы 4 невозможно вывести одновременно A и $\neg A$.

Определённое выше исчисление предикатов называют узким исчислением предикатов, в отличие от нерассматриваемого расширенного исчисления, в котором допускаются кванторы не только по предметным переменным, но и по предикатным переменным.

Теорема (Гёделя)

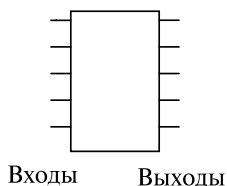
В узком исчислении предикатов всякая общезначимая формула выводима.

3. Булевы функции

Определение и примеры

n -местная булева функция (БФ) $f: \{0,1\}^n \rightarrow \{0,1\}$.

Пример



0 — тока нет, 1 — тока нет.
На каждом выходе БФ от входов.

Пример

Сложное предложение. Сегодня вторник, и идет дождь. О каждом предложении можно сказать истинно или ложно. Сопоставим истине — 1, лжи — 0. Сложное предложение — БФ от простых предложений. Y = если $П1$, то $П2$

П1	0	0	1	1
П2	0	1	0	1
Y	1	1	0	1

Если $x = y$, то $0 = 0$.

Для любой БФ $f(x_1, x_2, x_3, \dots, x_n)$ можно построить таблицу:

x_1	x_2	x_3	...	x_{n-1}	x_n	$f(x_1, x_2, x_3, \dots, x_n)$
0	0	0	...	0	0	α_1
0	0	0	...	0	1	α_2
		
1	1	1	...	1	0	.
1	1	1	...	1	1	.

Лемма о количестве

Количество n -местных БФ равно 2^{2^n} .

Доказательство

Всего $|B|^{|A|}$ функций из A в B . У нас $A = \{0,1\}^n$, $B = \{0,1\}$, $|A| = 2^n$.

Пример 1

$n=1$

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	1	0	1	0

$f_0(x) = 0$, $f_3(x) = 1$ — константы, $f_1(x) = x$;

$f_2(x) = \bar{x}$ (отрицание x).

Пример 2

$n=2$, $2^{2^2} = 16$

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$f_0(x, y) = 0$, $f_{15}(x, y) = 1$ — константы;

$f_3(x, y) = x$;

$f_5(x, y) = y$;

$f_{10}(x, y) = \bar{y}$;

$f_{12}(x, y) = \bar{x}$;

$f_1(x, y) = x \wedge y = xy$ (конъюнкция, умножение, «и»);

$f_7(x, y) = x \vee y$ (дизъюнкция, «или»);

$f_{13}(x, y) = x \rightarrow y$ (импликация, «если..., то»);

$f_{11}(x, y) = y \rightarrow x$;

$f_9(x, y) = x \leftrightarrow y$ («эквивалентность, «тогда и только тогда»);

$x \leftrightarrow y = (x \rightarrow y) \wedge (y \rightarrow x)$;

$f_6(x, y) = x \oplus y$ (сложение по модулю 2);

$x \oplus y = \overline{x \leftrightarrow y}$;

$f_{14}(x, y) = x | y$ (штрих Шеффера);

$f_8(x, y) = x \uparrow y$ (стрелка Пирса);

$f_2(x, y) = \overline{f_{13}(x, y)} = \overline{x \rightarrow y}$;

$f_4(x, y) = \overline{y \rightarrow x}$.

Суперпозиция функций

Если $f(x_1, x_2, x_3 \dots x_n)$, $f_1(y_{11}, y_{12}, y_{13} \dots y_{1k_1})$... $f_2(y_{21}, y_{22}, y_{23} \dots y_{2k_2})$... $f_n(y_{n1}, y_{n2}, y_{n3} \dots y_{nk_n})$, то функция $h(y_{11}, y_{12} \dots y_{nk_n}) = f(f_1(y_{11}, y_{12}, y_{13} \dots y_{1k_1}) \dots f_2(y_{21}, y_{22}, y_{23} \dots y_{2k_2}) \dots f_n(y_{n1}, y_{n2}, y_{n3} \dots y_{nk_n}))$ называется *суперпозицией* этих функций.

Тождества

1. $x \vee y = y \vee x$. 1'. $x \wedge y = y \wedge x$.
2. $(x \vee y) \vee z = x \vee (y \vee z)$. 2'. $(x \wedge y) \wedge z = x \wedge (y \wedge z)$.

Проверить можно с помощью таблицы:

x	y	z	$x \vee y$	$y \vee z$	$(x \vee y) \vee z$	$x \vee (y \vee z)$
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	0	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

3. $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ 3'. $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$

- | | |
|--|---|
| 4. $x \vee x = x$. | 4'. $x \wedge x = x$. |
| 5. $x \vee 1 = 1$. | 5'. $x \wedge 0 = 0$. |
| 6. $x \wedge 1 = x$. | 6'. $x \vee 0 = x$. |
| 7. $x \vee \bar{x} = 1$. | 7'. $x \wedge \bar{x} = 0$. |
| 8. $\overline{\overline{x}} = x$. | |
| 9. $(x \wedge y) \vee y = y$. | 9'. $(x \vee y) \wedge y = y$. |
| 10. $\overline{x \vee y} = \bar{x} \wedge \bar{y}$. | 10'. $\overline{x \wedge y} = \bar{x} \vee \bar{y}$. |

Замечание

Если в тождествах для операций с множествами заменить \cap на \wedge , \cup на \vee , U на 1, \emptyset на 0 и отрицание на дополнение, то получим 19 тождеств для БФ.

Проверим Закон де Моргана:

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

Дизъюнктивная нормальная форма БФ

Обозначение $a^b = \begin{cases} a, & b = 1; \\ \bar{a}, & b = 0. \end{cases}$

Замечание: $a^b = a \leftrightarrow b$.

Лемма 1

Для любой булевой функции $f: \{0,1\}^n \rightarrow \{0,1\}$ верно тождество $f(x_1, x_2, \dots, x_n) = \vee x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} f(\alpha_1, \alpha_2 \dots \alpha_n)$, где дизъюнкция берется по всем наборам $(\alpha_1, \alpha_2 \dots \alpha_n) \in \{0,1\}^n$, для которых $f(\alpha_1, \alpha_2 \dots \alpha_n) = 1$.

Доказательство

Пусть при $(x_1, x_2 \dots x_n) = (b_1, b_2 \dots b_n)$ левая часть равна 1. В правой части есть дизъюнкт $x_1^{b_1}, x_2^{b_2} \dots x_n^{b_n} f(b_1, b_2 \dots b_n)$. При $(x_1, x_2 \dots x_n) = (b_1, b_2 \dots b_n)$ он равен $b_1^{b_1}, b_2^{b_2} \dots b_n^{b_n} f(b_1, b_2 \dots b_n) = 1$. Значит и вся правая часть равна 1.

Пусть при $(x_1, x_2 \dots x_n) = (b_1, b_2 \dots b_n)$ левая часть равна 0. Рассмотрим произвольный дизъюнкт из правой части $x_1^{\alpha_1}, x_2^{\alpha_2} \dots x_n^{\alpha_n} f(\alpha_1, \alpha_2 \dots \alpha_n)$. При $(x_1, x_2 \dots x_n) = (b_1, b_2 \dots b_n)$ он равен $b_1^{\alpha_1} b_2^{\alpha_2} \dots b_n^{\alpha_n} f(\alpha_1, \alpha_2 \dots \alpha_n)$.

Если $\exists i \in \{1 \dots n\}, b_i \neq \alpha_i$, то $b_i^{\alpha_i} = 0$, если $\forall i \in \{1 \dots n\}, b_i = \alpha_i$, то $f(\alpha_1, \alpha_2 \dots \alpha_n) = f(b_1, b_2 \dots b_n) = 0$. Т.е. дизъюнкт всегда равен 0. Все дизъюнкты в правой части равны 0, значит вся правая часть равна 0.

Теорема

$\forall f: \{0,1\}^n \rightarrow \{0,1\} \exists! S \subseteq \{0,1\}^n f(x_1, x_2 \dots x_n) = \bigvee_{(\alpha_1, \alpha_2 \dots \alpha_n) \in S} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} f(\alpha_1, \alpha_2 \dots \alpha_n)$, где дизъюнкция берется по всем наборам $(\alpha_1, \alpha_2 \dots \alpha_n) \in S$.

Доказательство

Для доказательства существования такого множества в силу леммы 1 достаточно положить $S = \{(\alpha_1, \alpha_2 \dots \alpha_n) \in \{0,1\}^n \mid f(\alpha_1, \alpha_2 \dots \alpha_n) = 1\}$.

При этом считаем, что пустое множество S соответствует нулевой булевой функции f .

Для доказательства единственности, заметим, что выражений для правой части столько, сколько множеств $S \subseteq \{0,1\}^n$ т.е. $|\beta(\{0,1\}^n)| = 2^{|\{0,1\}^n|} = 2^{2^n}$

и n -местных БФ тоже 2^{2^n} . Каждой правой части соответствует ровно одна БФ, и каждой БФ соответствует выражение правой части. Если какой-то БФ соответствует более одного выражения правой части, то на все функции не хватит таких выражений.

Если $f(x_1, x_2 \dots x_n) = \bigvee_{(\alpha_1, \alpha_2 \dots \alpha_n) \in S} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} f(\alpha_1, \alpha_2 \dots \alpha_n)$, где дизъюнкция берется по всем наборам $(\alpha_1, \alpha_2 \dots \alpha_n) \in S$, то правая часть равенства называется дизъюнктивной нормальной формой функции f .

Пример 1

Построим ДНФ для функции $x \rightarrow y : x \rightarrow y = x^0 y^0 \vee x^0 y^1 \vee x^1 y^1$

x	y	$x \rightarrow y$
0	0	1
0	1	1
1	0	0
1	1	1

Проверка

x	y	\bar{x}	\bar{y}	$\bar{x}\bar{y}$	$\bar{x}y$	xy	$\bar{x}\bar{y} \vee \bar{x}y \vee xy$
0	0	1	1	1	0	0	1
0	1	1	0	0	1	0	1
1	0	0	1	0	0	0	0
1	1	0	0	0	0	1	1

Пример 2

У нас есть 3 кнопки. Требуется спроектировать устройство, которое выдает сигнал, когда нажаты хотя бы 2 кнопки.

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

$f(x, y, z)$ — функция голосования трех. Теперь, если мы обладаем большим запасом деталей, позволяющих вычислять \wedge , \vee и \neg , то формула $f(x, y, z) = \bar{x}yz \vee x\bar{y}z \vee xy\bar{z} \vee xyz$ позволяет собрать требуемое устройство. При этом потребуется 8 деталей « \wedge », 3 детали « \vee » и 3 детали « \neg ».

Заметив, что $xy\bar{z} \vee xyz = xy(\bar{z} \vee z) = xy$ и $x\bar{y}z = x\bar{y}z \vee xyz \vee xyz$, можно сократить количество необходимых деталей:

$$f(x, y, z) = yz \vee xz \vee xy = (y \vee x)z \vee xy \quad (\text{теперь нужно } 2\text{«}\wedge\text{» и } 2\text{«}\vee\text{»}).$$

Полиномы Жегалкина

Теорема о ДНФ говорит о том, что любую БФ можно представить в виде суперпозиции \wedge , \vee и \neg .

Система БФ A — *полная*, если любая БФ является суперпозицией функций из A . Например,

из $x \vee y = \overline{\bar{x}} \wedge \overline{\bar{y}}$ следует, что $\{\wedge, \neg\}$ — полная система;

из $x \wedge y = \overline{\bar{x} \vee \bar{y}}$ следует, что $\{\vee, \neg\}$ — полная система.

Любая БФ может быть выражена через \wedge , \vee и \neg . Но $\bar{x} = 1 \oplus x$, а заменив, таким образом, все отрицания, получим выражение через $1, \oplus$ и \cdot .

Эти функции удовлетворяют следующим тождествам:

- | | | |
|--|---|---|
| <ol style="list-style-type: none"> 1. $x \oplus y = y \oplus x$ 2. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ 3. $x \oplus 0 = x$ 4. $x \oplus x = 0$ 5. $(x \oplus y)z = xz \oplus yz$ 6. $xy = yx$ 7. $(xy)z = x(yz)$ 8. $x \cdot 1 = x$ 9. $x \neq 0 \Rightarrow x = 1 \Rightarrow xx = 1$ | } | <p>9 аксиом двухэлементного поля
 $\Rightarrow \langle \{0, 1\}, \oplus, \cdot \rangle$ — поле</p> |
|--|---|---|

Раскроем в полученном ранее выражении скобки, получим многочлен. Заметим, что $x \cdot x = x \Rightarrow \forall k \geq 1 \ x^k = x$, т.е. в каждом одночлене каждая переменная стоит в степени 1 или отсутствует. Таким образом, получим тождество вида $f(x_1, x_2, \dots, x_n) = \sum_{S \subseteq \{1, 2, \dots, n\}} \alpha_S \prod_{i \in S} x_i$. Его правая часть называется *полином Жегалкина*.

Теорема

Каждая n -местная БФ однозначно (!) представима (\exists) в виде полинома Жегалкина.

Доказательство

Существование доказано перед формулировкой теоремы. Докажем единственность. Каждому полиному соответствует ровно одна БФ. Сколько всего полиномов для n -местных БФ? Каждый полином определяется вектором

коэффициентов $(\alpha_{\emptyset}, \alpha_{\{1\}}, \alpha_{\{2\}}, \alpha_{\{1,2\}}, \alpha_{\{3\}}, \alpha_{\{1,3\}}, \alpha_{\{2,3\}}, \alpha_{\{1,2,3\}} \dots \alpha_{\{4\}} \dots \alpha_{\{1,2,\dots,n\}})$. Таких векторов 2^{2^n} . Таким образом число полиномов от n переменных равно числу n -местных функций. Значит каждой булевой функции соответствует ровно один полином.

Замкнутые классы БФ

Класс БФ C — замкнутый, если каждая суперпозиция функций из C лежит в C .

Лемма

Пусть C — замкнутый класс, содержащий не все БФ, $A \subseteq C$. Тогда A неполная система.

Доказательство.

Предположим противное. A — полная, тогда есть суперпозиция функций из A , не лежащая в C , что противоречит определению C .

Примеры

1. Все БФ — замкнутый класс.

2. $\{x\}$

3. $\{0, 1\}$

4. $\{0, 1, x\}$

5. $\{0, 1, x, \bar{x}\}$

Замкнутые классы

Для доказательства достаточно заметить, что $f(y(x)) = h(x)$, т. е. суперпозиция функций от одной переменной является функцией от одной переменной.

6. $\{\vee, -\}$ не замкнутый класс.

7. Все 2-местные БФ — незамкнутый класс.

Важный пример 1

Говорят, что функция $f(x_1, \dots, x_n)$ сохраняет константу c , если $f(c, c, \dots, c) = c$.

Пусть $T_c = \{f \mid f(c, c, \dots, c) = c\}$.

Утверждение 1

T_0 и T_1 — замкнутые классы.

Доказательство.

Пусть $c \in \{0,1\}$. Пусть $f(x_1, \dots, x_n) \in T_c$, $f_1(y_{11}, \dots, y_{1k_1}) \in T_c, \dots$

$f(y_{n1}, \dots, y_{nk_n}) \in T_c$.

Если $h(y_{11} \dots y_{nk_n}) = f(f_1(y_{11}, \dots, y_{1k_1}) \dots f_n(y_{n1}, \dots, y_{nk_n}))$, то

$h(c, c, \dots, c) = f(f_1(c, c, \dots, c), \dots, f_n(c, c, \dots, c)) = f(c, c, \dots, c) = c$.

Как узнать по таблице $f \in T_0$ или $f \notin T_0$?

x_1	x_2	\dots	x_n	f
0	0	\vdots	0	f_1
0	0	\vdots	1	f_2
\vdots	\vdots	\vdots	\vdots	\vdots
1	1	\vdots	0	\vdots
1	1	\vdots	1	f_n

Для этого необходимо рассмотреть f_1 и f_n .

	$\in T_0$	$\notin T_0$
$\in T_1$	$x, xy, x \vee y$	$1, x \leftrightarrow y, x \rightarrow y$
$\notin T_1$	$0, x + y$	\bar{x}

Важный пример 2

Функция $g = (x_1, \dots, x_n)$ двойственная для $f(x_1, \dots, x_n)$ (обозначение $g = f^*$),

если $g(x_1, \dots, x_n) = \overline{f(\bar{x}_1, \dots, \bar{x}_n)}$.

Например, из $x \vee y = \overline{\bar{x} \wedge \bar{y}}$ следует $\vee = \wedge^*$.

Если $f(x) = 0$, то $f^*(x) = \overline{f(\bar{x})} = \bar{0} = 1$.

Если $f(x) = \bar{x}$, то $f^*(x) = \overline{f(\bar{x})} = \overline{\bar{\bar{x}}} = \bar{x}$.

f — самодвойственная, если $f^* = f$. Пусть $S = \{f \mid f^* = f\}$.

Утверждение 2

S — замкнутый класс.

Доказательство

Пусть $f, f_1 \dots f_n \in S$. $h = f(f_1(y_{11}, \dots, y_{1k_1}) \dots f_n(y_{n1}, \dots, y_{nk_n}))$.

$$\begin{aligned}
h^*(y_{11}, \dots, y_{1k_1}) &= \overline{h(\overline{y_{11}} \dots \overline{y_{nk_n}})} = \overline{f(f_1(\overline{y_{11}}, \dots, \overline{y_{1k_1}}) \dots f_n(\overline{y_{n1}}, \dots, \overline{y_{nk_n}}))}. \\
f_1(\overline{y_{11}}, \dots, \overline{y_{1k_1}}) &= \overline{f_1(y_{11}, \dots, y_{1k_1})} = [\text{т.к. } f_1 \dots f_n \in S] = \\
&= \left(\overline{f_1(\overline{y_{11}}, \dots, \overline{y_{1k_1}})} \dots \overline{f_n(\overline{y_{n1}}, \dots, \overline{y_{nk_n}})} \right) = \\
&= [\text{т.к. } f \in S] = f(f_1(y_{11}, \dots, y_{1k_1}) \dots f_n(y_{n1}, \dots, y_{nk_n})) = h(y_{11}, \dots, y_{nk_n}) \Rightarrow h \in S.
\end{aligned}$$

Как по таблице узнать $f \in S$ или $f \notin S$?

x_1	x_2	\dots	x_n	f
0	0	\vdots	0	α
0	0	\vdots	1	β
γ_1	γ_2		γ_n	γ
$\overline{\gamma_1}$	$\overline{\gamma_2}$	\vdots	$\overline{\gamma_n}$	$\overline{\gamma}$
1	1	\vdots	0	$\overline{\beta}$
1	1	\vdots	1	$\overline{\alpha}$

$$\forall x_1, x_2 \dots x_n \quad f(\overline{x_1}, \overline{x_2} \dots \overline{x_n}) = \overline{f(x_1, x_2 \dots x_n)}$$

$\in S$	$\notin S$
$\overline{x}, x, xy \vee xz \vee yz$	$0, 1, xy, x \leftrightarrow y, x \rightarrow y, x + y, x y$

$$x^* = \overline{\overline{x}}$$

$$f(x, y, z) = xy \vee xz \vee yz.$$

$$\begin{aligned}
f^*(x, y, z) &= \overline{\overline{xy} \vee \overline{xz} \vee \overline{yz}} = \overline{\overline{xy} \cdot \overline{xz} \cdot \overline{yz}} = (x \vee y)(x \vee z)(y \vee z) = \\
&= x \cdot x \cdot y \vee x \cdot x \cdot z \vee x \cdot z \cdot y \vee x \cdot z \cdot z \vee y \cdot x \cdot y \vee y \cdot x \cdot z \vee y \cdot z \cdot y \vee y \cdot z \cdot z = \\
&= xy \vee xz \vee xyz \vee xz \vee xy \vee xyz \vee yz \vee yz = xy \vee xz \vee yz \vee xyz = xy \vee xz \vee yz.
\end{aligned}$$

Самодвойственность этой функции можно увидеть и по таблице:

x	y	z	$xy \vee xz \vee yz$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1

x	y	z	$xy \vee xz \vee yz$
1	1	0	1
1	1	1	1

Важный пример 3

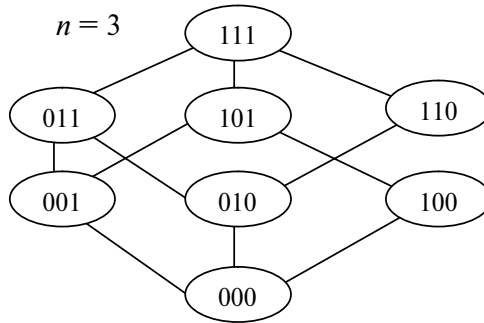
Пусть

$$\vec{\alpha} = (\alpha_1, \alpha_2 \dots \alpha_n) \in \{0, 1\}^n, \quad \vec{\beta} = (\beta_1, \beta_2 \dots \beta_n) \in \{0, 1\}^n.$$

Положим по определению $\vec{\alpha} \leq \vec{\beta} \Leftrightarrow \forall i \in \{1 \dots n\} \alpha_i \leq \beta_i$.

