Математические основы информатики

Лекция 2.
Введение в теорию множеств и математическую логику.

Сергей Леонидович Бабичев

Вспоминаем обозначения

$x \in [a;b]$	$a \leqslant x \leqslant b$
$x \in [a;b)$	$a \leqslant x < b$
$x \in \mathbb{Z}$	x — целое число
$x \in \mathbb{Z}_M$	x — целое число, $0 \leqslant x < M$
$x \in \mathbb{N}$	x — целое число, $x > 0$
$x \in \mathbb{P}$	x — простое число
$x \in \mathbb{Q}$	x — рациональное число
$x \in \mathbb{R}$	x — действительное число
$a \vdots b$	a делится нацело на b
$a \not\vdots b$	a не делится нацело на b
$r = a \pmod p$	остаток от деления нацело a на p, $r \in [0, p)$
$a \equiv b \pmod{()p}$	a и b сравнимы по модулю p
$\forall x:$	для каждого x ...
$\exists x:$	существует x такое, что ...

Множества

- *Множество* — фундаментальное понятие математики.
  Определение: *Множество* — произвольный набор *элементов*. Если элемент x является элементом множества A, то x *принадлежит* A или $x \in A$.
- Что тогда такое *набор*?
- Пусть понятия *набор* и *множество* будут аксиоматическими.

Задание состава элементов множества

1. Перечислением:

$$A = \{3, 1, 4, 6\}, \tag{1}$$

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} \tag{2}$$

   Множества с повторяющимися элементами называются *мультимножествами* или *комплектами*. Мы их рассматривать не будем.

2. Заданием свойств. В множество включаются элементы, удовлетворяющие заданному свойству.

$$\{x : x > 0, x \vdots 2\}. \tag{3}$$

Подмножества

Определение: Множество A есть *подмножество* множества B, если каждый из элементов множества A принадлежит множеству B. Это обозначается так:

$$A \subset B. \tag{4}$$

- Если $A \subset B$ и $B \subset A$, то $A = B$ — множества A и B равны.
- Если $A \subset B$ и $A \neq B$, то A — *собственное подмножество* B.

Определение: Число элементов множества A обозначается через $|A|$.

Отношения на подмножествах

- Для отношения $\subset$:
  1. *Рефлексивность*: $\forall A : A \subset A$;
  2. *Антисимметричность*: $\forall A, B : A \subset B \wedge B \subset A \implies A = B$;
  3. *Транзитивность*: $\forall A, B, C : A \subset B \wedge B \subset C \implies A \subset C$;
- Для отношения $=$:
  1. *Рефлексивность*: $\forall A : A = A$;
  2. *Симметричность*: $\forall A, B : A = B \implies B \subset A$;
  3. *Транзитивность*: $\forall A, B, C : A = B \wedge B = C \implies A = C$;
- *Пустое множество* $\emptyset$, есть подмножество любого множества.

$$\forall A : \emptyset \subset A \tag{5}$$

- Не путайте знаки $\in$ и $\subset$!

Парадокс Рассела

- Наши определения множеств и подмножеств интуитивны, но наивны.
- Бертран Рассел (1872-1970).
- Пусть множество A есть множество всех множеств, не являющихся его собственными элементами.

$$A = \{X : X \notin A\}. \tag{6}$$

- С одной стороны, по определению, $A \notin A$, но тогда A нужно включить в множество.
- С другой стороны, если $A \in A$, то не выполняется исходное условие.
- Может ли всемогущее существо создать камень, который оно не может поднять?

Универсум. Операции над множествами

Определение: *Универсум* — множество, которому заведомо принадлежат все элементы всех рассматриваемых множеств. Его обычно обозначают как U.

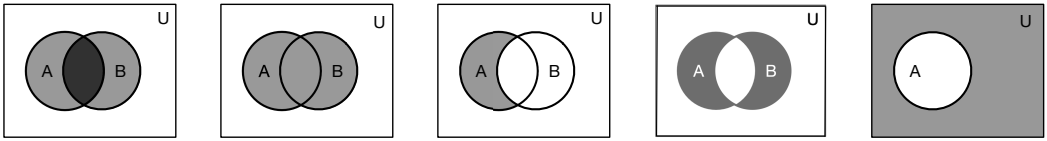
Определение: Для заданных множеств A, B и универсума U:

- *объединение:*
$$A \cup B = \{x : x \in A \vee x \in B\}; \tag{7}$$
- *пересечение:*
$$A \cap B = \{x : x \in A \wedge x \in B\}; \tag{8}$$
- *разность:*
$$A \setminus B = \{x : x \in A \wedge x \notin B\}; \tag{9}$$
- *симметрическая разность:*
$$A \triangle B = \{x : x \in A \wedge x \notin B \vee x \in B \wedge x \notin A\}; \tag{10}$$
- *дополнение:*
$$\overline{A} = \{x : x \notin A\} = U \setminus A. \tag{11}$$

Определение: Объединение двух непересекающихся множеств называют *дизъюнктным объединением*.