Тогда \leq — бинарное отношение на $\{0, 1\}^n$

\leq рефлексивно,
 \leq антисимметрично,
 \leq транзитивно,
 }
 $\Rightarrow \leq$ — порядок на $\{0, 1\}^n$.



Отметим, что $001 \not\leq 110$, $110 \not\leq 001$, т.е. эти векторы несравнимы относительно введенного порядка.

Функция $f(x_1, \dots, x_n)$ *монотонная*, если она сохраняет порядок \leq , т.е.

$$\forall \vec{\alpha}, \vec{\beta} \in \{0, 1\}^n \quad \vec{\alpha} \leq \vec{\beta} \Rightarrow f(\vec{\alpha}) \leq f(\vec{\beta}).$$

Пусть $M = \{f \mid f \text{ — монотонная}\}$.

Утверждение 3

M — замкнутый класс.

Доказательство

Пусть $f, f_1 \dots f_n \in \mathcal{S}$. $h = f(f_1(y_{11}, \dots, y_{1k_1}) \dots f_n(y_{n1}, \dots, y_{nk_n}))$.

Рассмотрим два произвольных вектора

$$\vec{\alpha} = (\alpha_{11}, \alpha_{12} \dots \alpha_{1k} \alpha_{21}, \alpha_{22} \dots \alpha_{2k_2} \dots \alpha_{n1} \alpha_{n2} \dots \alpha_{nk_n})$$

$$\vec{\beta} = (\beta_{11}, \beta_{12} \dots \beta_{1k}, \beta_{21}, \beta_{22} \dots \beta_{2k_2} \dots \beta_{n1} \beta_{n2} \dots \beta_{nk_n}).$$

Обозначим «части» векторов $\vec{\alpha}$ и $\vec{\beta}$ так:

$$\vec{\alpha}_i = (\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{ik_i}), \quad \vec{\beta}_i = (\beta_{i1}, \beta_{i2}, \dots, \beta_{ik_i}). \text{ Тогда}$$

$$h(\vec{\alpha}) = f(f_1(\vec{\alpha}_1) \dots f_n(\vec{\alpha}_n)), \text{ и } h(\vec{\beta}) = f(f_1(\vec{\beta}_1) \dots f_n(\vec{\beta}_n)).$$

Пусть $\vec{\alpha} \leq \vec{\beta}$, тогда $\vec{\alpha}_1 \leq \vec{\beta}_1, \vec{\alpha}_2 \leq \vec{\beta}_2 \dots \vec{\alpha}_n \leq \vec{\beta}_n$. Теперь, в силу произвольности выбранных векторов $\vec{\alpha}$ и $\vec{\beta}$, и следующих очевидных импликаций

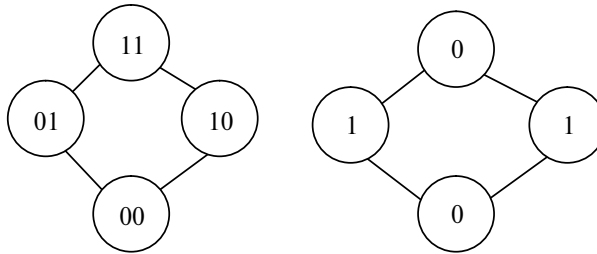
$$f_1 \in M, \dots, f_n \in M \Rightarrow f_1(\vec{\alpha}_1) \leq f_1(\vec{\beta}_1) \dots f_n(\vec{\alpha}_n) \leq f_n(\vec{\beta}_n)$$

$$\text{и } f \in M \Rightarrow h(\vec{\alpha}) = f(f_1(\vec{\alpha}_1) \dots f_n(\vec{\alpha}_n)) \leq f(f_1(\vec{\beta}_1) \dots f_n(\vec{\beta}_n)) = h(\vec{\beta}),$$

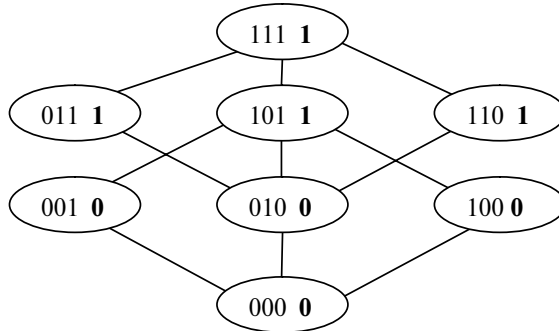
получаем $h \in M$.

$\in M$	$\notin M$
$0, 1, xy, x, x \vee y, xy \vee xz \vee yz$	$\bar{x}, x \leftrightarrow y, x \rightarrow y, x + y,$

По определению монотонности $f \in M \Leftrightarrow \forall \vec{\alpha}, \vec{\beta} \vec{\alpha} \leq \vec{\beta} \Rightarrow f(\vec{\alpha}) \leq f(\vec{\beta})$, значит $f \notin M \Leftrightarrow \exists \vec{\alpha}, \vec{\beta} \vec{\alpha} \leq \vec{\beta}$ и $f(\vec{\alpha}) > f(\vec{\beta})$. Например, функция $x + y$ не монотонна, поскольку $\vec{\alpha} = (0, 1), \vec{\beta} = (1, 1), \vec{\alpha} \leq \vec{\beta}$, но $0 + 1 > 1 + 1$. На диаграмме отношения порядка это выглядит так, что под некоторым нулем располагается единица:



Проверим функцию голосования трех:



Она — монотонная.

Важный пример 4

$f(x_1, \dots, x_n)$ линейная, если $\exists a_0, a_1 \dots a_n \in \{0, 1\} \ f(x_1, \dots, x_n) = a_0 + a_1x + \dots + a_nx_n$. Пусть $L = \{f \mid f \text{ — линейная}\}$.

Утверждение 4

L — замкнутый класс.

$\in L$	$\notin L$
$\bar{x}, 0, 1, x, x \leftrightarrow y, x + y$	$xy, x \rightarrow y, x \mid y, xy \vee xz \vee yz, x \vee y$

Почему это так? Например, xy — это полином Жегалкина, а он единственный (по Теореме), значит в виде многочлена первой степени конъюнкцию представить невозможно. Аналогично, находя полиномы Жегалкина оставшихся функций, доказываем их линейность или нелинейность:

$$x \vee y = x + y + xy;$$

$$x \rightarrow y = 1 + x + xy;$$

$$x \leftrightarrow y = 1 + x + y;$$

$$x \mid y = 1 + xy;$$

$$xy \vee xz \vee yz = xy + xz + yz.$$

Теорема Поста

Теорема

Система функций A полна тогда и только тогда, когда A не содержится ни в одном из пяти классов: T_1, T_2, S, M, L .

Доказательство. Необходимость доказана в утверждениях 1–4. Докажем достаточность.

1. Лемма о несамодвойственной функции

Подставляя вместо аргументов несамодвойственной функции \bar{x} или x , можно получить константу.

Пусть $f(x_1, \dots, x_n)$ — несамодвойственная функция, тогда найдется вектор $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \{0, 1\}^n$, что $f(\alpha_1, \alpha_2, \dots, \alpha_n) = f(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$. Пусть $\varphi_i(x) = x$ при $\alpha_i = 1$ и $\varphi_i(x) = \bar{x}$ при $\alpha_i = 0$. Тогда функция $h(x) = f(\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x))$ получена подстановкой \bar{x} или x вместо аргументов f и обладает свойством

$$\begin{aligned} h(1) &= f(\varphi_1(1), \varphi_2(1), \dots, \varphi_n(1)) = f(\alpha_1, \alpha_2, \dots, \alpha_n) = \\ &= f(\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) = f(\varphi_1(0), \varphi_2(0), \dots, \varphi_n(0)) = h(0), \end{aligned}$$

значит — это константа.

2. Получение констант (из A)

$A \not\subseteq T_0 \Rightarrow \exists f_0 \in A \setminus T_0$. Если $f_0(1, 1, \dots, 1) = 0$, то $f_0(x, x, \dots, x) = \bar{x}$. Тогда по лемме о несамодвойственной функции из A можно получить константу. Вторая константа получается как отрицание первой.

Если $f_0(1, 1, \dots, 1) = 1$, то $f_0(x, x, \dots, x) = 1$.

$A \not\subseteq T_1 \Rightarrow \exists f_1 \in A \setminus T_1$. Повторяя для f_1 рассуждения, проведенные для f_0 , получим либо константу 0, либо обе константы.

3. Получение отрицания (из A и констант)

$A \not\subseteq M \Rightarrow \exists f_M \in A \setminus M$. Поскольку f_M немонотонная, найдутся векторы $\bar{\alpha}, \bar{\beta} \in \{0, 1\}^n$, что $\bar{\alpha} \leq \bar{\beta}$, $f_M(\bar{\alpha}) = 1$ и $f_M(\bar{\beta}) = 0$. Пусть $\bar{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\bar{\beta} = (\beta_1, \beta_2, \dots, \beta_n)$. Обозначим через I множество тех индексов, для которых $\alpha_i = \beta_i$. Пусть $\varphi_i(x) = \alpha_i$ при $i \in I$ и $\varphi_i(x) = x$ в противном случае. Тогда

функция $h(x) = f_M(\varphi_1(x), \varphi_2(x), \dots, \varphi_n(x))$ получена подстановкой x или констант вместо аргументов f_M и обладает свойствами:

$$h(0) = f_M(\varphi_1(0), \varphi_2(0), \dots, \varphi_n(0)) = f_M(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$$

и $h(1) = f_M(\varphi_1(1), \varphi_2(1), \dots, \varphi_n(1)) = f_M(\beta_1, \beta_2, \dots, \beta_n) = 0$, т.е. является отрицанием.

4. Получение умножения (из А констант и отрицания)

$$A \subsetneq L \Rightarrow \exists f_L \in A \setminus L.$$

Получим сначала нелинейную функцию двух аргументов:

$$f_L(x_1 x_2 \dots x_n) \notin L;$$

$$f_L(x_1 x_2 \dots x_n) = \sum_{S \subseteq \{1 \dots n\}} \alpha_S \prod_{i \in S} x_i.$$

Пусть T — наименьшее по мощности множество $|T| \geq 2$ такое, что $\alpha_T = 1$.

Выберем $i, j \in T, i \neq j$.

Сделаем замену:

$$x_i \rightarrow x;$$

$$x_j \rightarrow y;$$

$$x_k \rightarrow 1, \text{ если } k \in T \setminus \{i, j\};$$

$$x_k \rightarrow 0, \text{ если } k \notin T.$$

После замены получим БФ от 2-х переменных x и y :

$$\psi(x, y) = A + Bx + Cy + Dxy. \text{ Найдем } D.$$

Пусть из слагаемого $\alpha_S \prod_{k \in S} x_k$ при замене получим $xу$. Тогда $\alpha_S = 1$, $i, j \in S, |S| \geq 2$. Кроме того, никакое x_k ($k \in S$) не заменилось на 0, значит $k \in S \Rightarrow k \in T$, т.е. $S \subseteq T$. В силу минимальности T , получим, $S = T$, т.е. $xу$ получится при замене ровно 1 раз. Следовательно, $D = 1$.

$$\psi(x, y) = A + Bx + Cy + xy.$$

$$\begin{aligned} \varphi(x, y) &= \psi(x + C, y + B) = A + B(x + C) + C(y + B) + (x + C)(y + B) = \\ &= A + Bx + BC + Cy + BC + xy + Bx + Cy + BC = A + BC + xy. \end{aligned}$$

$$\text{Отсюда } (A + BC + \varphi(x, y)) = xy.$$

Сложения не нужно: $x = 0 + x, x + 1 = \bar{x}$, что и требовалось доказать.

Следствие 1

В каждой полной системе есть полная подсистема, состоящая из не более, чем 4-х функций.

Доказательство.

Пусть A — полная система.

$f_0 \in A \setminus T_0, f_1 \in A \setminus T_1, f_S \in A \setminus S, f_M \in A \setminus M, f_L \in A \setminus L \Rightarrow \{f_0, f_1, f_S, f_M, f_L\}$ —

полная.

$f_0(1, \dots, 1) = 1 \rightarrow f_1$ не нужна.

$f_0(1 \dots 1) = 0 \rightarrow f_0 \notin S \rightarrow f_S$ не нужна.

Пример 1

$f_0 = 0$;

$f_1 = 1$;

$f_2 = xy$;

$f_3 = x + y + z$.

	T_0	T_1	S	M	L
f_0	+	—	—	+	+
f_1	—	+	—	+	+
f_2	+	+	—	+	—
f_3	+	+	+	—	+

"+" — \in .

"—" — \notin .

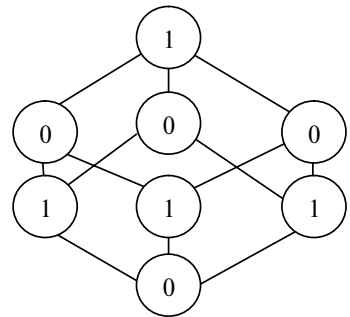
$f_3 : 0 + 0 + 0 = 0$.

$f_3 : 1 + 1 + 1 = 1$.

$\overline{x} + \overline{y} + \overline{z} = 1 + (1 + x) + (1 + y) + (1 + z) = x + y + z$.

$(1, 0, 0) \leq (1, 1, 0)$.

$1 + 0 + 0 > 1 + 1 + 0$.



В каждом столбике есть "—" , значит по теореме Поста эта система полная $\{0, 1, xy, x + y + z\}$. Любая собственная подсистема этой системы не полная.

Пример 2

Полные системы вида $\{f(x, y)\}$:

x	y	F	$ $	\uparrow
0	0	1	1	1
0	1	γ	0	1
1	0	γ	0	1
1	1	0	0	0

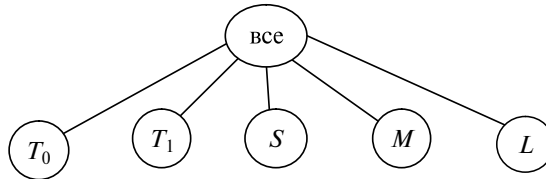
$$x | y = \overline{xy} = 1 + xy \notin L.$$

$$x \uparrow y = \overline{x \vee y} = \bar{x} \cdot \bar{y} = (1+x)(1+y) = 1+x+y+xy \notin L.$$

$\{| \}, \{ \uparrow \}$ — полные.

Следствие 2

T_0, T_1, S, M, L — полный список максимальных по включению замкнутых классов, отличных от множества всех БФ.



Доказательство

Легко убедиться, что для каждой пары из описанных в условии классов найдется функция, лежащая в первом и не лежащая во втором. Например, такие «различающие» функции представлены в следующей таблице:

	$\notin T_0$	$\notin T_1$	$\notin S$	$\notin M$	$\notin L$
$\in T_0$		0	0	$x+y$	xy
$\in T_1$	1		1	$x \leftrightarrow y$	xy
$\in S$	\bar{x}	\bar{x}		\bar{x}	$xy \vee yz \vee xz$
$\in M$	1	0	0		xy
$\in L$	1	0	0	\bar{x}	

Рассмотрим $C \in \{T_0, T_1, S, M, L\}$. Найдется $f \notin C$, значит, $\{f\} \cup C$ не помещается ни в один из классов T_0, T_1, S, M, L , поэтому это полная система, следовательно, множество всех суперпозиций функций этой системы

$(\langle \{f\} \cup C \rangle)$ — все БФ. Таким образом, C — максимальный по включению замкнутый класс.

Пусть X — еще один максимальный замкнутый класс.

Тогда X не помещается в $T_0, T_1, S, M, L \Rightarrow \langle X \rangle$ все БФ.

Пример 3

Пусть у нас имеется большой запас деталей двух типов, вычисляющих следующие трехместные булевы функции:

x	y	z	f_1	f_2
0	0	0	0	1
0	0	1	1	1
0	1	0	1	0
0	1	1	0	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	0
1	1	1	0	1

Можно ли из этих деталей собрать схему, вычисляющую умножение, и если можно, то как?

Полнота:

	T_0	T_1	S	M	L
f_1	+	—	—	—	+
f_2	—	+	—	—	—

$$f_1(x, y, z) \notin M? \quad f_2(x, y, z) \notin M?$$

$$(0, 0, 1) \leq (1, 1, 1); \quad (0, 0, 0) \leq (1, 1, 0);$$

$$f_1(0, 0, 1) = 1 > 0 = f_1(1, 1, 1); \quad f_2(0, 0, 0) = 1 > 0 = f_2(1, 1, 0).$$

$$\text{ПЖ } f_1(x, y, z) = y + z;$$

$$\text{ПЖ } f_2(x, y, z) = z + \overline{xy}z = 1 + x + y + xy + xz + yz + xyz.$$

ПЖ для f_2 можно найти и непосредственно по таблице (см. выше):

$$f_2(x, y, z) = a_0 + a_1x + a_2y + a_3z + a_{23}yz + a_{12}xy + a_{13}xz.$$

$$a_0 = f(0, 0, 0) = 1,$$

$$a_0 + a_1 = f(1, 0, 0) = 0 \Rightarrow a_1 = 1,$$

$$a_0 + a_2 = f(0,1,0) = 0 \Rightarrow a_2 = 1,$$

$$a_0 + a_3 = f(0,0,1) = 0 \Rightarrow a_3 = 0,$$

$$a_0 + a_1 + a_2 + a_3 = f(1,1,0) = 0 \Rightarrow a_{12} = 1, \text{ и т. д.}$$

Константы:

$$1 = f_2(x, x, x) \text{ и } 0 = f_1(x, x, x).$$

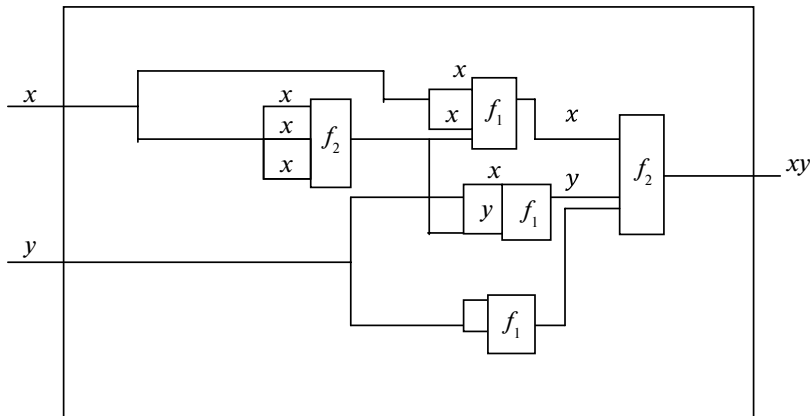
Отрицание:

$$f_1(0,0,1) = 1 \text{ и } f_1(1,1,1) = 0 \Rightarrow f_1(x, x, 1) = \bar{x}.$$

Умножение:

$$f_2(x, y, 0) = 1 + x + y + xy.$$

$$f_2(\bar{x}, \bar{y}, 0) = 1 + \bar{x} + \bar{y} + \bar{x}\bar{y} = 1 + (1+x) + (1+y) + (1+x+y+xy) = xy.$$



$$xy = f_2(f_1(x, x, f_2(x, x, x)), f_1(y, y, f_2(x, x, x)), f_1(y, y, y)).$$

Пример 4

$$\text{Всего } n\text{-местных БФ } 2^{2n} = \left| \{0,1\}^{\{0,1\}^n} \right|.$$

$$\left| T_0 \cap \{0,1\}^{\{0,1\}^n} \right| = 2^{2n-1} = \frac{1}{2} 2^{2n} \text{ (по виду таблицы).}$$

$$\text{Самодвойственных } \left| S \cap \{0,1\}^{\{0,1\}^n} \right| = 2^{2n-1} \text{ (по виду таблицы).}$$

$$\text{Линейных } \left| L \cap \{0,1\}^{\{0,1\}^n} \right| = 2^{2n+1} \text{ (по определению).}$$

Сколько монотонных?

4. Комбинаторика

Основные правила

Комбинаторика — это есть техника подсчета количества элементов в конечных множествах.

Отметим основные правила данного раздела математики:

1) Правило суммы:

Пусть $R = \{A_1, A_2, \dots, A_n\}$ — разбиение A .

Тогда верно равенство $|A| = |A_1| + |A_2| + \dots + |A_n|$.

2) Правило произведения:

Пусть $R = \{A_1, A_2, \dots, A_n\}$ — разбиение A . Тогда $\forall i \ |A_i| = m \ |A| = mn$.

Пример

$$|A| = m, |B| = n \Rightarrow |A \times B| = mn.$$

Доказательство

Пусть $A = \{a_1, a_2, \dots, a_m\}$, а $R = \{\{a_1\} \times B, \{a_2\} \times B, \dots, \{a_m\} \times B\}$ — разбиение $A \times B$, тогда $\forall i$ имеется биекция

$$\varphi: \{a_i\} \times B \xrightarrow{\sim} B \quad \varphi|a; b| = b \Rightarrow |\{a_i\} \times B| = |B| = n \quad |A \times B| = mn.$$

Пример

$$|A| = n \Rightarrow |A^k| = n^k.$$

Доказательство

Применим индукцию по k :

База индукции: $k = 1 \quad |A^1| = n = n^1$.

Шаг индукции: $|A^{k+1}| = |A^k \times A| = |A^k| n = n^k n = n^{k+1}$.

При построении шага индукции воспользовались равенством из примера, приведенного выше.

Пример

$$|A| = m, |B| = n \Rightarrow |B^A| = n^m, \quad |B^A| = \{\varphi \mid \varphi: A \rightarrow B\}.$$

Доказательство.

Пусть $A = \{a_1, a_2, \dots, a_m\}$.

Каждой функции $\varphi: A \rightarrow B$ поставим в соответствие цепочку: $|\varphi(a_1), \varphi(a_2), \dots, \varphi(a_m)| \in B^m$, вследствие чего будем иметь функцию, которая является биекцией. Тогда, учитывая пример 2, получим следующее равенство: $|B^A| = |B^m| = n^m$.

Элементарные комбинаторные функции

Число размещений из n по k — это количество упорядоченных цепочек длины k различных элементов n элементного множества. Число размещений обозначается следующим образом:

$$A_n^k = \left[\begin{matrix} n \\ k \end{matrix} \right].$$

Пример

Пусть $n = 4, k = 2$ для множества $\{A, B, C, D\}$.

Тогда можно составить следующие размещения из 4 по 2:

$AB, BA, CA, DA, AC, BC, CB, DB, AD, BD, CD, DC$. Значит, $A_4^2 = 12$.

Если возьмем множество из 6 элементов и посчитаем аналогично число размещений из 6 по 3, то получим $A_6^3 = 120$.

Приходим к формуле

$$A_n^k = \underset{1}{n}(\underset{2}{n-1})(\underset{3}{n-2})\dots(\underset{k}{n-k+1}) = \frac{n!}{(n-k)!}.$$

Таким образом, формула для вычисления числа размещений имеет вид:

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

Перестановка на $\{1 \dots n\}$ — это биекция из X в X . Число перестановок вычисляется по формуле $P_n = A_n^n = \frac{n!}{0!} = n!$

Число сочетаний из n по k — это есть число k — элементарных подмножеств n — элементного множества. Число сочетаний обозначается следующим образом: $C_n^k = \binom{n}{k}$.

Свойства числа сочетаний

$$1) C_n^0 = 1, C_n^k = 0, k < 0, k > n.$$

$$2) C_n^k = C_n^{n-k}.$$

Доказательство

Пусть $|A| = n, B \subseteq A, |B| = k \Rightarrow A \setminus B \subseteq A, |A \setminus B| = n - k$, то есть $\varphi(B) = A \setminus B$ — биекция между k -элементами и $(n - k)$ — элементами указанных множеств.

$$3) C_n^k + C_n^{k+1} = C_{n+1}^{k+1}.$$

Доказательство

$|A| = n + 1, a \in A$. Разобьём все $k + 1$ элементные подмножества множества A на 2 вида:

а) с элементом a ; остальные k элементов — из множества $A \setminus \{a\}$. Таких подмножеств будет C_n^k ;

б) без элемента a ; все $k + 1$ элементов — из множества $A \setminus \{a\}$. Таких подмножеств будет C_n^{k+1} . Свойство доказано.

Треугольник Паскаля

$$\begin{array}{rcl}
 & & 1 \\
 & & 1 \ 1 \\
 C_0^0 & & 1 \ 2 \ 1 \\
 C_1^0 \ C_1^1 & \Rightarrow & 1 \ 3 \ 3 \ 1 \\
 C_2^0 \ C_2^1 \ C_2^2 & & 1 \ 4 \ 6 \ 4 \ 1 \\
 C_3^0 \ C_3^1 \ C_3^2 \ C_3^3 & & 1 \ 5 \ 10 \ 10 \ 5 \ 1 \\
 & & 1 \ 6 \ 15 \ 20 \ 15 \ 6 \ 1
 \end{array}$$

4) Бином Ньютона.

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

Доказательство

$$(x + y)^n = \underbrace{(x + y)(x + y) \dots (x + y)}_n = \sum x^k y^{n-k}.$$

C_n^k — число k -элементных подмножеств некоторых скобок, из которых берется x n -элементного множества всех скобок.

$$5) C_n^k = \frac{n!}{(n-k)!k!}$$

Для данного свойства приведем два доказательства.

Доказательство I

Пусть

A_n^k — число упорядоченных цепочек длины k .

C_n^k — число неупорядоченных цепочек длины k .

P_k — число способов упорядочения цепочек длины k .

Тогда

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

Доказательство II

Пусть $A = \{a_1, a_2, \dots, a_n\}$. Каждому $x \subseteq A$ поставим в соответствие X_x следующим образом:

$$X_x|a| = \begin{cases} 1, & a \in X, \\ 0, & a \notin U. \end{cases}$$

Тогда

$$|x| = k \Leftrightarrow |\text{supp } X_x| = k.$$

$X_x \leftrightarrow |X_x(a_1), X_x(a_2), \dots, X_x(a_n)|$ — это анаграмма слова.

Всего у такого слова $\underbrace{11\dots 1}_k \underbrace{00\dots 0}_{n-k} \frac{n!}{(n-k)!k!}$ анаграмм.

6) Треугольник Паскаля:

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & / \backslash & & & & \\ 0 & & \mathbf{0} & & & & \\ & & / \backslash / \backslash & & & & \\ 0 & & \mathbf{0} & & 0 & & \\ & & / \backslash / \backslash / \backslash & & & & \\ 0 & & \mathbf{0} & & 0 & & 0 \\ & & / \backslash / \backslash / \backslash / \backslash & & & & \\ 0 & & 0 & & \mathbf{0} & & 0 & & 0 \end{array}$$

Сумма элементов, выделенных полужирным, равна элементу, выделенному полужирным курсивом.

$$C_n^n + C_{n+1}^n + C_{n+2}^n + \dots + C_{n+k}^n = C_{n+k+1}^{n+1}.$$

Доказательство

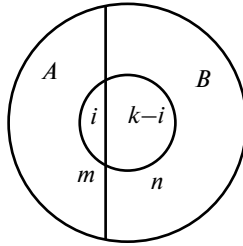
Доказательство проведем с помощью индукции по k :

Б. И. при $k = 0$ $C_n^n = 1 = C_{n+1}^{n+1}$.

Ш. И. $C_n^n + C_{n+1}^n + C_{n+2}^n + \dots + C_{n+k}^n + C_{n+k+1}^n = C_{n+k+1}^{n+1} + C_{n+k+1}^n = C_{n+k+2}^{n+1}$.

$$7) C_{m+n}^k = \sum_{i=0}^k C_m^i \cdot C_n^{k-i}.$$

Доказательство



$C_m^i C_n^{k-i}$ множеств пересекающихся с A по i элементам и с B по $n-i$ элементам.

ε — первообразная — это есть корень из 1-й степени n , если $\varepsilon^n = 1$.

$$\forall k \in \{1, \dots, n-1\}, \varepsilon^k \neq 1.$$

Пусть $\varepsilon^3 = 1, \varepsilon \neq 1$.

Тогда с использованием свойства 4 можно записать следующие равенства:

$$(1 + \varepsilon)^n = C_n^0 + C_n^1 \varepsilon + C_n^2 \varepsilon^2 + C_n^3 \varepsilon^3 + C_n^4 \varepsilon + C_n^5 \varepsilon^2 + C_n^6 + \dots,$$

$$(1 + \varepsilon^2)^n = C_n^0 + C_n^1 \varepsilon^2 + C_n^2 \varepsilon^4 + C_n^3 + C_n^4 \varepsilon^2 + C_n^5 \varepsilon + C_n^6 + \dots,$$

$$(1 + 1)^n = C_n^0 + C_n^1 + C_n^2 + C_n^3 + C_n^4 + C_n^5 + C_n^6 + \dots$$

Заметим, что

$$1 + \varepsilon + \varepsilon^2 = \frac{\varepsilon^3 - 1}{\varepsilon - 1} = \frac{0}{\neq 0} = 0.$$

А теперь, сложив первые три равенства и преобразовав полученную правую часть при помощи четвертой формулы, придем к равенству:

$$\frac{(1 + \varepsilon)^n + (1 + \varepsilon^2)^n + 2^n}{3} = C_n^0 + C_n^3 + C_n^6 + C_n^9 + \dots$$

Учитывая, что

$$\varepsilon^2 = \varepsilon^{-1},$$

получим

$$|\varepsilon| = 1 = |\varepsilon^{-1}| \Rightarrow \varepsilon^{-1} = \bar{\varepsilon}.$$

$$(1 + \varepsilon^2)^n = (1 + \bar{\varepsilon})^n = (\overline{1 + \varepsilon})^n = \overline{(1 + \varepsilon)^n}.$$

$$C_n^0 + C_n^3 + \dots = \frac{2 \operatorname{Re}(1 + \varepsilon)^n + 2^n}{3}.$$

$$\text{Пусть } \varepsilon = -\frac{1}{2} + i \frac{\sqrt{3}}{2} \Rightarrow \varepsilon + 1 = \frac{1}{2} + i \frac{\sqrt{3}}{2} = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3}.$$

Тогда

$$(1 + \varepsilon)^n = \underbrace{\cos \frac{\pi n}{3}}_{\operatorname{Re}} + i \sin \frac{\pi n}{3},$$

$$C_n^0 + C_n^2 + \dots = \frac{2^n + 2 \cos \frac{\pi n}{3}}{3}.$$

Число размещений с повторениями — это число способов разместить n одинаковых предметов по k различным большим ящикам.

Обозначение \tilde{C}_n^k .

Построим биекцию между раскладками n одинаковых предметов по k различным большим ящикам и словами, составленными из n нулей и $k-1$ единиц:

$$\tilde{C}_{20}^6 = C_{25}^5,$$

$$\tilde{C}_n^k = C_{n+k-1}^{k-1} = C_{n+k-1}^n.$$

Задача (о кроликах)

В момент $t = 0$ родилась пара кроликов. Кролики два месяца растут, а потом каждый месяц приносят по одной новорожденной паре. Сколько пар кроликов будет через 10 месяцев, 1000 месяцев.

Пусть F_k — количество пар кроликов в момент $t = k$. Тогда

$$F_0 = 1 \quad \forall n \geq 1 \Rightarrow F_n = \underbrace{F_{n-1}}_{\text{старые}} + \underbrace{F_{n-2}}_{\text{новорожденные}}$$

$$F_1 = 1,$$

$$F_2 = 2, F_3 = 3, F_4 = 5, F_5 = 8, F_6 = 13, F_7 = 21, F_8 = 34, \dots$$

Построенная последовательность $\{F_n\}_{n=0}^{\infty}$ — последовательность Фибоначчи.

$\{a_n\}_{n=0}^{\infty} \subseteq R^{\infty}$ — это рекуррентная последовательность, если

$$\exists f: R^{\infty} \rightarrow R, \exists n_0 \in N, \forall n \geq n_0 \quad a_n = f(a_{n-1}, a_{n-1}, \dots, a_0, 0, \dots, 0).$$

$\{a_n\}_{n=0}^{\infty} \subseteq R^{\infty}$ — это рекуррентная последовательность порядка m , если

$$\exists f: R^m \rightarrow R \quad \forall n \geq m \quad a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-m}).$$

$\{a_n\}_{n=0}^{\infty} \subseteq R^{\infty}$ — это линейная рекуррентная последовательность порядка m , если $\exists \alpha_1, \alpha_2, \dots, \alpha_m \in R, \quad \forall n \geq m \quad a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \dots + \alpha_m a_{n-m}$ — линейное рекуррентное соотношение порядка m .

Пусть $\{a_n\}_{n=0}^{\infty} \subseteq R^{\infty}$, тогда $f(x) = \sum_{n=0}^{\infty} a_n x^n$ — это есть обыкновенная производящая функция последовательности $\{a_n\}_{n=0}^{\infty}$.

Рассмотрим действия с рядами. Пусть $g(x) = \sum_{n=0}^{\infty} b_n x^n$.

Тогда будут справедливы следующие равенства:

$$1) \quad f(x) + g(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

$$2) \quad f(x) \cdot g(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n.$$

$$3) \quad f(\alpha x^k) = \sum_{n=0}^{\infty} \alpha^n x^{kn}.$$

$$4) \quad f'(x) = \sum_{n=0}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n.$$

$$5) \quad \int_0^x f(t) dt = \sum_{n=0}^{\infty} \frac{a_n x^{n+1}}{n+1} = \sum_{n=1}^{\infty} \frac{a_{n-1}}{n} x^n.$$

Лемма

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \quad a_0 \neq 0 \quad (\exists a_0^{-1}) \quad \text{тогда} \quad \exists f^{-1}(x) = \sum_{n=0}^{\infty} b_n x^n.$$

Доказательство

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1.$$

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n = 1.$$

$$a_0 b_0 = 1 \rightarrow b_0 = a_0^{-1}.$$

$$a_0 b_1 + a_1 b_0 = 0 \rightarrow b_1 = a_0^{-1} (-b_0 a_1).$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \rightarrow b_2 = a_0^{-1} (-a_1 b_1 - a_2 b_0).$$

$$a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 0 \rightarrow b_3 = a_0^{-1} (-a_1 b_2 - a_2 b_1 - a_3 b_0).$$

.....

$$\frac{1}{(1-x)^2} = \left(\frac{1}{1-x} \right)' = \sum_{n=0}^{\infty} (x^n)' = \sum_{n=0}^{\infty} n x^{n-1} = \sum_{n=0}^{\infty} (n+1) x^n.$$

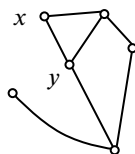
Тогда

$$\begin{aligned} & \left(\sum_{n=0}^{\infty} (n+1) x^n \right) \cdot (1-2x-x^2) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n = \\ & = \sum_{n=0}^{\infty} \left(\sum_{k=n-2}^n (k+1) b_{n-k} \right) x^n = \\ & = 1 + (2x + 1(-2x)) + \sum_{n=2}^{\infty} ((n-1)1 + n(-2) + (n+1)1) x^n = 1. \end{aligned}$$

5. Теория графов

Определение и задание графа

Приведем пример графа. Важно, какие точки соединены, а какие нет. Это способ изображения любого симметричного бинарного отношения.

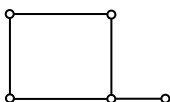


Помеченный граф G — это есть $G = (V, E)$, где V — конечное множество вершин, а $E = \{\{x, y\} \mid x \neq y; x, y \in V\} = V^{(2)}$ — множество ребер.

Пример

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

Как еще можно задать граф? Матрице бинарного отношения соответствует матрица смежности графика.



Матрица смежности графа — это есть матрица $M = (\alpha_{ij})_{n \times n}$, где $n = |V|$, коэффициенты которой находятся следующим образом:

$$\alpha_{ij} = \begin{cases} 1, & i\text{-я и } j\text{-я вершина — ребро,} \\ 0, & \text{иначе.} \end{cases}$$

Согласно определению, матрица смежности выше приведенного графа имеет вид

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Матрица инцидентности графа — это матрица $I = (\beta_{ij})_{n \times m}$, где $n = |V|$, $m = |E|$, а элементы β определяются следующим образом:

$$\beta_{ij} = \begin{cases} 1, & \text{если } i\text{-вершина принадлежит } j\text{-му ребру,} \\ 0, & \text{иначе.} \end{cases}$$

Матрица инцидентности выше приведенного графа имеет вид

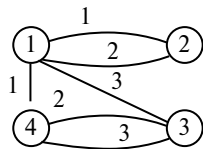
$$I = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

где $m = |E|$, $n = |V|$, причем для числа ребер справедлива оценка $0 \leq m \leq |V^2| = C_n^2$.