Знакомые картинки: круги Эйлера

Другое название: диаграммы Венна.



1) $A \cap B$; 2) $A \cup B$; 3) $A \setminus B$; 4) $A \triangle B$; 5) $\overline{A}$.

Законы операций над множествами

Над операциями над множествами действует несколько законов:

- *коммутативности:*

$$A \cap B = B \cap A; \tag{12}$$

$$A \cup B = B \cup A; \tag{13}$$

- *ассоциативности:*

$$(A \cap B) \cap C = A \cap (B \cap C); \tag{14}$$

$$(A \cup B) \cup C = A \cup (B \cup C); \tag{15}$$

- *дистрибутивности:*

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C); \tag{16}$$

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C); \tag{17}$$

- *де Моргана*:

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}; \tag{18}$$

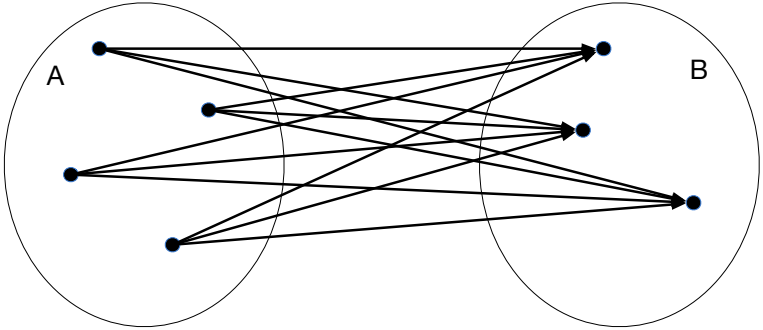
$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}; \tag{19}$$

Декартово произведение множеств

Определение: Множество всех упорядоченных пар (a, b), где $a \in A$, $b \in B$, называется *Декартовым произведением* множеств A и B и обозначается $A \times B$.

$$|A \times B| = |A| \times |B|. \tag{20}$$

Другое название — *прямое произведение*.



Декартово произведение множеств

$$F : A \to B. \tag{21}$$

- Неформально обобщается на произведение любого конечного числа множеств.
- Множества, которые мы умножаем, могут быть одним и тем же множеством.
- Тогда появляется операция *возведения в степень*.
- Множество $\mathbb{B} = \{0, 1\}$ при возведении в степень m даст 2^m элементов.

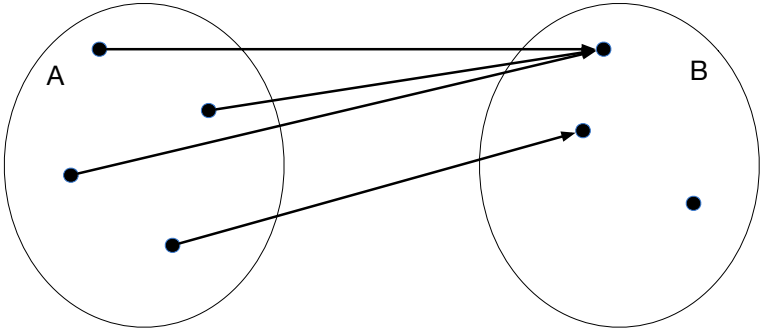
Соответствия и отображения

Декартово произведение двух множеств определяет связи каждый $\rightarrow$ каждый. Это — частный случай *соответствия* множеств.

Определение: *Соответствие* F между множествами A и B есть какое-либо подмножество Декартова произведения $F \subset A \times B$.

Определение: Если в $F : A \rightarrow B$ для каждого элемента $a \in A$ имеется ровно одно $b \in B$, то это *отображение* A на B или *функция* $b = F(a)$.