Мультиграф — это есть граф $G = (V, E)$, где V — конечное множество вершин, а E — множество ребер с кратностями, т. е. $E \subseteq V^{(2)} \times N$.

Пример

$G = (\{1, 2, 3, 4\}, \{(\{1, 2\}, 1), (\{1, 2\}, 2), (\{1, 3\}, 3), (\{1, 4\}, 1), (\{3, 4\}, 1), (\{3, 4\}, 2), (\{3, 4\}, 3)\})$.



Матрица смежности мультиграфа G есть матрица $M = (\alpha_{ij})_{n \times m}$, где $n = |V|$, $m = |E|$, α_{ij} — количество рёбер, соединяющих i -ю и j -ю вершины.

Матрицы смежности и инцидентности для графа, рассматриваемого в примере, имеют вид

$$M = \begin{pmatrix} 0 & 2 & 1 & 1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Степень вершины v — это есть число ребер, инцидентных данной вершине. Степень вершины v обозначается записью $\deg v$.

Лемма о рукопожатиях

$$\sum_{v \in V} \deg v = 2|E|.$$

Доказательство

Сумма степеней всех вершин графа равна числу концов ребер данного графа, а именно:

$$\sum_{v \in V} \deg v = 2|E|.$$

Пример

В графе 100 вершин, каждая соединена с 15-ю другими. Сколько в графе ребер?

Ответ: $\frac{100 \cdot 15}{2} = 750.$

$G = (V, E)$ — ориентированный граф (ОРГРАФ (digraph)), если V — конечное множество (вершины), а $E \subseteq V \times V$.

$G = (V, E)$ — ориентированный мультиграф, если $E \subseteq V \times V \times N$.

Матрица смежности ориентированного графа — это матрица $M = (\alpha_{ij})_{n \times n}$, α_{ij} = количество ребер с началом в i -й вершине и концом в j -й.

Матрица инцидентности ориентированного графа — это матрица

$$I = (\beta_{ij})_{n \times m}, \beta_{ij} = \begin{cases} 1, & i\text{-я вершина — начало } j\text{-го ребра,} \\ -1, & i\text{-я вершина — конец } j\text{-го ребра,} \\ a \neq \pm 1, & i\text{-я вершина — и начало, и конец } j\text{-го ребра,} \\ 0, & \text{иначе.} \end{cases}$$

$\deg_+ v$ — степень исхода вершины v — это число ребер с началом в вершине v .

$\deg_- v$ — степень захода вершины v — это есть число ребер с концом v .

Лемма о рукопожатиях (для орграфов)

$$\sum_{v \in V} \deg_+ v = |E| = \sum_{v \in V} \deg_- v.$$

Доказательство

Количество начал рёбер = количеству рёбер = количеству концов рёбер.

Операции с множествами

Пусть даны два графа: $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$, тогда можно построить следующие графы:

$$G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2),$$

$$G_1 \cap G_2 = (V_1 \cap V_2, E_1 \cap E_2),$$

$$G_1 \setminus G_2 = (V_1 \setminus V_2, E_1 \setminus E_2),$$

$$G_1 \setminus G_2 = (V_1 \setminus V_2, E_1 \setminus E_2 \cap (V_1 \setminus V_2)^{(2)}).$$

$$H = (U, F), G = (V, E) \text{ — графы,}$$

$$H \subseteq G \text{ (} H \text{ подграф } G \text{) — если } U \subseteq V, F \subseteq E.$$

Изоморфизм графов

$\varphi: V_1 \rightarrow V_2$ — изоморфизм графов $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$, если $\forall u, v \in V_1 \quad \{u, v\} \in E_1 \Leftrightarrow \{\varphi(u), \varphi(v)\} \in E_2$.

Замечание

Если картинки графов изображены одинаково, то такая функция есть.

Если между графами G_1 и G_2 существует изоморфизм, то говорят (G_1 изоморфен G_2), пишут — $G_1 \cong G_2$.

Теорема (об изоморфизме)

Отношение изоморфизма есть эквивалентность на множестве графов.

Доказательство.

1) \cong рефлексивно (тождественное отображение — изоморфизм).

2) \cong симметрично:

$$G_1 \cong G_2, \text{ то есть } \exists \varphi: \forall V_1 \rightarrow V_2 \quad \forall u, v \quad \{u, v\} \in E_1 \Leftrightarrow \{\varphi^{-1}(u), \varphi^{-1}(v)\} \in E_2.$$

Заметим, что $\varphi^{-1}: V_2 \rightarrow V_1$

$$\forall a, b \in V_2 \quad \varphi^{-1}(a) = u, \quad \varphi(u) = a,$$

$$\varphi^{-1}(b) = v, \quad \varphi(v) = b,$$

$$\{a, b\} \in E_2 \Leftrightarrow \{\varphi^{-1}(u), \varphi^{-1}(v)\} \in E_1.$$

3) \cong транзитивно:

$$G_1 \cong G_2, G_2 \cong G_3.$$

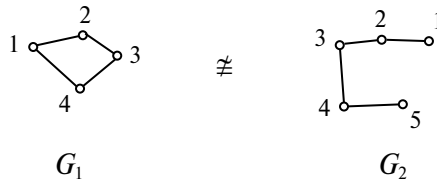
$$\begin{aligned}
\varphi: V_1 &\rightarrow V_2 \quad \forall u, v \in V_1 \quad \{u, v\} \in E_1 \leftrightarrow \{\varphi(u), \varphi(v)\} \in E_2, \\
\psi: V_2 &\rightarrow V_3 \quad \forall x, y \in V_2 \quad \{x, y\} \in E_2 \leftrightarrow \{\psi(x), \psi(y)\} \in E_3, \\
\varphi \circ \psi: V_1 &\rightarrow V_3 \quad \forall u, v \in V_1 \quad \{u, v\} \in E_1 \xrightarrow{\varphi} \{\varphi(u), \varphi(v)\} \in E_2 \xrightarrow{\psi} \\
&\xrightarrow{\psi} \{\psi(\varphi(u)), \psi(\varphi(v))\} \in E_3.
\end{aligned}$$

Абстрактный граф — это есть класс множества помеченных графов по отношению изоморфизма \cong .

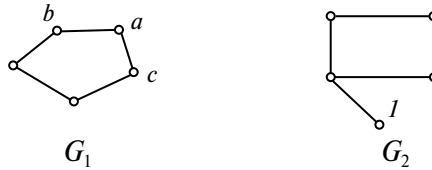
Замечание

Одинаковые изображения \Rightarrow один и тот же абстрактный граф.

Пример



Данные графы не являются изоморфными, так как имеют разное количество вершин.



Предположим, что эти графы изоморфны, и вершине 1 соответствует вершина a . Тогда вершинам b и c должны соответствовать два различных соседа вершины 1 во втором графе. Однако их не существует, и, следовательно, графы неизоморфны.

Эти соображения можно обобщить следующим образом:

Замечание

Если φ изоморфизм G_1 на G_2 то $\forall v \in V_1 \quad \deg v = \deg \varphi(v)$.

В связи с этим возникает следующее понятие:

Для графа $G = (V, E)$, $|V| = n$, упорядоченный набор степеней его вершин, x_1, x_2, \dots, x_n , где $x_i \in N \cup \{0\}$, называется степенной последовательностью графа G .

Замечание

Степенные последовательности изоморфных графов одинаковы.

О сложности алгоритмов

Будем пользоваться интуитивным понятием алгоритма. Каждый алгоритм имеет ВХОД — последовательность битов. Пусть n — длина ВХОДА. Под сложностью алгоритма будем понимать такую функцию $t: N \rightarrow N$, что $t(n)$ — это наибольшее число битовых операций, выполняемых алгоритмом при длине входа равной n . Будем интересоваться лишь скоростью роста таких функций.

$f(x) = O(g(x))$, если $\exists c > 0 \forall x > 0 \ f(x) \leq cg(x)$.

$$f(x) \approx g(x) \Leftrightarrow \begin{cases} f(x) = O(g(x)) \\ g(x) = O(f(x)) \end{cases}.$$

Рассмотрим задачу о нахождении Det .

Дано: $A = (\alpha_{ij})_{m \times m}$, $\alpha_{ij} \in \{0, 1\}$.

Найти: $Det(A) \text{ MOD } 2$ (то есть найти $|A|$ над полем $\{0, 1\}$).

Алгоритм 1 состоит в рекурсивном разложении по 1-й строке:

$$|A| = a_{11} \cdot A_{11} + a_{12} \cdot A_{12} + \dots + a_{1m} \cdot A_{1m},$$

$$t(m) \geq m \cdot t(m-1), \quad t(m) \geq m!, \quad t(n) \geq (\sqrt{n})!$$

$\forall k \ t(n) > n^k$ ($t(n)$ растет быстрее любого многочлена).

Алгоритм 2 позволит решить данную задачу при помощи метода Гаусса.

Проводим элементарными преобразованиями по строкам матрицу к верхнему треугольному виду:

$$t(m) \leq m + 3m + (m-1)m = m^2 + 3m,$$

$$t(m) \leq m + 3m + (m-1)m + t(m-1),$$

$$t(m) \leq (m+3)m + t(m-1) \leq \dots$$

$$\begin{aligned}
&\leq t(m) \leq (m+3)m + t(m-1) = 2C_{m+1}^2 + C_m^1 + t(m-1) \leq \\
&\leq \dots \leq \sum_{k=1}^{m+1} 2C_k^2 + \sum_{k=1}^m 2C_k^1 = 2C_{m+2}^3 + 2C_{m+1}^2 = \frac{(m+2)(m+1)m}{3} + (m+1)m = \\
&= \frac{(m+1)m(m+5)}{3} = O(m^3).
\end{aligned}$$

В итоге получили, что наибольшее число битовых операций удовлетворяет следующему равенству:

$$t(n) = O\left(n^{\frac{3}{2}}\right).$$

Сложность задачи — это минимальная сложность алгоритма, решающего задачу.

Сложность $\text{ADD} \sim n$.

Сложность Det между n и $n^{3/2}$.

Замечание

Задача считается простой, если ее сложность есть многочлен от n ($O(n^k)$). Алгоритм эффективный, если $t(n) = O(n^k)$.

Введем следующие обозначения:

Множество P — множество всех задач, для которых есть эффективный алгоритм.

Множество NP — множество задач, для которых есть алгоритм, который проверяет решение за время $O(n^k)$.

Задача называется *NP-полной задачей* — если наличие алгоритма, решающего ее за время $O(n^k)$, означает, что для любой задачи из NP существует алгоритм решающий ее за время $O(n^k)$.

Теорема Кука

Задача «выполнимость» NP -полна (в настоящее время известно около 510^3 NP -полных задач).

Вопрос $P = NP?$ — это один из вопросов на миллион долларов.

Сложность задачи проверки изоморфизма графов не известна. Легко показать, что эта задача лежит в классе NP . Для нее в настоящее время нет полиномиального алгоритма и не доказано, что эта задача NP -полна.

Маршруты

Маршрут в графе $G = (V, E)$ — это последовательность $v_0 e_1 v_1 e_2 v_2, \dots, e_n v_n$, $e_i \in E$, $v_i \in V$ такая, что $\forall i \in \{1, \dots, n\} e_i = \{v_{i-1}, v_i\}$, v_0 — начало маршрута, v_n — конец маршрута, n — длина маршрута.

Маршрут с началом u и концом v называется (u, v) -маршрутом.

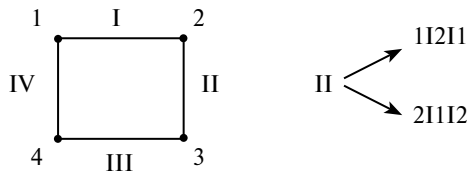
Замечание 1

Последовательность $v_0 e_1 e_2 \dots e_n$ однозначно определяет маршрут.

Замечание 2

e_1, e_2, \dots, e_n может уже не определять маршрут.

Пример



Замечание 3

Пусть G — граф (без кратных ребер), тогда $v_0, v_1, v_2, \dots, v_n$ однозначно определен маршрут.

Цепь — маршрут без повторяющихся ребер.

Простой маршрут — это маршрут, в котором вершины v_0, v_1, \dots, v_{n-1} попарно различны и $v_n \notin \{v_1, v_2, \dots, v_{n-1}\}$.

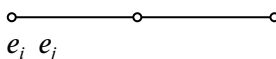
Замечание 4

Каждый простой маршрут, кроме маршрута $veuev$, является цепью.

Доказательство

Воспользуемся методом от противного. Предположим, что $e_i = e_j$ ($i < j$).

Если $j = i + 1$, то $v_{i-1} = v_j = v_{i+1} \Rightarrow i = 0, j = 1$.



Если $j = i + 1$, то $\{v_{i-1}, v_i\} = \{v_{j-1}, v_j\}$,

$$v_i = \begin{cases} v_j, \\ v_{j-1}. \end{cases}$$

Маршрут называется *циклическим*, если $v_0 = v_n$.

Циклическая цепь — это цикл.

Утверждение 1

Из каждого (u, v) маршрута можно выделить простую (u, v) -цепь ($u \neq v$).

Доказательство

Пусть дан маршрут:

$$u = v_0 e_1 v_1 e_2 v_2 \dots v_{n-1} e_n v_n = v.$$

Если вершины v_0, v_1, \dots, v_{n-1} попарно различны и $v_n \notin \{v_1, \dots, v_{n-1}\}$ (то есть v_0, \dots, v_n попарно различны), то это уже простой (u, v) маршрут (по замечанию 2).

Если $v_i = v_j$ ($i < j$), $v_0 e_1 v_1 e_2 v_2 \dots e_i v_i \cancel{e_{i+1} v_{i+1} \dots e_j v_j} e_{j+1} \dots e_n v_n$.

Получим (u, v) -маршрут меньшей длины путем удаления указанных выше ребра и вершины.

Действуя таким образом, получим конечный процесс, обрывающийся в ситуации, когда маршрут простой.

Утверждение 2

Из каждого цикла можно выделить простой цикл (положительной длины).

Доказательство

Пусть дан маршрут

$$v_0 e_1 v_1 e_2 v_2 \dots e_n v_n = v_0, \quad |\{e_1, e_2, \dots, e_n\}| = n, \quad v_1 \neq v_0 = v_n,$$

тогда $v_1 e_2 v_2 e_3 v_3 \dots e_n v_n = v$, $u \neq v$ — это (u, v) -цепь.

Выделим простую (u, v) -цепь (по утверждению 1): $u = u_1 f_2 u_2 f_3 u_3 \dots f_m u_m = v$.

Тогда $u = u_1 f_2 u_2 f_3 u_3 \dots f_m u_m = v = v_n = v_0$ — цикл, в котором вершины не могут повторяться.

Все пары вершин, кроме (v_0, u_m) , — пары разных вершин.

Пример

12421 → 121

1 I 2 II 4 III 2 I 1 вычеркиванием нельзя получить 1 III 2 II 2 II 1.

Утверждение 3

Объединение двух различных (u, v) -цепей содержит простой цикл.

Доказательство

Даны цепи:

$$u = v_0 e_1 v_1 e_2 v_2 \dots e_n v_n = v,$$

$$u = u_0 f_1 u_1 f_2 u_2 \dots f_m u_m = v.$$

Пойдем по цепям слева направо. Поскольку они разные, то возможны два случая:

$$1) \exists i: e_i \neq f_i.$$

$$2) \forall i \leq \min\{m, n\} e_i = f_i \Rightarrow n > m.$$

В случае 2) $v_m e_{m+1} v_{m+1} \dots e_n v_n = v_m$ — цикл. По утверждениям 2 и 3 можно выделить простой цикл.

Пусть реализуется случай 1). Найдем такое наименьшее i , что $e_i \neq f_i$. Тогда $v_0 = u_0, \dots, v_{i-1} = u_{i-1} = x$, $v_i \neq u_i$.

Найдем на 1-й цепи первую вершину, следующую после вершины x и лежащую на 2-й цепи, назовем ее y . Рассмотрим маршрут $x \xrightarrow{1} y \xrightarrow{2(\text{обратно})} x$.

Заметим, что он является циклом.

Внутри кусков $x \xrightarrow{1} y$ и $y \xrightarrow{2(\text{обратно})} x$ ребра не повторяются, так как это части цепей. Предположение о том, что некоторое ребро e куска $x \xrightarrow{1} y$ встречается на куске $y \xrightarrow{2(\text{обратно})} x$ противоречит выбору y . Рассмотрим вершину перед ребром e . По утверждению 2 можно выделить простой маршрут.

Утверждение 4

Пусть C и D есть два разных цикла с общим ребром e . Тогда $C \cup D \setminus \{e\}$ содержит цикл.

Доказательство

Рассмотрим ребро $e = \{u, v\}$.

Тогда $C \setminus \{e\}$ — это (u, v) -цепь, $D \setminus \{e\}$ — это другая (u, v) -цепь.

По утверждению 3 $(C \setminus \{e\}) \cup (D \setminus \{e\})$ содержит простой цикл

$$(C \setminus \{e\}) \cup (D \setminus \{e\}) = (C \cup D) \setminus \{e\}.$$

СВЯЗНОСТЬ

$G = (V, E)$ — граф, $u, v \in V$.

$u \sim v$ (и связана с V) \Leftrightarrow в G есть (u, v) -маршрут.

$\sim \subseteq V \times V$.

Утверждение

\sim — эквивалентность на V .

Доказательство.

\sim — рефлексивно ($\forall u \in V$ есть (u, u) -маршрут нулевой длины).

\sim — симметрично (каждый маршрут, переписанный в обратном порядке, снова является маршрутом).

\sim — транзитивно (маршруты (u, v) и (v, ω) можно соединить по вершине v , в результате чего получится (u, ω) -маршрут).

Класс эквивалентности $[v]$ называется компонентой связности графа G .
Число компонент связности графа G обозначают через $k(G)$.

Утверждение

Следующие условия эквивалентны:

1) $k(G) = 1$,

2) $\exists u \in V \quad \forall v \in V \quad u \sim v$,

3) $\forall u, v \in V \quad u \sim v$.

Доказательство

3) \rightarrow 2) очевидно.

2) \rightarrow 1)

$V = [u] \Rightarrow k(G) = 1$.

1) \rightarrow 3)

$\forall u, v \in V \quad \exists \omega \in V \quad u \in [\omega], \quad v \in [\omega],$

$$\begin{cases} u \sim \omega \\ v \sim \omega \end{cases} \rightarrow \begin{cases} u \sim \omega \\ \omega \sim v \end{cases} \rightarrow u \sim v.$$

Ребро e — мост в графе G , если $k(G \setminus e) > k(G)$.

Замечание

$$\forall e \in E \quad k(G \setminus e) > k(G).$$

Доказательство

$u \sim v \Leftrightarrow$ в G есть (u, v) -маршрут.

$u \approx v \Leftrightarrow$ в графе $G \setminus e$ есть (u, v) -маршрут.