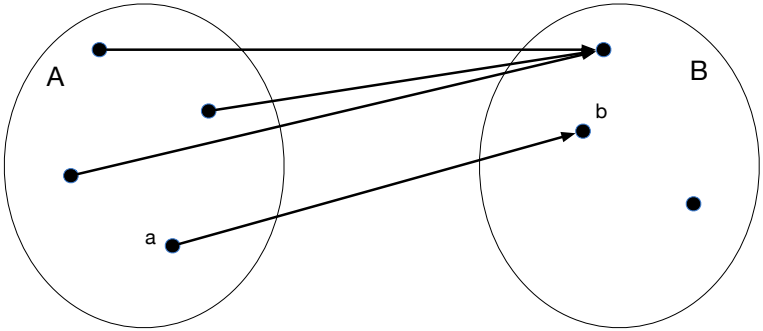
$$F : A \rightarrow B. \tag{22}$$



Определение: b называется *образом* точки a при этом отображении,

$$F^{-1}(b) \stackrel{\text{def}}{=} \{a \in A : F(a) = b\}. \tag{23}$$

а a — прообразом.



Определение: Множество всех $b \in B$ с непустым прообразом есть *образ отображения* $F : A \to B$.

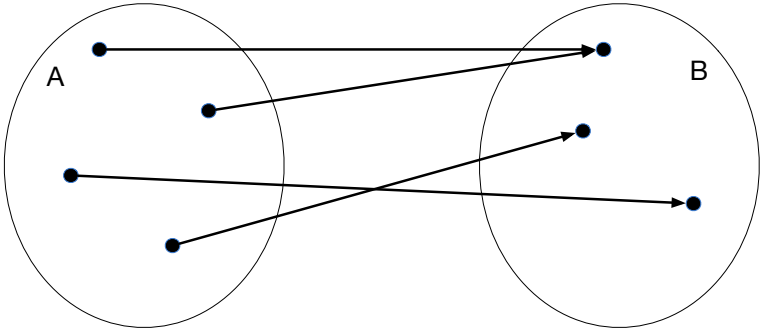
$$\text{im}(F) \stackrel{\text{def}}{=} \{b \in B : F^{-1}(b) \neq \emptyset\} = \{b \in B : \exists a \in A : F(a) = b\}. \tag{24}$$

Определение: Отображения $F : A \to B$ и $G : A \to B$ *равны*, если

$$\forall a \in X : F(a) = G(a). \tag{25}$$

Определение: Отображение $F : A \to B$ есть *сюръекция* $A \twoheadrightarrow B$, если

$$\mathsf{im}(F) = B. \tag{26}$$



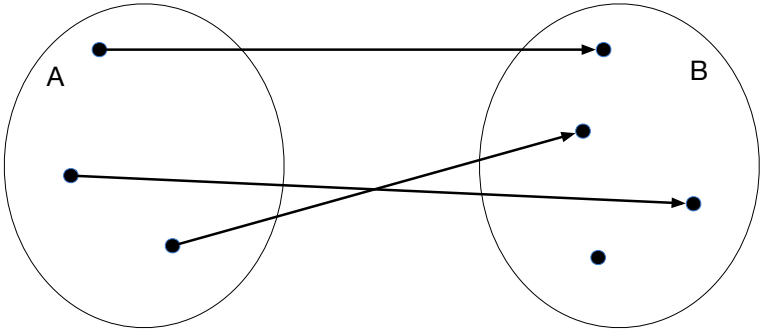
Сюръекция A на B.

Как увидеть, что отображение сюръективно: прообраз каждого элемента $b \in B$ не пуст.

Другие термины для сюръекции: *наложение*, *эпиморфизм*.

Определение: Отображение $F : A \to B$ есть *инъекция* $A \hookrightarrow B$, если

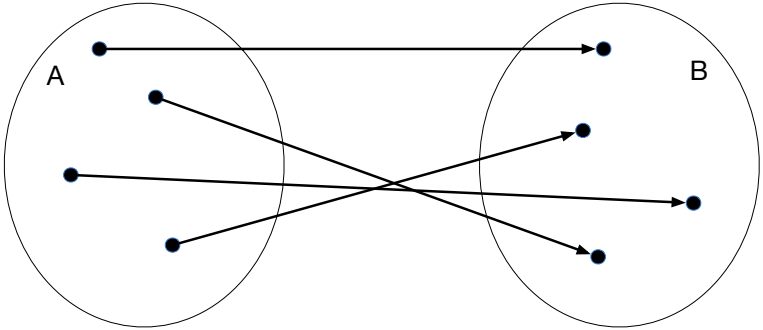
$$\forall a_1, a_2 \in A : F(a_1) = F(a_2) \implies a_1 = a_2. \tag{27}$$



Инъекция A на B.