Очевидно $\approx \subseteq \sim$.

$$V_{\approx} = \{A_1, A_2, \dots, A_m\},$$

$$V_{\sim} = \{B_1, B_2, \dots, B_k\},$$

$$|A_1| + |A_2| + \dots + |A_m| = |V| = |B_1| + |B_2| + \dots + |B_k|.$$

Тогда

$$\forall i, j \quad i \neq j: B_i \cap B_j = \emptyset, A_i \subseteq B_i \Rightarrow A_i \not\subseteq B_j \text{ и } \forall i \quad B_i \neq \emptyset \quad \exists v \in B_i.$$

$A_i = [v]_{\sim} \Rightarrow A_i \subseteq B_i$. Это значит, что мы построили инъективное отобра-

жение: $\varphi: \{1, \dots, k\} \rightarrow \{1, 2, \dots, m\} \quad \varphi(i) = (t)$.

Значит, $m \geq k$. Таким образом $\forall e \in E$:

$$1) \quad e \text{ — мост} \Rightarrow k(G \setminus e) > k(G),$$

$$2) \quad e \text{ — не мост} \Rightarrow k(G \setminus e) = k(G).$$

Лемма (о мосте)

$$1) \quad e \text{ — мост} \Rightarrow k(G \setminus e) = k(G) + 1.$$

$$2) \quad e \text{ — мост} \Rightarrow e \text{ не лежит ни в каком цикле } G.$$

$$3) \quad e \text{ не лежит ни в каком цикле } G \Rightarrow e \text{ — мост.}$$

Доказательство

$$e = \{x, y\}.$$

Заметим, что $[x]_{\sim} = [x]_{\approx} \cup [y]_{\approx}$.

$$\supseteq: [x]_{\approx} \subseteq [x]_{\sim}, \text{ так как } \approx \subseteq \sim \left(z \in [x]_{\approx} \rightarrow z \approx x \rightarrow z \in [x]_{\sim} \right),$$

$$[y]_{\approx} \subseteq [x]_{\sim} \quad z \in [y]_{\approx} \rightarrow z \approx y \rightarrow \begin{cases} y \sim x \\ z \sim y \end{cases} \rightarrow z \sim x \rightarrow z \in [x]_{\sim}$$

$$\subseteq: z \in [x]_{\sim}$$

То есть, в G есть (z, x) -маршрут, если на нем нет e , тогда

$z \approx x \rightarrow z \in [x]_{\approx} \rightarrow z \in [x]_{\approx} \cup [y]_{\approx}$, но если на этом маршруте есть e , тогда

$$z = v_0 e_1 v_1 e_2 v_2 \dots e_n v_n = x.$$

Найдем наименьшее i , такое что $e_i = e$.

$$v_{i-1} \in \{x, y\} \left\{ \begin{array}{l} v_{i-1} = x \Rightarrow z \approx x \rightarrow z \in [x]_{\approx} \\ v_{i-1} = y \Rightarrow z \approx y \rightarrow z \in [y]_{\approx} \end{array} \right. \Rightarrow z \in [x]_{\approx} \cup [y]_{\approx}.$$

Заметим, что если $[x]_{\approx} \subseteq [y]_{\approx}$, то $[z]_{\approx} = [y]_{\approx}$.

$z \notin [x]_{\approx} \Rightarrow z \not\approx x \rightarrow z \not\approx y \Rightarrow \text{на } \forall (z, v)$ -маршруте в графе G нет ребра e , то есть каждый (z, v) -маршрут в G является маршрутом в $G \setminus e$, отсюда $k(G \setminus e) = k(G) \Leftrightarrow [x]_{\approx} = [y]_{\approx}$.

А если $[x]_{\approx} \neq [y]_{\approx}$, то $k(G \setminus e) = k(G) + 1$.

Но если e лежит в цикле графа $G \Rightarrow$ в графе $G \setminus e$ есть (x, y) -маршрут, то есть $x \approx y \Rightarrow e$ — не мост.

e не мост $\Rightarrow x \approx y$ и в графе $G \setminus e$ есть (x, y) -маршрут, тогда выделим из него простой маршрут, добавим e и получим цикл с ребром e .

Число реберной связности графа $\varepsilon(G)$ — это есть наименьшее число ребер, которое нужно удалить из графа, чтобы он стал несвязным.

Замечание 1

Граф G — несвязный $\Leftrightarrow \varepsilon(G) = 0$.

Граф G — связный с мостом $\Leftrightarrow \varepsilon(G) = 1$.

Замечание 2

$$\varepsilon(G) \leq \min \deg v, \quad v \in V.$$

Пример

$\varepsilon(P_n) = 1$, так как каждое ребро в цепи — мост.

Если $\varepsilon(C_n) = 2$, мостов нет.

Число вершинной связности графа $\nu(G)$ — это наименьшее число вершин, которое нужно удалить из графа, чтобы он стал несвязным или одновершинным.

Пример

$$\nu(k_n) = n - 1.$$

Теорема

$$v(G) \leq \varepsilon(G).$$

Доказательство

Пусть граф G несвязный $\Rightarrow v(G) = 0 = \varepsilon(G)$.

А теперь пусть G связный граф, тогда возможны следующие случаи.

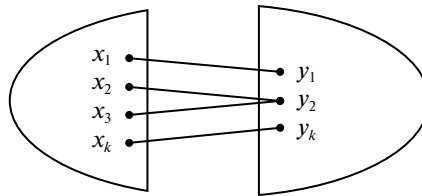
Случай 1: в G есть мост $\Rightarrow \varepsilon(G) = 1$.

Если $V = \{x, y\}$, то удаление вершины x делает граф одновершинным $v(G) = 1 = \varepsilon(G)$.

Если $|V| > 2$ в $G \setminus e \llbracket x \rrbracket > 1$ или $\llbracket y \rrbracket > 1$.

удалим x , если $\llbracket x \rrbracket > 1$
удалим y , если $\llbracket y \rrbracket > 1$ $\Rightarrow v(G) = 1 = \varepsilon(G)$.

Случай 2 состоит в том, что в графе G нет моста $\Rightarrow \varepsilon(G) = k > 1$.

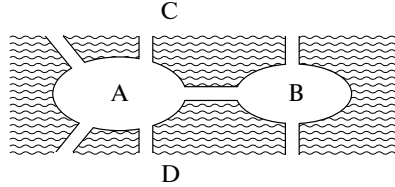


Пусть $\{x_1, y_1\}, \{x_2, y_2\}, \dots, \{x_k, y_k\}$ — множество рёбер, удаление которого делает граф несвязным. $\forall i \in \{1 \dots k-1\}$ удалим из множества $\{x_i, y_i\}$ одну вершину, не принадлежащую $\{x_k, y_k\}$. Получим либо несвязный граф, либо связный граф с мостом $\{x_k, y_k\}$. Удаление одной вершины делает его несвязным или одновершинным.

$$v(G) \leq k = \varepsilon(G).$$

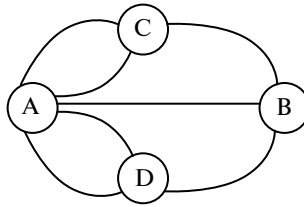
Эйлеровы пути

Задача о Кёнигсбергских мостах:



Можно ли так прогуляться по городу, чтобы пройти по каждому мосту ровно 1 раз?

Пройти = перейти с берега на берег. Поставим в соответствие изображенной выше карте граф, вершины которого — участки суши, а ребрами будут мосты. Полученный таким образом граф является мультиграфом:



Существует ли маршрут для прогулки, который проходит — содержит, по каждому мосту ровно 1 раз? (эквивалентно: существует ли в графе цепь, проходящая через все ребра?)

Данная задача сводится к задаче нарисовать мультиграф одним росчерком.

Эйлерова цепь — это цепь, содержащая все ребра графа.

Эйлеров цикл (ЭЦ) — это есть цикл, содержащий все ребра графа.

Теорема (Эйлера)

Дан граф G без изолированных вершин. Тогда в графе G есть ЭЦ \Leftrightarrow

- 1) G — связный,
- 2) $\forall v \in V \deg v$ — четная.

Доказательство

$\Rightarrow u, v \in V$ есть (u, v) — маршрут по ЭЦ ((1) выполняется).

Пойдем по ЭЦ, $\forall v \in V$ входим в вершину v столько раз, сколько выходим. $\Rightarrow \deg v$ будет четной.

$\Leftarrow v_0 \in V$, пойдём из вершины v_0 , стирая за собой рёбра. Допустим, что пришли в $v \neq v_0$. Зашли в v на 1 раз больше, чем вышли из $v_0 \Rightarrow$ стерли нечётное число инцидентных вершине v рёбер \Rightarrow остались нестертые инцидентные v рёбра.

То есть, если процесс блуждания остановился, то мы в v_0 (и стерли все инцидентные v_0 рёбра). Итак, пройден некоторый цикл P_0 . Если все рёбра стерты, то цикл P_0 эйлеров. Пусть остались нестертые рёбра. Покажем, что на цикле P_0 есть вершина v_1 , у которой остались нестертые инцидентные рёбра. Воспользуемся методом от противного: пусть остались лишь рёбра, соединяющие вершины вне $P_0 \Rightarrow$ рёбер между вершинами P_0 и вершинами с нестертыми рёбрами вообще не было (мы их не стирали). Это противоречит связности.

Замечание

Заметим, что после стирания P_0 , у всех вершин по-прежнему чётная степень (стёрли чётное число рёбер у каждой вершины).

Пойдём из вершины v_1 , стирая за собой рёбра, аналогично 1-му абзацу построим цикл C_1 .

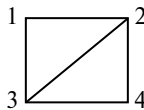
Пусть $P_1 = v_0 \xrightarrow{P_0(\text{начало})} v_1 \xrightarrow{C_1} v_1 \xrightarrow{P_0(\text{конец})} v_0$ — цикл.

Итак, получен новый цикл из вершины v_0 длиной $>$ длины P_0 .

Значит, получили процесс увеличения длины цикла, обрывающийся тогда и только тогда, когда цикл будет Эйлеров. Это и есть процесс построения ЭЦ.

Набор цепей покрывает граф, если каждое ребро графа — это ребро какой-то цепи из набора.

Набор цепей рёбер не пересекается, если у цепей нет общих рёбер.



$\{1,2,3,4, 3241\}$ — набор, покрывающий граф.

$\{123,241\}$ — реберно-непересекающийся набор.

$\{12,23,34,24,14\}$ — реберно-непересекающийся набор, покрывающий граф.

$\{214\,324\}$ — реберно-непересекающийся набор, покрывающий граф.

Замечание

Эйлерова цепь в одиночку образует реберно-непересекающийся набор, покрывающий граф.

Следствие из Теоремы Эйлера

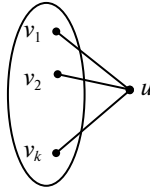
Граф G — связный с k вершинами нечетной степени. Тогда в минимальном (по числу цепей) реберно-непересекающемся наборе, покрывающем граф, будет $k/2$ цепей.

Доказательство

По Лемме о рукопожатиях k — четно.

Пусть граф покрыт l реберно-непересекающимися цепями.

Рассмотрим вершину нечетной степени. Если концы некоторой цепи не лежат в v , то цепь покрывает четное число инцидентных v ребер. Значит, найдется конец цепи, лежащий в вершине v . Количество концов цепей \geq количеству вершин нечетной степени, то есть $2l \geq k \Rightarrow l \geq k/2$: $k/2$ цепей всегда достаточно.



v_1, v_2, \dots, v_k — вершины нечетной степени.

u — новая вершина, соединим u с v_i ($i \in \{1 \dots k\}$) и получим связный граф с четными степенями вершин, по теореме Эйлера в нем есть ЭЦ.

Удалим все вхождения u и все ребра с u , цикл развалится на $k/2$ частей — цепей, они реберно-непересекающиеся (по определению цикла) и покрывают граф (по определению ЭЦ и по построению графа).

Теорема об оценке числа ребер

$G = (V, E)$ — граф, $|V| = n$, $|E| = m$, k — компонента.

Тогда $n - k \leq m \leq C_{n-k+1}^2 = \frac{(n-k+1)(n-k)}{2}$.

Доказательство

1) Проведем индукцию по числу ребер:

База индукции:

$m = 0 \Rightarrow$ каждая вершина — компонента $\Rightarrow k = n \Rightarrow n - k = 0 \leq m$.

Шаг индукции:

$m > 0$ для всех графов, в которых $< m$ ребер, неравенство $n - k \leq m$ выполняется.

$e \in E$, либо e — мост $\xrightarrow{\text{Лемма о мосте}} k(G \setminus e) = k(G) + 1$,

либо e — не мост $\xrightarrow{\text{Определение моста и замечание}} k(G \setminus e) = k(G)$.

Тогда

$$m(G \setminus e) = m(G) - 1,$$

$$n(G \setminus e) = n(G).$$

По предположению индукции $n(G \setminus e) - k(G \setminus e) \leq m(G \setminus e)$,

$$n(G) - \begin{bmatrix} k(G) + 1 \\ k(G) \end{bmatrix} \leq m(G) - 1,$$

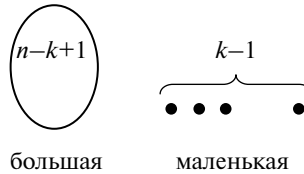
$$n(G) - (k(G) + 1) \leq m(G) - 1,$$

$$n(G) - k(G) \leq m(G) - 1 \leq m(G).$$

2) Рассмотрим экстремальный пример, то есть граф с n вершинами, k компонентами и наибольшим (для этих n и k) числом ребер.

Покажем, что в экстремальном примере не может быть больше двух компонент. Воспользуемся методом от противного. Пусть есть две компоненты: k_1 и k_2 , $|k_1| = p$, $|k_2| = q$, $p \geq q > 1$, v — вершина k_2 . Удалим все ребра, инцидентные v , соединим v ребрами со всеми вершинами k_1 . В полученном графе столько же вершин и столько же компонент, что и в исходном. Число ребер увеличилось не менее чем на величину $p = q + 1 > 0$.

Получили противоречие с экстремальностью исходного графа. То есть, экстремальный пример имеет вид



$$m \leq C_{n-k+1}^2.$$

Деревья

Дерево — связный граф без циклов.

Лес — граф без циклов.

Теорема (об эквивалентных определениях дерева)

Для графа G эквивалентны следующие условия:

- 1) граф G — дерево.
- 2) G — связный и $m(G) = n(G) - 1$.
- 3) G — без циклов и $m(G) = n(G) - 1$.
- 4) $\forall u, v \in V \exists!$ простая (u, v) — цепь.
- 5) G без циклов, $\forall u, v \in V, \{u, v\} \notin E$ $G + \{u, v\}$ содержит ровно 1 цикл.

Доказательство

1) \rightarrow 2) индукция по числу ребер.

База индукции:

$$m(G) = 0 + G \text{ связный} \Rightarrow n(G) = 1.$$

Шаг индукции:

$m(G) > 0$ (для всех деревьев с меньшим числом ребер уже доказано).

$$e \in E \xrightarrow[\text{определение дерева}]{\text{Лемма о мосте}} e \text{ — мост} \xrightarrow{\text{Лемма о мосте}} k(G \setminus e) = k(G) + 1 = 2.$$

Пусть T_1 и T_2 — компоненты $G \setminus e$, они деревья и $m(T_1) + m(T_2) = m(G) - 1$,

то есть $m(T_1) < m(G)$ и $m(T_2) < m(G)$.

По определению индукции:

$$m(T_1) = n(T_1) - 1, \quad \frac{m(T_2) = n(T_2) - 1}{m(G_1) - 1 = n(G) - 2}, \quad m(G) = n(G) - 1.$$

2) \rightarrow 3) Воспользуемся методом от противного:

В графе G есть цикл C , пусть e ребро цикла G . Следовательно, e — не мост.

$$k(G \setminus e) = k(G) = 1,$$

$$n(G \setminus e) = n(G),$$

$$m(G \setminus e) = m(G) - 1,$$

$$m(G \setminus e) = m(G) - 1 = n(G) - 2 = n(G \setminus e) - k(G \setminus e) - 1 < n(G \setminus e) - k(G \setminus e).$$

Это противоречит теореме об оценке числа ребер.

3) \rightarrow 4) Докажем, что граф G связный.

Сначала докажем существование.

Пусть T_1, T_2, \dots, T_k его компоненты — деревья (так как 1) \rightarrow 2) уже доказано). Тогда

$$m(T_1) = n(T_1) - 1$$

+

$$m(T_2) = n(T_2) - 1$$

+

...

+

$$\frac{m(T_k) = n(T_k) - 1}{n(G) - 1 = m(G) = n(G) - k} \Rightarrow k = 1.$$

Граф G будет связным, то есть $\forall u, v \in V (u, v)$ — маршрут. По утверждению 1-му про маршруты из него можно выделить простую (u, v) -цепь.

Теперь докажем единственность.

Воспользуемся методом от противного: есть 2 разные (u, v) -цепи. По утверждению 3-му про маршруты их объединение содержит цикл (противоречие).

4) \rightarrow 5) граф G без циклов? Простой цикл образует две разные цепи:

$G + \{u, v\}$ содержит цикл, $\{u, v\} + (u, v)$ — цепь.

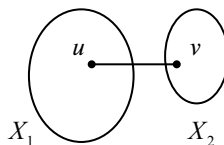
Снова применим метод от противного:

C и D — разные циклы в $G + \{u, v\}$.

$\{u, v\}$ содержатся в C и D .

По утверждению 4-му про маршруты $C \cup D \setminus \{u, v\}$ содержит цикл (противоречие).

5) \rightarrow 1) Докажем связность методом от противного.



$$u \in X_1, v \in X_2.$$

$G + \{u, v\}$ содержит цикл с ребром $\{u, v\}$ (так как G без циклов).

Но удаление $\{u, v\}$ разделяет компоненты, то есть $\{u, v\}$ — мост в графе $G + \{u, v\} \xrightarrow{\text{Лемма о мосте}} \{u, v\}$, который не лежит ни в каком цикле (противоречие).

Если в дереве $n > 1$, то в нем $\forall v \deg v > 0$.

Лист — вершина степени 1 в дереве.

Следствие 1

В каждом дереве (при $n > 1$) не менее двух листьев.

Доказательство

Пусть l листьев $\Rightarrow n - l$ имеют степень ≥ 2 .

$$2(n-1) = 2m = \sum_{v \in V} \deg v = \sum_{v-\text{лист}} \deg v + \sum_{v-\text{не лист}} \deg v \geq l + 2(n-l) = 2n-l, l \geq 2.$$

Остовной подграф графа $G = (V, E)$ — это есть граф $H = (V, F)$, $F \subseteq E$, $k(H) = k(G)$.

Остов (каркас) графа G — есть остовной подграф с минимальным числом ребер.

Замечание

Каждая компонента остова — дерево. Иначе, удалив ребро в цикле, уменьшим число ребер, не изменив числа компонент.

Обратно: Если в остовном подграфе каждая компонента — дерево, то удаление любого ребра увеличивает число компонент связности, то есть то, что остается, — уже не остовной подграф.

Следствие 2

Остовной подграф, у которого каждая компонента — дерево, является остовом.