При этом отображении прообраз каждого элемента $b \in B$ содержит не более одного элемента. Обратите внимание, что прообраза может не быть вообще! Инъекцию ещё называют словами *вложение* или *мономорфизм*.

Определение: Отображение $F : A \to B$ есть биекция, если оно одновременно является инъекцией и сюръекцией и обозначается $A \widetilde{=} B$.



Биекция A на B.

Для каждого элемента $a \in A$ существует ровно один элемент $b \in B$ такой, что $F(a) = b$. Другие термины: *взаимно-однозначное* соответствие, *изоморфизм*.

Алгебра множеств

- Как доказывать эквивалентность высказываний над множествами?
- Как доказать, например, один из законов дистрибутивности?

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

- Будем доказывать, что любой элемент одной части является элементом другой.

Доказываем закон дистрибутивности

1. Доказываем $L \implies R$. Пусть $x \in (A \cap B) \cup C$.
2. По определению объединения $x \in (A \cup B)$ или $x \in C$.
3. $x \in C \implies x \in (A \cup C)$.
4. $x \in C \implies x \in (B \cup C)$.
5. $x \in (A \cup C) \cap (B \cup C)$. Доказали $L \implies R$.
6. Доказываем $R \implies L$. Пусть $x \in (A \cup C) \cap (B \cup C)$.
7. По определению пересечения $x \in (A \cup C)$ и $x \in (B \cup C)$.
8. Теперь если $x \in C$, то $x \in (A \cap B) \cup C$.
9. Если же $x \notin C$, то так как $x \in (A \cup C) \implies x \in A$.
10. Аналогично доказываем, что $x \in B$.
11. Так как $x \in A$ и $x \in B \implies x \in (A \cap B)$.
12. Из (8) и (11) следует $R \implies L$.

Мощность множества: немного подробнее

- **Утверждение.** Для конечных множеств A и B существует биекция тогда и только тогда, когда $|A| = |B|$. Равномощные множества A и B обозначаются

$$A \cong B \tag{28}$$

- **Утверждение.** Для множеств A, B и C верно:
  - $A \cong A$. — рефлексивность;
  - если $A \cong B$, то $B \cong A$ — симметричность;
  - если $A \cong B$ и $B \cong C$, то $A \cong C$ — транзитивность.
- Отношения, для которых выполняются свойства рефлексивности, симметричности и транзитивности, называются *отношениями эквивалентности*.

Счётные множества

Определение: Множеством натуральных чисел называется множество $\mathbb{N} = \{0, 1, 2, \dots, \}$.
Определение: Множество A называется счётным, если оно равномощно множеству $\mathbb{N}$.

Парадокс Галиллея

- Рассмотрим множество квадратов всех натуральных чисел

$$Q = \{n^2 : n \in \mathbb{N}\} \tag{29}$$

- Не все числа — квадраты.
- Но множество равномощно $\mathbb{N}$.
- Множество $\mathbb{N}$ равномощно своему подмножеству Q.

Свойства счётных множеств

- **Метафора Гильберта**. Пусть имеется отель, где для каждого $x \in \mathbb{N}$ есть одноместная комната с номером N. Множество счётное, если его можно расселить в этом отеле.

Утверждение. Если A — счётное множество и $b \notin A$, то $A \cup B$ тоже счётно.
Доказательство. Пусть x есть биекция $\mathbb{N} \to A$. Тогда определим биекцию $y : \mathbb{N} \to (A \cup \{b\})$ таким образом:

$$y(0) \to b$$
$$y(n) = x(n-1) \text{ для } n > 0$$

Утверждение. Если A — счётное множество и B — конечное, то $A \cup B$ тоже счётно.
Утверждение. Если A и B — счётные множествато $A \cup B$ тоже счётно.
Утверждение. Если для каждого $n \in \mathbb{N}$ множество A_n счётно, то множество $A_0 \cup A_1 \cup \ldots$ тоже счётно.

Примеры несчётных множеств. Континуумы.