Доказательство

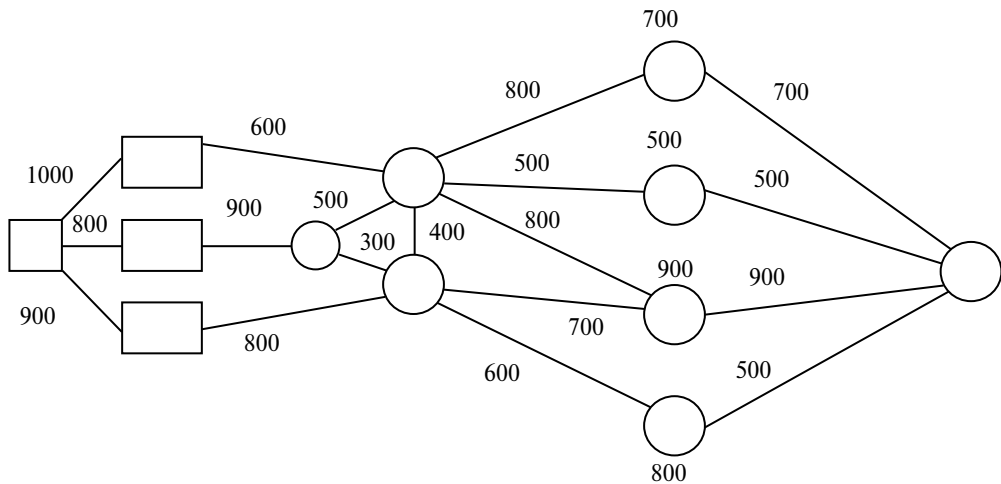
Оценим число ребер в остовном подграфе снизу (по Теореме об оценке) оно $\geq n - k$.

Если в остовном подграфе каждая компонента — дерево, то в ней ребер на 1 меньше, чем вершин, то есть во всем графе ребер $n - k$, по определению — это остов. Для получения остова из цикла нужно удалить $m - n + k$ ребер.

Циклический ранг графа — это сумма

$$\gamma(G) = m(G) + k(G).$$

Потоки в сетях



(G, S, t, c) — сеть, если $G = (V, E)$ — орграф $S, t \in V$, где S — источник, t — сток.

$c: E \rightarrow R^+$ — функция пропускной способности.

(G, S, t, ω) — сеть S' . Поток f в сети S — это есть функция $f: E \rightarrow R^+ \cup \{0\}$

такая, что выполняются условия:

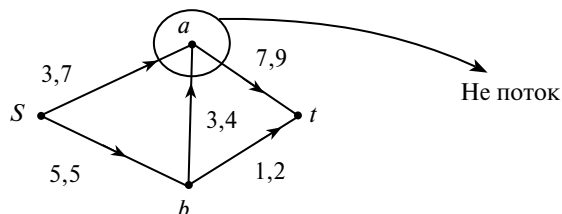
П1: $\forall e \in E \quad f(e) \leq c(e)$,

П2: $\forall u \in V$.

$$\sum_{\substack{v \in V \\ (u,v) \in E}} f(u,v) - \sum_{\substack{v \in V \\ (v,u) \in E}} f(v,u) = \begin{cases} 0, & u \neq s, t \\ p \geq 0, & u = s \\ -p, & u = t \end{cases}$$

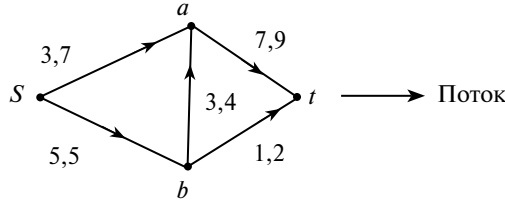
Такую функцию называют потоком. Он вытекает из вершины s и втекает в вершину t .

Пример



Договоримся записывать поток на ребре и его пропускную способность через запятую, рядом с соответствующей этому ребру стрелкой.

В примере первые цифры не задают поток.



$p = p(f)$ — величина потока, сам поток — это функция.

Сокращение записи:

$$A, B \subseteq V,$$

$$h: E \rightarrow R^+ \cup \{0\},$$

$$(A, B) = \{(x, y) \mid x \in A, y \in B, (x, y) \in E\},$$

$$h(A, B) = \sum_{(x, y) \in (A, B)} h(x, y),$$

$$(\{s, a\}, \{b, t\}) = \{(a, t), (s, b)\},$$

$$(\{s, a, b\}, \{a, b, t\}) = E,$$

$$c(\{s, a\}, \{b, t\}) = 14,$$

$$f(\{s, a\}, \{b, t\}) = 12.$$

П2 представляется как

$$f(\{u\}, v) - f(v, \{u\}) = \begin{cases} 0, & u \neq s, t \\ p, & u = s \\ -p, & u = t \end{cases}$$

Разрез в сети — это (X, \bar{X}) , где $X \subseteq V$, $\bar{X} = V \setminus X$.

Лемма о разрезе

(G, S, t, c) — сеть.

Тогда $\forall x \subseteq V$ $s \in x$, $t \notin x$ $\forall f$ (f — поток) $P(f) = f(x, \bar{x}) - f(\bar{x}, x) \leq c(x, \bar{x})$.

Доказательство. 1) $f(x, V) - f(V, x) = \sum_{x \in x} f(\{x\}, V) - f(V, \{x\}) = P(f)$,

$$f(x, V) - f(V, x) = f(x, x) + f(x, \bar{x}) - f(x, x) - f(\bar{x}, x) = f(x, \bar{x}) - f(\bar{x}, x).$$

2) Из П1 $\Rightarrow f(x, \bar{x}) \leq c(x, \bar{x})$ по определению потока

$$f: E \rightarrow \mathbb{R}^+ \cup \{0\} \quad \forall e \in E \quad f(e) \geq 0, \quad f(\bar{x}, x) \geq 0, \quad -f(\bar{x}, x) \leq 0.$$

Теорема (Форда–Фалкерсона)

$$\max P(f) = \min c(x, \bar{x}), \quad f \text{ — поток, } x \subseteq V, S \in x, t \notin x.$$

Доказательство

$$\max f \leq \min c(x, \bar{x}) \quad (\text{по лемме о разрезе}).$$

Докажем достижимость: возьмем максимальный поток f (то есть поток с наибольшим значением P). Построим x по правилам:

1) $S \in x$.

2) $u \in x \quad f(u, v) < c(u, v) \Rightarrow v \in x$.

3) $u \in x \quad f(v, u) > 0 \Rightarrow v \in x$.

Заметим, что $t \notin x$.

Будем рассуждать «от противного». Если $t \in x$, то от S до t есть путь, построенный по правилам 1 и 2: $S = v_0, v_1, \dots, v_k = t$.

Правило 1:

$$\begin{array}{c} v_i \quad \xrightarrow{\quad} \quad v_{i+1} \\ \bullet \quad \xrightarrow{\quad} \quad \bullet \end{array} \Rightarrow f(v_i, v_{i+1}) < c(v_i, v_{i+1}).$$

Попутное ребро

Правило 2:

$$\begin{array}{c} v_i \quad \xleftarrow{\quad} \quad v_{i+1} \\ \bullet \quad \xleftarrow{\quad} \quad \bullet \end{array} \quad f(v_i, v_{i+1}) > 0.$$

Встречное ребро

$$\varepsilon_1 = \min(c(e) - f(e)) > 0, \quad e \text{ — попутное.}$$

$$\varepsilon_2 = \min f(e) > 0, \quad e \text{ — встречное.}$$

$$\varepsilon = \min\{\varepsilon_1, \varepsilon_2\}.$$

$$f'(e) = \begin{cases} f(e) + \varepsilon, & e \text{ — попутное} \rightarrow \forall e \in E \quad f'(e) \leq c(e), \\ f(e) - \varepsilon, & e \text{ — встречное} \rightarrow f': E \rightarrow \mathbb{R}^+ \cup \{0\}, \\ f(e), & e \text{ не входит в найденный } (s, t)\text{-маршрут.} \end{cases}$$

(s, t) -путь, построенный по правилам 1 и 2, — это есть увеличивающий путь, а ε — увеличивающее значение.

Замечание 1

Если в сети с потоком есть увеличивающий путь, то поток можно увеличить.

Замечание 2

Если в сети с потоком нет увеличивающего пути, то поток \max (по Теореме Форда-Фалкерсона).

Доказательство

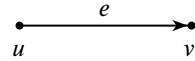
Увеличивающего пути нет \Rightarrow по правилам 1, 2, 3 построим $x, S \in x, t \notin x$ и $P(f) = c(x, \bar{x}) \geq \min \{c(x, \bar{x}) \mid x \subseteq V, S \in x, t \notin x\}$.

Значит, $P(f) = \max \{P(f) \mid f - \text{поток}\}, f - \text{максимальный поток}$.

Алгоритм поиска максимального потока

1. Берем какой-нибудь поток (например $\forall e f(e) = 0$).
2. Ищем увеличивающий путь. Если нашли, то увеличиваем вдоль него поток на ϵ (увеличив значение); переход на 2. Иначе стоп, поток максимальный.

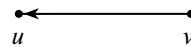
Алгоритм поиска кратчайшего увеличивающего пути



если $f(e) = 0$, то путь попутный — да, встречный — нет;



если $f(e) = c(e)$, то путь попутный — нет, встречный — да;



если $0 < f(e) < c(e)$, то путь может быть и попутным и встречным.



Замечание

В полученном ориентированном графе есть ориентированный (s, t) -путь \Leftrightarrow в исходной сети с истоком есть увеличивающий путь.

Расстояние в графах

Расстояние между вершинами u и v во взвешенном графе $G((G, \omega))$ — это есть длина кратчайшей (u, v) -цепи. Обозначение: $\rho(u, v)$.

Замечание 1

ρ — метрика на V , т. е.

- 1) $\rho(u, u) = 0$,
- 2) $\rho(u, v) = \rho(v, u)$ — функция симметрична относительно аргументов,
- 3) $\rho(u, v) + \rho(v, w) \geq \rho(u, w)$.

Доказательство. Некоторая цепь \geq кратчайшая цепь.

Замечание 2

Расстояние не во взвешенном графе G — это расстояние во взвешенном графе (G, ω) , где $\forall e \in E \quad \omega(e) = 1$.

Алгоритм Дейкстры.

Вход: $G = (V, E)$, $\omega: E \rightarrow R^+$, $u \in V$.

Выход: $\forall v \in V, \rho(u, v)$.

Требуется две функции: $d: V \rightarrow R^+$ (функция текущего расстояния)

и $e: V \rightarrow V$ (частичная функция текущего предшественника).

$S \subseteq V$ (список найденных, но не обработанных вершин).

$v \rightarrow S$ (вершину v поместить в список S).

$v \leftarrow S$ (из S вынимается вершина с наименьшим значением d и помещается в переменную v).

0) $\forall v \in V \quad d(v) = +\infty, d(u) = 0, e(v) = NULL, u \rightarrow S$;

1) Если $S = \emptyset$, то *стоп*;

2) $v \leftarrow S$;

3) $\forall x \in V \quad x$ — смежна с вершиной v .

если $d(x) > d(v) + \omega(v, x)$,

то $d(x) = d(v) + \omega(v, x)$.

$e(x) = v, x \rightarrow S$.

4) Переход на п. 1).

Пусть $M = \min d(v) \mid v \in S$.

Замечание 1

M не убывает (пока $S \neq \emptyset$).

Доказательство

Очевидно, следует из п. 3) алгоритма.

Замечание 2

$v \rightarrow S \Rightarrow d(v) \rightarrow M$.

Замечание 3

$\forall v \ d(v)$ — не возрастает.

Замечание 4

Если вершина v удалена из списка S , то v не попадает больше в список.

Доказательство

Очевидно, следует из описания алгоритма.

Лемма 1

Каждая вершина удаляется только один раз. Граф G — связный, шаг 2 (алгоритма) срабатывает ровно $m(G)$ раз.

Доказательство

Из замечаний 1, 2, 3, 4 следует, что шаг 2 срабатывает $\sum m(G)$ раз $\forall v \neq u$.

Вначале $d(v) = \infty$, значит, просмотрев какой-нибудь маршрут (u, v) , мы поместим v в список S . В силу шага 1 вершина будет удалена.

Замечание 5

Если $d(v) < \infty$, то $d(v)$ — это длина некоторого (v, u) маршрута (а именно, $v, e(v), e^2(v), \dots, u$).

Доказательство

Воспользуемся методом от противного. Допустим это не так. Найдем первое выполнение шага 3, когда это нарушается, то есть $d(x)$ — не длина никакого (x, v) — маршрута. Но $d(v)$ — это длина маршрута $v, e(v), e^2(v), \dots, u$ $d(x) = d(v) + \omega(v, x)$ и это длина $(v, e(v), e^2(v), \dots, u) = x, e(x), e^2(x), \dots, u$ (противоречие).

Замечание 6

$\forall v$ в любой момент выполнение алгоритма $d(v) \geq \rho(u, v)$.

Лемма 2. В конце работы алгоритма $\forall v \in V \quad d(v) = \rho(u, v)$.

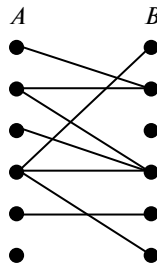
Доказательство. Воспользуемся методом доказательства от противного. Пусть существует такая вершина $v \in V$, что в конце работы алгоритма для этой вершины $d(v) > \rho(u, v)$ (замечание 6). Пусть v — самая близкая к вершине u вершина с таким свойством. Рассмотрим кратчайший (u, v) -маршрут u, \dots, y, v $d(y) = \rho(u, y) < \rho(u, v)$. Рассмотрим шаг, на котором вершина y вынута из списка и просматриваются её соседи. В этот момент уже в силу замечаний 1, 2, 3, 4 $d(y) = \rho(u, y)$. Вершина v — сосед y , в этот момент $d(v) > \rho(u, v) = \rho(u, y) + \omega(y, v) = d(y) + \omega(y, v)$ (в силу Замечания 3), то есть выполняется равенство $d(v) = d(y) + \omega(y, v) = \rho(u, v)$. Получили противоречие.

Леммы 1, 2 дают теорему о корректности алгоритма Дейкстры.

Двудольные графы

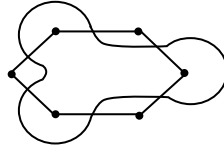
Пример

$$A \cap B = \emptyset, \rho \subseteq A \times B.$$

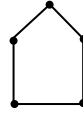


Граф $G=(V, E)$ двудольный, если $\exists A, B \subseteq V \quad A \cup B = V, A \cap B = \emptyset \forall \{u, v\} \in E \quad u \in A, v \in B$ (или наоборот), A, B — доли графа.

Пример



Двудольный



Не двудольный

Теорема Кенига (критерий двудольности)

Граф G — двудольный \Leftrightarrow в G нет циклов нечетной длины.

Доказательство

\Rightarrow Берем ЛЮБОЙ цикл:

$$v_0 v_1 v_2 v_3 \dots v_{n-1} v_n = v_0,$$

$$A B A B \dots A = A.$$

Части A, B , на которые делится двудольный граф, называются долями.

Доля A , где $v_0 \forall k \in N \cup \{0\}, v_{2k} \in A, v_{2k+1} \in B$, значит, число n — четное.

\Leftarrow Заметим, что если каждая компонента двудольная, то и весь граф двудольный. Очевидно, достаточно доказать \Leftarrow только для связного графа. Выберем вершину $u \in V$ так, что выполняется следующее:

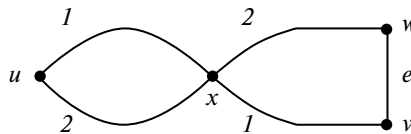
$$A = \{v \in V (\rho(u, v) - \text{четно})\} \quad B = \{v \in V (\rho(u, v) - \text{нечетно})\}.$$

Очевидно: $A \cup B = V$ (G — связный), $A \cap B = \emptyset$.

Покажем, что НЕТ ребер внутри частей.

Воспользуемся методом от противного. Вершины w, v лежат в одной части: $e = \{w, v\} \in E, \rho(u, v) \equiv \rho(u, w) \pmod{2}$.

Найдем кратчайшие маршруты:



x — последняя вершина на первом маршруте из тех, которые лежат и на втором маршруте, а это значит, что на первом пути нет вершин второго маршрута. Второй маршрут простой, так как кратчайший $\Rightarrow x \xrightarrow{1} v \xrightarrow{e} w \xrightarrow{2} x$ — простой цикл. Если $x = v$ и $w \xrightarrow{2} x$ — это снова ребро e , то v — предпоследняя вершина кратчайшего (u, w) -маршрута $\Rightarrow \rho(u, v) + 1 = \rho(u, w)$. А это противо-

речие. То есть цикл всегда есть. Заметим, что длины u, x частей первого и второго маршрутов одинаковы (иначе можно сократить какой-то кратчайший маршрут) и равны $\rho(u, x)$.

Длина найденного цикла равна

$$\begin{aligned} \rho(u, w) - \rho(u, x) + \rho(u, v) - \rho(u, x) + 1 = \\ = \rho(u, w) + \rho(u, v) - 2\rho(u, x) + 1. \end{aligned}$$

Она будет нечетной (противоречие).

Алгоритм проверки двудольности связного графа

- 1) Выберем $u \in V$.
- 2) Измерим $\rho(u, v) \quad \forall v \in V$.

Проверим, если есть $v, w \in V, \rho(u, v) = \rho(u, w)$ и $\{v, w\} \in E$, то граф не двудольный, иначе, граф — двудольный.

Замечание

Шаг 2 можно делать в ходе выполнения шага 1. Проверим корректность шага 2.

Если ..., то ... \Rightarrow находим цикл нечетной длины \Rightarrow так как граф не двудольный.

Иначе $\Rightarrow A$ и B из доказательства.

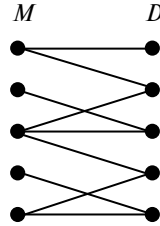
Действительно, v, w в одной части и соединены ребром

$$e \Rightarrow (\rho(u, v) - \rho(u, w)) = \begin{cases} 0, \\ 1. \end{cases}$$

(из неравенства треугольника).

Но это не равно 0, и это равно 1, так как $\rho(u, v) \equiv \rho(u, w) \pmod{2}$ (противоречие).

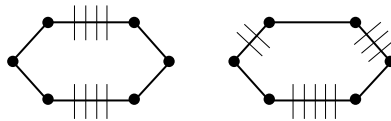
Паросочетание



Паросочетание — множество попарно непересекающихся ребер.

Максимальное паросочетание есть паросочетание, не лежащее ни в каком другом паросочетании.

Пример



Оба паросочетания максимальные.

Наибольшее паросочетание есть паросочетание с наибольшим числом ребер.

Замечание 1

Пусть $\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases} \Rightarrow$ для любого увеличивающего пути $\varepsilon = 1$.

Доказательство

$S \bullet \rightarrow \bullet \leftarrow \bullet \rightarrow \bullet \rightarrow \bullet \leftarrow \bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet t$

На попутных $f < c \Rightarrow f = 0$.

На встречных $f > 0 \Rightarrow f = 1$.

$\varepsilon = \min \{ \min c(e) = f(e) (e - \text{попутное}), \min f(e) (e - \text{встречное}) \} = 1$.

Замечание 2

Пусть $\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases} \Rightarrow$ после изменения потока вдоль ПУТИ

$\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases}$.