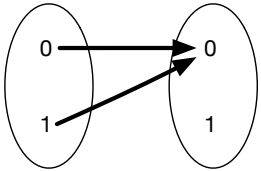
- Достаточно доказать, что множество $\{0,1\}^{\mathbb{N}}$ несчётно.
- **Диагональный метод Кантора**.
- **Теорема о количестве точек на отрезке**. Множество точек P на отрезке $[0,1]$ равномощно множеству $\{0,1\}^{\mathbb{N}}$.
- textbfЛемма. Если A бесконечно, а B счётно, то $A \cup B \cong A$.

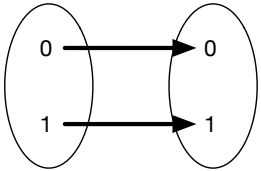
Почему нас интересует логика?

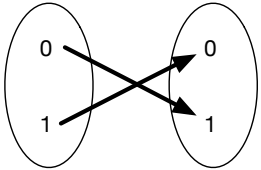
- Доказывать корректность алгоритмов можно с помощью аппарата математической логики: если верно высказывание A и верны все преобразования, то будет верно и высказывание B, которое есть следствие этих преобразований.
- Представление чисел в современных компьютерах в подавляющем количестве случаев двоичное. Знание этого представления позволяет делать невероятные трюки, ускоряющие исполнение некоторых алгоритмов в десятки раз. Работа с битами в представлении числа — интересная математическая задача

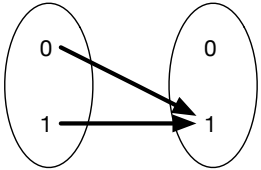
Логические операции и их операнды

- Сколько имеется функций от одного логического аргумента?
- *Аргумент* (элемент множества D) может быть 0 или 1, а *значение* функции — тоже либо 0, либо 1.
- Нужна функция $\rightarrow$ образ прообраза единственен.









Все возможные логические функции от одной переменной.

Логические функции от одного аргумента

- Упорядочим все такие возможные функции по их значениям.

Функция 00	
x	f(x)
0	0
1	0

Функция 01	
x	f(x)
0	0
1	1

Функция 10	
x	f(x)
0	1
1	0

Функция 00	
x	f(x)
0	1
1	1

- Функция 00 — функция *тривиального нуля*.
- Функция 01 — тривиальная функция *тавтологии*.
- Единственная нетривиальная функция — функция 10. Функция логического отрицания, not, $\bar{x}$.
- функция 11 — функция *тривиальной единицы*, или *тривиальной истины*.

Функции от двух аргументов

- Функции от кортежей-пар.
- Множество кортежей-аргументов содержит $2^2 = 4$ элемента.
- Множество различных функций $= 2^{2^2} = 16$.
- Для функции с любым количеством аргументов строится *таблица истинности* и она получает номер по последнему столбцу.

Функция 0110		
x	y	f(x,y)
0	0	0
0	1	1
1	0	1
1	1	0

Пример одной из функций.

Другое представление функций с двумя аргументами

Функция 0000		
	0	1
0	0	0
1	0	0

Функция 0001		
	0	1
0	0	0
1	0	1

Функция 0010		
	0	1
0	0	0
1	1	0

Функция 0011		
	0	1
0	0	0
1	1	1

Функция 0100		
	0	1
0	0	1
1	0	0

Функция 0101		
	0	1
0	0	1
1	0	1

Функция 0110		
	0	1
0	0	1
1	1	0

Функция 0111		
	0	1
0	0	1
1	1	1

Функция 1000		
	0	1
0	1	0
1	0	0

Функция 1001		
	0	1
0	1	0
1	0	1

Функция 1010		
	0	1
0	1	0
1	1	0

Функция 1011		
	0	1
0	1	0
1	1	1

Функция 1100		
	0	1
0	1	1
1	0	0

Функция 1101		
	0	1
0	1	1
1	0	1

Функция 1110		
	0	1
0	1	1
1	1	0

Функция 1111		
	0	1
0	1	1
1	1	1

Классифицируем функции по номерам

- Ряд архивных (VAX-11) и современных (IBM Z390) компьютеров имеют машинные команды логических операций с тремя операндами.
- Два операнда — аргументы операции.
- Третий операнд — число от 0 до 15.
- Результат — побитовая заданная операция над операндами.

Наблюдения над таблицей

- Применение not к первому аргументу — меняются местами строки.
- Применение not к второму аргументу — меняются местами столбцы.
- Применение not к таблице — инвертируются все значения.