Утверждение

При работе алгоритма поиска максимального потока будет найден поток со свойством $\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases}$.

Замечание 3

Пусть в алгоритме есть поток со свойством $\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases} \Rightarrow$ величины p . Тогда множество $\{\{u, v\} / u \in A, v \in B, f(u, v) = 1\}$ — паросочетание мощности p .

Доказательство

В каждую вершину A не может втекать больше 1. Из каждой вершины B не может вытекать больше 1. Величина потока через разрез $(\{S\} \cup A, B \cup \{t\})$ равна числу ребер, на которых они не равны 1.

Замечание 4

Если в двудольном графе есть паросочетания мощности m , тогда в соответствии ему есть поток величины m со свойством $\forall e \in E \quad f(e) = \begin{cases} 0 \\ 1 \end{cases}$.

Доказательство

Определим нужный поток:

$$\forall \{u, v\} \in M \quad (u \in A, v \in B), \quad f(s, u) = f(u, v) = f(w, t) = 1, \quad P(f) = m.$$

Теорема (о корректности алгоритма)

Множество ребер двудольного графа, на которых найденный алгоритм максимального потока не равен 0, если наибольшее паросочетание.

Доказательство

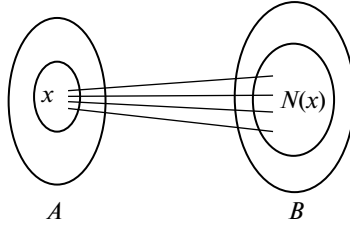
Очевидно, следует из утверждения и замечаний 3 и 4.

Теорема Холла (о трансверсальных). В двудольном графе $G = (A \cup B, E)$ есть паросочетания мощности $|A|$ тогда и только тогда, когда $\forall x \subseteq A \quad |N(x)| \geq |x|$.

$|N(x)|$ — окружение x , то есть $\{v \in V \mid \exists u \in x \quad \{u, v\} \in E\}$.

Замечание

В двудольном графе $x \subseteq A \Rightarrow N(x) \subseteq B$.



Доказательство

\Rightarrow Воспользуемся методом от противного. Пусть $\exists x \subseteq A$, $|N(x)| < |x| \Rightarrow$ любое парасочетание не использует какую-то вершину из x , а значит, и из A .

\Leftarrow Проведем индукцию по длине $|A|$.

База индукции: $|A| = 1$, $|N(A)| \geq |A| = 1$, то есть ребро с началом в A . Это парасочетание мощности $1 = |A|$.

Шаг индукции: $|A| = m$. Предположим, что для всех двудольных графов, у которых доля A состоит из $< m$ вершин, утверждение доказано.

1-й случай:

$\forall x \subseteq A \quad |N(x)| > |x| \quad a \in A, b \in B \quad e = \{a, b\} \in E$. Строим G' : $A' = A \setminus a$,

$$B' = B \setminus b, \quad \forall x' \subseteq A' \subseteq A, \quad N_{G'}(x') = \begin{cases} N_G(x'), \\ N_G(x') \setminus b, \end{cases}$$

$$|N_{G'}(x')| = \begin{cases} |N_G(x')| \\ |N_G(x')| - 1 \end{cases} \geq |x'|.$$

По предположению индукции в графе G' есть парасочетания мощности $|A'| = m - 1$. Вместе с ребром e получим в G парасочетания мощности $m = |A|$.

2-й случай:

$$\exists A_0 \subseteq A, \quad |N(A_0)| = |A_0|.$$

$$G' = G(A_0 \cup N(A_0)).$$

$$G'' = G(\bar{A}_0 \cup \overline{N(A_0)}).$$

$\forall x \subseteq A_0, N_G(x) = N_{G'}(x) \Rightarrow |x| \leq |N_{G'}(x)|$ по положению индукции в графе G' есть парасочетания мощности (A_0) , $\forall x \subseteq \bar{A}_0$.

$$\begin{aligned} |A_0| + |x| = |A_0 \cup x| \leq |N_G(A_0 \cup x)| = |N_G(A_0) \cup N_{G'}(x)| = |N_{G'}(A_0)| + \\ + |N_{G'}(x)| \Rightarrow |x| \leq |N_{G'}(x)|. \end{aligned}$$

По предположению индукции в графе G'' есть паросочетания мощности $|A_0|$. Объединение двух найденных паросочетаний есть паросочетание мощности $|N|$ в графе G .

Следствие

В G есть паросочетания мощности $t \Leftrightarrow \forall x \subseteq A, t \leq |A| + |N(x)| - |x|$.

Доказательство

Добавим в долю B еще $|A| - t$ новых вершин, соединив каждую добавленную вершину с каждой вершиной доли A . Получим граф G' . В G есть паросочетания мощности $t \Leftrightarrow$ (очевидно) в графе G' есть паросочетание мощности $|A|$.

Возьмем в G паросочетания мощности t . В нем не задействованы $|A| - t$ вершин доли A . Соединим каждую из этих незадействованных вершин со своей добавленной вершиной.

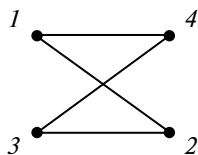
Возьмем в G' паросочетания мощности $|A|$. Удалим из правой доли добавленные вершины (их $|A| - t$). Вместе с ними удалены $\leq |A| - t$ ребер паросочетаний. Осталось паросочетание в G мощности $\geq t$.

$$\forall x \subseteq A, |x| \leq |N_{G'}(x)| = |A| - t + |N_G(x)|.$$

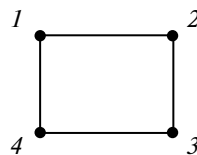
Плоские и планарные графы

Планарный граф G — это граф, который изображен на плоскости без пересечения ребер.

Пример



Не плоский планарный



Плоский планарный

Граф G — планарный граф, если он изоморфен плоскому графу, или G можно изобразить на плоскости без пересечения ребер.

Замечание 1

Любой граф можно уложить в \mathbb{R}^3 из пересечения ребер. Рассмотрим пучок из $|E|$ плоскостей, расположим \forall на прямой пересечения пучка. Каждое ребро — полуокружность в своей плоскости.

Замечание 2

Граф можно уложить на сфере без пересечения ребер $\Leftrightarrow G$ — планарный.

Доказательство

Отрезок AB есть диаметр. Точка B есть единственная точка пересечения сферы и плоскости.

Строим проекцию Π на сферу относительно точки A , которую можно взаимно однозначно спроектировать на плоскость.

Замечание 3

Выпуклый многогранник — это плоский граф.

Грань плоского графа — это есть часть плоскости, ограниченная ребрами.

6. Автоматы и языки

Языки

Σ — алфавит (конечный) — множество букв.

Σ^+ — множество всех слов.

$\langle \Sigma^+, \cdot \rangle$ — свободная полугруппа.

λ — пустое слово.

$\Sigma^+ \cup \{\lambda\} = \Sigma^*$.

$\langle \Sigma^*, \cdot \rangle$ — свободный моноид.

«Свободный»: $\forall M$ — моноид $\forall \varphi: \Sigma \rightarrow M \exists! \hat{\varphi}: \Sigma^* \rightarrow M$ (гомоморфизм):

$\hat{\varphi}(\lambda) = 1, \forall a \in \Sigma \hat{\varphi}(a) = \varphi(a)$.

Языком называется подмножество свободного моноида.

Примеры

1. Русский язык.
2. Язык программирования.
3. Геном человека — язык, $\Sigma = \{A, C, T, G\}$.
4. Организм — язык, алфавит — множество аминокислот.
5. Множество простых чисел ($\Sigma = \{1\}$).

Операции с языками

1° Теоретико-множественные операции:

$\cup, \cap, -, \setminus$

$(L \subseteq \Sigma^* \Rightarrow \bar{L} = \Sigma^* \setminus L)$

2° Произведение языков:

$L, K \subseteq \Sigma^* \Rightarrow L \cdot K = \{uv \mid u \in L, v \in K\}$.

Пример

$K = \{a^{2n} \mid n \in N\}$.

$$K = \{a^{7^n} \mid n \in N\}.$$

$$L \cdot K = \{a^9, a^{11}, a^{13}, a^{15}, a^{16}, a^{17}, a^{18} \dots\} = \{a^9, a^{11}, a^{13}\} \cup \{a^n \mid n \geq 19\}.$$

3° Левое (правое) частное:

$$K^{-1}L = \{v \mid \exists u \in K : uv \in L\},$$

$$LK^{-1} = \{v \mid \exists u \in K : vu \in L\}.$$

Пример

$$L = \{ab, ba, ab^2\},$$

$$K = \{a, a^2, b\},$$

$$K^{-1}L = \{b, a, b^2\}.$$

Упрощенные обозначения:

$$\{u\} \rightarrow u.$$

$$\{v \mid uv \in L\} = u^{-1}L.$$

$$L \cup K = K + L.$$

$$(a + ab)ba(a + b) = \{aba^2, abab, ab^2a^2, ab^2ab\}.$$

4° Итерация языка:

$$L \subseteq \Sigma^* \Rightarrow L^* = \{\lambda\} \cup L^1 \cup L^2 \cup L^3 \cup \dots = \bigcup_{n=0}^{\infty} L^n (L^0 = \{\lambda\}).$$

Примеры

$$L = \{a^5, a^8\}.$$

$$L^* = \{\lambda, a^5, a^8, a^{10}, a^{13}, a^{15}, a^{16}, a^{18}, a^{20}, a^{21}, a^{23}, a^{24}, a^{25}, a^{26}, a^{28} \dots\}.$$

$$\Sigma = \{a, b\}.$$

$(a + b)^*ab(a + b)^*$ — множество всех слов, содержащих ab в качестве подмножества.

u — префикс ω , если $\omega = u \cdot v$;

u — суффикс ω , если $\omega = v \cdot u$;

u — фактор (подслово), если $\omega = v \cdot u$.

Рациональным выражением называется выражение из букв и λ с применением операций $+$, \cdot , $*$.

Автоматы. Распознаватели

Машина получает воздействие (символы конечного алфавита), меняет-ся ее состояние.

Детерминированным конечным автоматом (ДКА) называется тройка: $A = (Q, \Sigma, \delta)$, где Σ — конечный алфавит, Q — множество состояний (конечное), $\delta: Q \times \Sigma \rightarrow Q$ — функция переходов.

При этом если $\delta(q_1, a) = q_2$ и $\delta(q_2, b) = q_3$, то хотелось бы, чтобы $\delta(q_1, ab) = q_3$, т. е. чтобы δ продолжалась до $\Sigma^*: Q \times \Sigma^* \rightarrow Q$ следующим образом:

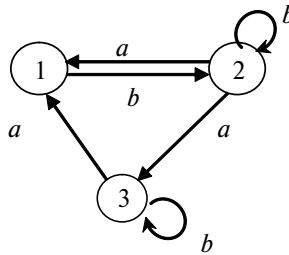
1. $\forall q \in Q: \delta(q, \lambda) = q$;
2. $\forall q \in Q, a \in \Sigma, u \in \Sigma^*: \delta(q, ua) = \delta(\delta(q, u), a)$.

Изображение — ориентированный граф с помеченными вершинами и ребрами.

Примеры

1. $Q = \{1, 2, 3\}$, $\Sigma = \{a, b\}$.

δ	1	2	3
A	2	3	1
b	2	2	3



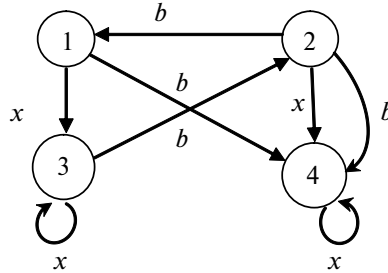
$$A = (Q, \Sigma, \delta)$$

2. Привидение:

$Q = \{\text{молчит (1), хохочет (2), ухает (3), топает (4)}\}$,

$\Sigma = \{\text{хлопнуть дверью (x), включить музыку (b)}\}$.

δ	1	2	3	4
x	3	4	3	4
b	4	1	2	2



Автомат $A = (Q, \Sigma, \delta)$ называется синхронизируемым, если

$\exists \omega \in \Sigma^* \exists q \in Q : \forall p \in Q : \delta(p, \omega) = q$ (т. е. ω синхронизирует автомат A).

Пусть у автомата известно начальное состояние $q_0 \in Q$ и выделено множество $T \subseteq Q$ заключительных состояний.

Слово ω принимается автоматом $A = (Q, \Sigma, \delta)$, если $\delta(q_0, \omega) \in T$.

$L(A)$ — множество всех принимаемых автоматом слов ($L(A) = \{\omega \mid \delta(q_0, \omega) \in T\}$) называется языком, распознаваемым автоматом $A = (Q, \Sigma, \delta, q_0, T)$.

Пятерку $(Q, \Sigma, \delta, q_0, T)$ иногда называют конечным распознавателем.

Пример

1.

	\downarrow	\uparrow	\uparrow
δ	0	1	2
0	0	2	1
1	1	0	2

$q_0 = 0$,

$T = \{1, 2\}$,

$A = (Q, \Sigma, \delta, q_0, T)$,

$$L(A) = \left\{ 1, 10, 01, 001, 010, 100, 101, 111, 0001, 0010, \right. \\ \left. 0100, 0101, 0111, 1000, 1010, 1011, 1101, 1110, \dots \right\},$$

$$\bar{L}(A) = \{0, 00, 11, 000, 011, 110, 0000, 0011, 0110, 1001, 1100, 1111, \dots\},$$

$$\omega \in \bar{L}(A) \Leftrightarrow \delta(q_0, \omega) \notin T \Leftrightarrow \delta(0, \omega) = 0,$$

$$L_0 = \{\omega \mid \delta(0, \omega) = 0\},$$

$$L_1 = \{\omega \mid \delta(0, \omega) = 1\},$$

$$L_2 = \{\omega \mid \delta(0, \omega) = 2\}.$$

Гипотеза: $\omega \in L_i \Leftrightarrow \overline{\omega_2} \equiv i \pmod{3}$, где $\overline{\omega_2}$ — значение соответствующего ω двоичного числа.

Докажем методом индукции по длине слова:

База индукции. $\delta(0, 0) = 0$, $\delta(0, 1) = 1$.

Шаг индукции. Если $\omega = v0 \Rightarrow \overline{\omega_2} = 2 \cdot \overline{v_2}$,

$$\overline{v_2} \equiv 0 \pmod{3} \Rightarrow \overline{\omega_2} \equiv 0 \pmod{3}.$$

$$\overline{v_2} \equiv 1 \pmod{3} \Rightarrow \overline{\omega_2} \equiv 2 \pmod{3}.$$

$$\overline{v_2} \equiv 2 \pmod{3} \Rightarrow \overline{\omega_2} \equiv 1 \pmod{3}.$$

При этом

$$v \in L_0 \Rightarrow \omega \in L_0,$$

$$v \in L_1 \Rightarrow \omega \in L_2,$$

$$v \in L_2 \Rightarrow \omega \in L_1.$$

Случай $\omega = v1$ рассматривается аналогично.

2. Хочется распознавать правильно записанные десятичные числа (без знака). Правильно: 123, 0.10, 1.3, 123,0,0.0. Неверно: ..1,1.,00.1,1.1.1,01.

Можно ли построить соответствующий автомат? Более общий вопрос: можно ли с помощью конечного распознавателя распознать любой язык?

Приведем пример языка, дающего отрицательный ответ на заданный вопрос:

$$\Sigma = \{a, b\}, \quad L = \{a^n b^n \mid n \in N_0\}.$$

Докажем, что не существует автомата $A: L = L(A)$ методом «от противного»:

Пусть $A = (Q, \Sigma, \delta, q_0, T)$; $L = L(A)$.

Рассмотрим элементы $\delta(q_0, a), \delta(q_0, a^2), \delta(q_0, a^3) \dots$ из Q .

$|Q| < \infty \Rightarrow$ есть повторы, т. е. $\exists i < j : \delta(q_0, a^i) = \delta(q_0, a^j)$.

$\delta(q_0, a^i b^j) = \delta(\delta(q_0, a^i), b^j) \in T$.

Для слова $a^i b^j$ имеем $\delta(q_0, a^i b^j) \in T$

и $\delta(q_0, a^i b^j) = \delta(\delta(q_0, a^i), b^j) = \delta(\delta(q_0, a^j), b^i) = \delta(q_0, a^j b^i) \Rightarrow a^j b^i \in L$.

Поскольку $i < j$, это противоречит определению L .

Итак, не любой язык можно распознать с помощью конечного автомата.

Язык L называется распознаваемым, если $\exists A = (Q, \Sigma, \delta, q_0, T) : L = L(A)$.

Моноид переходов конечного автомата

Автомат $A = (Q, \Sigma, \delta)$ полностью определён действиями букв.

Каждая буква $a \in \Sigma$ определяет функцию $\delta(-, a) : Q \rightarrow Q$.

Функции $Q \rightarrow Q$ составляют симметрическую полугруппу $\tau(Q)$. Не только каждая буква из Σ определяет некоторую функцию $\delta(-, a) \in \tau(Q)$, но и каждое слово $\omega \in \Sigma^*$ дает функцию $\delta(-, \omega) \in \tau(Q)$, определенную следующим образом: $\omega = a_1 a_2 \dots a_n \Rightarrow \delta(-, \omega) = \delta((\dots \delta(\delta(-, a_1), a_2), \dots), a_n)$.

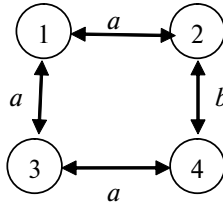
Мы получили полугруппу с единицей (т. е. моноид) $\{\delta(-, \omega) \mid \omega \in \Sigma^*\}$, который обозначается через $M(A)$ и называется моноидом переходов автомата A .

Отображение $\omega \rightarrow \delta(-, \omega)$ является гомоморфизмом, и, следовательно, моноид переходов автомата является гомоморфным образом свободного моноида Σ^* . Как свободный моноид порождается буквами ($\Sigma^* = \langle \Sigma \rangle$), так и моноид переходов порождается действиями букв:

$$M(A) = \langle \delta(-, a) \mid a \in \Sigma \rangle.$$

Конечный автомат дает пример алгебры унарных операций.

Пример



Моноид переходов:

δ	1	2	3	4
λ	1	2	3	4
a	2	1	4	3
b	3	4	1	2
a^2	1	2	3	4
ab	4	3	2	1
ba	4	3	2	1
b^2	1	2	3	4
aba	3	4	1	2
ab^2	2	1	4	3

Таблица Кели (таблица умножения)

	λ	a	b	ab
λ	λ	a	b	ab
a	a	λ	ab	b
b	b	ab	λ	a
ab	ab	b	a	λ

Моноид в данном примере является группой, которая обычно обозначается как V_4 (четвертая группа Клейна).

Распознавание автоматом и моноидом

Пусть внутри моноида M выбрано подмножество $P \subset M$ и, кроме того, имеется гомоморфизм $\varphi: \sum^* \rightarrow M$. Будем говорить, что (M, P, φ) распознает L , если $\forall \omega \in \sum^* \omega \in L \Leftrightarrow \varphi(\omega) \in P$ (другими словами, если $L = \varphi^{-1}(P)$).

Утверждение 1. Если L распознается автоматом, то L распознается моноидом переходов автомата.

Доказательство

Определим гомоморфизм $\varphi: \sum^* \rightarrow M(A)$ и множество P следующим образом: $\varphi(\omega) = \delta(-, \omega)$, $P = \varphi(L)$.

" \Rightarrow " по определению

" \Leftarrow ": $\omega \in \sum^* : \varphi(\omega) \in P : \exists v \in L \varphi(\omega) = \varphi(v) \Rightarrow \delta(-, \omega) = \delta(-, v)$,

$\delta(q_0, \omega) = \delta(q_0, v) \in T \Rightarrow \omega \in L$.

Утверждение 2. Если L распознается конечным моноидом M , то существует ДКА.

$A: L(A) = L$.

Доказательство

L распознается моноидом $M \Leftrightarrow \exists P \subseteq M, \varphi: \sum^* \rightarrow M : L = \varphi^{-1}(P)$.

Строим автомат, полагая $Q=M$, $\delta(q, a) = q \cdot \varphi(a)$, $q_0 = 1_M$, $T = P$.

Проверим требуемое условие. Пусть $\omega \in \sum^*$, $\omega = a_1 \cdots a_n$.

$\omega \in L \Leftrightarrow \varphi(\omega) \in P \Leftrightarrow \varphi(a_1) \cdots \varphi(a_n) \in P \Leftrightarrow (1_M \Leftrightarrow \varphi(a_1) \cdots \varphi(a_n)) \in P \Leftrightarrow$
 $\Leftrightarrow \delta(\delta(\dots(\delta(q_0, a_1), a_2) \dots) a_n) \in P \Leftrightarrow \delta(q_0, \omega) \in P = T \Leftrightarrow \omega \in L(A)$.

Свойства распознаваемых языков

1° L распознаваем $\Rightarrow \bar{L}$ распознаваем.

Если $L(A) = L$ для $A = (Q, \sum, \delta, q_0, T)$, то $\bar{L} = L(A')$ для $A' = (Q, \sum, \delta, q_0, Q \setminus T)$.

2° Если $L \subseteq \sum^*$ распознаваем и $\varphi: A^* \rightarrow \sum^*$ — гомоморфизм (шифр простой замены), то $\varphi^{-1}(L)$ распознаваем.

Доказательство

L распознаваем $\Rightarrow \exists M, |M| < \infty, \varphi: \sum^* \rightarrow M, P \subseteq M : \varphi^{-1}(P) = L$.

Тогда гомоморфизм $\varphi \circ \varphi^{-1}$ распознает $\varphi^{-1}L$. Действительно, проверим, что $(\varphi \circ \varphi^{-1})^{-1}P = \varphi^{-1}L$:

$$\begin{aligned}\omega \in (\varphi \circ \infty)^{-1} P &\Leftrightarrow (\varphi \circ \infty)(\omega) \in P \Leftrightarrow \infty(\varphi(\omega)) \in P \Leftrightarrow \\ &\Leftrightarrow \varphi(\omega) \in \infty^{-1} P \Leftrightarrow \varphi(\omega) \in L \Leftrightarrow \omega \in \varphi^{-1} L.\end{aligned}$$

3° Пусть L — распознаваемый и $K \subseteq \Sigma^*$.

Тогда $K^{-1}L$, LK^{-1} распознаваемы.

Доказательство

L — распознается $\Leftrightarrow \exists M, P \subseteq M, \infty: \Sigma^* \rightarrow M$ — гомоморфизм, $L = \infty^{-1} P$.

Рассмотрим $R = \{m \mid m \in M, \exists k \in K: \infty(k)m \in P\}$.

$$\begin{aligned}\omega \in K^{-1}L &\Leftrightarrow \exists k \in K: k\omega \in L \Leftrightarrow \exists k \in K: \infty(k\omega) \in P \Leftrightarrow \\ &\Leftrightarrow \exists k \in K: \infty(k)\infty(\omega) \in P \Leftrightarrow \infty(\omega) \in R.\end{aligned}$$

Значит, $(M, R \subseteq M, \infty: \Sigma^* \rightarrow M)$ распознает $K^{-1}L$.

Правое частное — аналогично.

4° Пусть L_1, L_2 — распознаваемы. Тогда $L_1 \cap L_2$ распознаваем.

Доказательство

$$L_1 \Rightarrow M_1, P_1 \subseteq M_1, \infty_1: \Sigma^* \rightarrow M_1, \infty_1^{-1} P_1 = L_1.$$

$$L_2 \Rightarrow M_2, P_2 \subseteq M_2, \infty_2: \Sigma^* \rightarrow M_2, \infty_2^{-1} P_2 = L_2.$$

$$M = M_1 \times M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}.$$

$$(a, b)(c, d) = (ac, bd).$$

Построим $\infty: \Sigma^* \rightarrow M$ (гомоморфизм):

$$\infty(\omega) = (\infty_1(\omega), \infty_2(\omega)).$$

Покажем $\infty^{-1} P = L_1 \cap L_2$, где $P = P_1 \times P_2$.

$$\omega \in \infty^{-1} P \Leftrightarrow \infty(\omega) \in P \Leftrightarrow (\infty_1(\omega), \infty_2(\omega)) \in P_1 \times P_2 \Leftrightarrow \begin{cases} \infty_1(\omega) \in P_1 \\ \infty_2(\omega) \in P_2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \omega \in L_1 \\ \omega \in L_2 \end{cases} \Leftrightarrow \omega \in L_1 \cap L_2.$$

Прямым произведением конечных автоматов (распознавателей)
 $A = ((Q, \sum, \delta), q_0, T)$, $B = ((R, \sum, \tau), r_0, S)$ называется автомат $A \times B = (Q \times R, \sum, \circ, (q_0, r_0), T \times S)$, где $\circ((q, r), a) = (\delta(q, a), \tau(r, a))$.

5° L_1, L_2 распознаваемы $\Rightarrow L_1 \cap L_2$ распознаваем.

Доказательство

В силу $L_1 \cap L_2 = \overline{L_1} \cap \overline{L_2}$, доказываемое утверждение является следствием $1^\circ, 4^\circ$.

Замкнутость множества распознаваемых языков относительно произведения и итерации

Утверждение 1. L_1 и L_2 распознаваемы $\Rightarrow L_1 L_2$ распознаваем.

Доказательство

Пусть L_1 распознается автоматом $A_1 = (Q_1, \sum, \delta_1, q_{01}, T_1)$ и L_2 распознается автоматом $A_2 = (Q_2, \sum, \delta_2, q_{02}, T_2)$.

$\forall a \in \sum \forall p \in Q_2 : \delta_2(q_{02}, a) = p \quad \forall t \in T_1$ создаем тройки (t, a, p) ,

т.е. строим НКА

$B = (Q_1 \cup Q_2, \sum, E, q_{02}, F)$,

где $E = \{(x, a, y) \mid \delta_1(x, a) = y\} \cup \{(x, a, y) \mid \delta_2(x, a) = y\} \cup$

$\cup \{(t, a, p) \mid t \in T_1 \& \delta_2(q_{02}, a) = p\}$,

$F = \begin{cases} T_2, \lambda \notin L_2, \\ T_1 \cup T_2, \lambda \in L_2. \end{cases}$

Проверим, что B распознает $L_1 L_2$.

$\omega \in L_1 L_2 \Rightarrow \exists u \in L_1, \exists v \in L_2 : \omega = uv \Rightarrow v A_1$ есть путь, помеченный и от q_{01} до T_1 , в A_2 есть путь, помеченный v от q_{02} до T_2 . Если $v = \lambda$, то $T_1 \subseteq F$, и, прочитав u в B , можно попасть в T_1 . Если же $v \neq \lambda$, то $v = ax, a \in \sum; \delta(q_{02}, a) = p$. Делаем переход из T_1 в p по добавленной стрелке, затем читаем в A_2 слово x из p и приходим в T_2 . Таким образом, v принимается B .

$\omega \in L(B) \Rightarrow$ есть путь, помеченный ω из q_{01} в F . Если путь приводит в T_1 , то он не выходит из $A_1 \Rightarrow \omega \in L_1 \text{ и } T_1 \subseteq F \Rightarrow \lambda \in L_2 \Rightarrow \omega = \omega\lambda \upharpoonright L_1 L_2$.

Если путь приводит в T_2 , то произошел ровно один переход из A_1 в A_2 по некоторому $a \in \Sigma$, при этом $\omega = u(av)$,

$$\delta_1(q_{01}, u) \in T_1 \Rightarrow u \in L_1,$$

$$\delta_2(q_{02}, av) \in T_2 \Rightarrow av \in L_2.$$

Следовательно, $\omega \in L_1 L_2$.

Утверждение 2. L — распознаваемый $\Rightarrow L^*$ — распознаваемый.

Доказательство

Строим $B = (Q \cup \{i\}, \Sigma, E, \{i\}, \{i\})$,

$$\text{где } E = \bigcup_{a \in \Sigma} (\{(p, a, q) \mid \delta(p, a) = q\} \cup \{(i, a, p) \mid \delta(q_0, a) = p\} \cup \{(q, a, i) \mid \delta(q, a) \in T\} \\ \cup \{(i, a, i) \mid \delta(q_0, a) \in T\}).$$

$$\omega \in L^* \Rightarrow \exists \omega_1, \dots, \omega_k \in L: \omega = \omega_1 \dots \omega_k \text{ либо } \omega = \lambda.$$

В последнем случае очевидно, что $\omega \in L(B)$.

Покажем, что для каждого j в B есть путь из i в i , помеченный ω_j .

$$|\omega_j| = 1 \Rightarrow \omega_j \in \Sigma \Rightarrow \delta(q_0, \omega_j) \in T \Rightarrow \text{есть петля из } i \text{ в } i, \text{ помеченная } \omega_j.$$

$$|\omega_j| \geq 2 \Rightarrow \omega_j = avb. \text{ Возьмем в } A \text{ путь, помеченный } avb, \text{ и заменим в нем}$$

шаги: первый — на шаг из i , последний — на шаг в i .

Соединяя найденные пути в один длинный путь из i в i , помеченный ω , получаем искомый путь, т.е. $\omega \in L(B)$.

Обратно, пусть $\omega \in L(B)$, т.е. в B есть путь из i в i , помеченный ω . Разобьем этот путь на такие куски с концами в i , у которых в середине i нет. Рассмотрим некоторый кусок, пусть он помечен словом v .

$$|v| = 1 \Rightarrow \delta(q_0, v) \in T,$$

$$|v| \geq 2 \Rightarrow v = aub \Rightarrow \delta(q_0, aub) \in T.$$

В каждом случае $v \in L \Rightarrow \omega \in L^*$.

Рациональность и распознаваемость языков

Теорема Клини

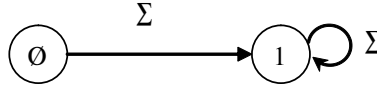
L рационален $\Leftrightarrow L$ распознаваем.

Доказательство

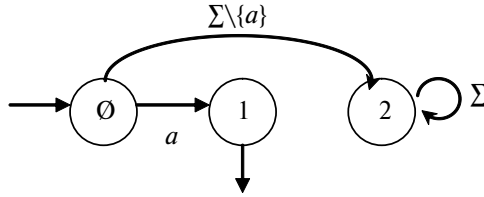
(\Rightarrow)

L рационален $\Rightarrow L$ записывается рациональным выражением.

$\{\lambda\}$ распознается следующим автоматом:



$a \in \Sigma \Rightarrow \{a\}$ распознается автоматом:



L_1, L_2 распознаваемы $\Rightarrow L_1 \cup L_2$ распознаваем.

L_1 и L_2 распознаваемы $\Rightarrow L_1 L_2$ распознаваем.

L распознаваем $\Rightarrow L^*$ распознаваем.

Далее — индукция по числу операций в рациональном выражении.

(\Leftarrow) $L = L(A), A = (Q, \Sigma, E, \delta, q_1, T), |Q| = n, Q = \{q_1 \dots q_n\}$.

Обозначим

$$L(i, j, k) = \left\{ \omega \in \Sigma^* \mid \delta(i, \omega) = j, \forall u : (\omega = uv, |u| > 0, |v| > 0) \Rightarrow (\delta(i, u) \in \{q_1 \dots q_{k-1}\}) \right\}.$$

Имеем $L(A) = \bigcup_{j: q_j \in T} L(1, j, n+1)$. Для доказательства рациональности этого

языка достаточно показать рациональность каждого из объединяемых языков. Индукцией по k покажем, что $\forall i, j L(i, j, k)$ рационален.

База индукции:

$L(i, i, 1) = \{\lambda\} \cup \{a \in \Sigma \mid \delta(i, a) = i\}$ — рациональный язык.

$L(i, j, 1) = \{a \in \Sigma \mid \delta(i, a) = j\}$ — рациональный язык.

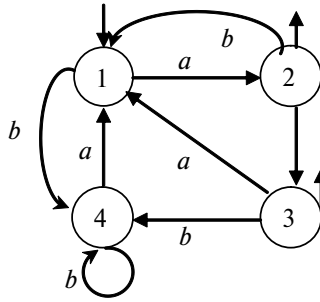
Шаг индукции:

$$L(i, j, k+1) = L(i, j, k) \cup L(i, k, k) (L(k, k, k))^* L(k, j, k).$$

Следствие

1. $L = \{a^n b^n \mid n \in N_0\}$ не является рациональным.
2. L_1, L_2 — рациональные языки $\Rightarrow \overline{L_1}, \overline{L_2}, L_1 \cap L_2$ — рациональные языки.

Пример



$$L_i = \left\{ \omega \in \Sigma^* \mid \delta(q_1, \omega) = q_i \right\}$$

$$\begin{cases} L_1 = \lambda + L_4 a + L_3 a + L_2 b \\ L_2 = L_1 a \\ L_3 = L_2 a \\ L_4 = L_3 b + L_1 a + L_4 b \end{cases}$$

$$\begin{cases} L_1 = \lambda + L_4 a + L_1 a^3 + L_1 a b \\ L_4 = L_1 a^2 b + L_1 b + L_4 b \end{cases}$$

Лемма

Пусть $\lambda \neq V$, тогда $L = U + LV \Leftrightarrow L = UV^*$.

Доказательство

$$(\Leftarrow) U + LV = U + (UV^*)V = U \cdot \{\lambda\} + U \cdot V + U \cdot V^2 + \dots = UV^* = L$$

$$(\Rightarrow) \omega \in L.$$

Либо $\omega \in U$, либо $\omega \in LV$.

1. $\omega \in U \Rightarrow \omega \in UV^*$.
2. $\omega \in LV$

Докажем методом «от противного». Предположим, что $\omega \notin UV^*$. Можно считать, что ω — кратчайшее из $L \setminus UV^*$.

Тогда $\omega = \omega_1 v, \omega_1 \in L, v \in V, v \neq \lambda$.

Поскольку $|\omega_1| < |\omega|$, то ω_1 короче самого короткого слова из $L \setminus UV^* \Rightarrow \omega_1 \in UV^*$. Тогда $\omega \in UV^*$.

Значит, $L \subseteq UV^*$ доказано.

Докажем обратное включение методом «от противного».

Пусть ω — кратчайшее слово из $UV^* \setminus L$.

$\omega = uv_1 \cdots v_k, u \in U, v_j \in V (k \geq 0)$.

Если $k = 0$, то $\omega = u \in U \Rightarrow \omega \in L$

Если $k > 0$, то $\omega = \omega_1 v_k, v_k \neq \lambda \Rightarrow |\omega_1| < |\omega| \Rightarrow \omega_1 \in L \Rightarrow$

$\Rightarrow \omega = \omega_1 v_k \in LV \subseteq L$

Теперь по доказанной лемме из $L_4 = L_1 a^2 b + L_1 b + L_4 b$ следует, что $L_4 = (L_1 a^2 b + L_1 b) b^* = L_1 (a^2 + \lambda) b b^*$; из $L_1 = \lambda + L_4 a + L_1 a^3 + L_1 a b = \lambda + L_1 (a^2 + \lambda) b b^* a + L_1 a^3 + L_1 a b = \lambda + L_1 ((a^2 + \lambda) b b^* a + a^3 + a b)$ следует, что $L_4 = ((a^2 + \lambda) b b^* a + a^3 + a b)^*$. Автомат распознает язык $L_2 + L_3 = L_1 a (\lambda + a) = ((a^2 + \lambda) b b^* a + a^3 + a b)^* a (\lambda + a)$.

Содержание

1. Логические исчисления	3
Множество, отношения, функции	3
Множества	3
Основное свойство множеств.....	3
Способы задания множеств.....	3
Операции с множествами	5
Свойства $\forall A, B, C$	5
Отношения.....	8
Основное свойство.....	8
Теорема (об отношениях эквивалентности)	10
Структуры порядка	11
Операции с отношениями	12
Функции.....	14
 2. Предикаты	20
Операции над предикатами.....	20
Кванторы.....	21
Предикатные формулы. Тавтологии.....	23
Исчисление предикатов	28
 3. Булевы функции	30
Определение и примеры.....	30
Суперпозиция функций	32
Тождества	32
Дизъюнктивная нормальная форма БФ	33
Полиномы Жегалкина.....	36
Замкнутые классы БФ	37
Теорема Поста	43
 4. Комбинаторика	49
Основные правила	49
Элементарные комбинаторные функции	50
Свойства числа сочетаний.....	51
Задача (о кроликах).....	54

5. Теория графов	57
Определение и задание графа	57
Операции с множествами.....	60
Изоморфизм графов	60
О сложности алгоритмов	62
Маршруты	64
Связность	67
Эйлеровы пути	71
Деревья	75
Потоки в сетях	78
Алгоритм поиска максимального потока	81
Расстояние в графах.....	82
Двудольные графы	84
Алгоритм проверки двудольности связного графа.....	86
Паросочетание	87
Плоские и планарные графы.....	90
 6. Автоматы и языки	 92
Языки	92
Операции с языками.....	92
Автоматы. Распознаватели	94
Моноид переходов конечного автомата	97
Распознавание автоматом и моноидом	98
Свойства распознаваемых языков	99
Замкнутость множества распознаваемых языков относительно произведения и итерации	101
Рациональность и распознаваемость языков	103

Учебное издание

Ананичев Дмитрий Сергеевич
Андреева Ирина Юрьевна
Гредасова Надежда Викторовна
Костоусов Кирилл Викторович

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Редактор О. С. Смирнова
Верстка О. П. Игнатьевой

Подписано в печать 04.12.2014. Формат $70 \times 100 \frac{1}{16}$.
Бумага писчая. Плоская печать. Гарнитура Newton.
Уч.-изд. л. 5,7. Усл. печ. л. 8,7. Тираж 100 экз.
Заказ 1.

Издательство Уральского университета
Редакционно-издательский отдел ИПЦ УрФУ
620049, Екатеринбург, ул. С. Ковалевской, 5
Тел.: 8 (343) 375-48-25, 375-46-85, 374-19-41
E-mail: rio@urfu.ru

Отпечатано в Издательско-полиграфическом центре УрФУ
620075, Екатеринбург, ул. Тургенева, 4
Тел.: 8 (343) 350-56-64, 350-90-13
Факс: 8 (343) 358-93-06
E-mail: press-urfu@mail.ru