0000 — тривиальный ноль, 1111 — тривиальная единица

Функция 0000		
	0	1
0	0	0
1	0	0

Функция 0001		
	0	1
0	0	0
1	0	1

Функция 0010		
	0	1
0	0	0
1	1	0

Функция 0011		
	0	1
0	0	0
1	1	1

Функция 0100		
	0	1
0	0	1
1	0	0

Функция 0101		
	0	1
0	0	1
1	0	1

Функция 0110		
	0	1
0	0	1
1	1	0

Функция 0111		
	0	1
0	0	1
1	1	1

Функция 1000		
	0	1
0	1	0
1	0	0

Функция 1001		
	0	1
0	1	0
1	0	1

Функция 1010		
	0	1
0	1	0
1	1	0

Функция 1011		
	0	1
0	1	0
1	1	1

Функция 1100		
	0	1
0	1	1
1	0	0

Функция 1101		
	0	1
0	1	1
1	0	1

Функция 1110		
	0	1
0	1	1
1	1	0

Функция 1111		
	0	1
0	1	1
1	1	1

Функции, зависящие ровно от одного аргумента

Функция 0000		
	0	1
0	0	0
1	0	0

Функция 0001		
	0	1
0	0	0
1	0	1

Функция 0010		
	0	1
0	0	0
1	1	0

Функция 0011		
	0	1
0	0	0
1	1	1

Функция 0100		
	0	1
0	0	1
1	0	0

Функция 0101		
	0	1
0	0	1
1	0	1

Функция 0110		
	0	1
0	0	1
1	1	0

Функция 0111		
	0	1
0	0	1
1	1	1

Функция 1000		
	0	1
0	1	0
1	0	0

Функция 1001		
	0	1
0	1	0
1	0	1

Функция 1010		
	0	1
0	1	0
1	1	0

Функция 1011		
	0	1
0	1	0
1	1	1

Функция 1100		
	0	1
0	1	1
1	0	0

Функция 1101		
	0	1
0	1	1
1	0	1

Функция 1110		
	0	1
0	1	1
1	1	0

Функция 1111		
	0	1
0	1	1
1	1	1

Функции ровно с одной единицей

Функция 0000		
	0	1
0	0	0
1	0	0

Функция 0001		
	0	1
0	0	0
1	0	1

Функция 0010		
	0	1
0	0	0
1	1	0

Функция 0011		
	0	1
0	0	0
1	1	1

Функция 0100		
	0	1
0	0	1
1	0	0

Функция 0101		
	0	1
0	0	1
1	0	1

Функция 0110		
	0	1
0	0	1
1	1	0

Функция 0111		
	0	1
0	0	1
1	1	1

Функция 1000		
	0	1
0	1	0
1	0	0

Функция 1001		
	0	1
0	1	0
1	0	1

Функция 1010		
	0	1
0	1	0
1	1	0

Функция 1011		
	0	1
0	1	0
1	1	1

Функция 1100		
	0	1
0	1	1
1	0	0

Функция 1101		
	0	1
0	1	1
1	0	1

Функция 1110		
	0	1
0	1	1
1	1	0

Функция 1111		
	0	1
0	1	1
1	1	1

Функции с тремя единицами — отрицание предыдущих

Функция 0000		
	0	1
0	0	0
1	0	0

Функция 0001		
	0	1
0	0	0
1	0	1

Функция 0010		
	0	1
0	0	0
1	1	0

Функция 0011		
	0	1
0	0	0
1	1	1

Функция 0100		
	0	1
0	0	1
1	0	0

Функция 0101		
	0	1
0	0	1
1	0	1

Функция 0110		
	0	1
0	0	1
1	1	0

Функция 0111		
	0	1
0	0	1
1	1	1

Функция 1000		
	0	1
0	1	0
1	0	0

Функция 1001		
	0	1
0	1	0
1	0	1

Функция 1010		
	0	1
0	1	0
1	1	0

Функция 1011		
	0	1
0	1	0
1	1	1

Функция 1100		
	0	1
0	1	1
1	0	0

Функция 1101		
	0	1
0	1	1
1	0	1

Функция 1110		
	0	1
0	1	1
1	1	0

Функция 1111		
	0	1
0	1	1
1	1	1

Все функции в одной таблице

0000: $\bot$
0001: $x \wedge y$
0010: $x \wedge \overline{y}$
0011: x
0100: $\overline{x} \wedge y$
0101: y
0110: $x \oplus y$, $x \not\equiv y$.
0111: $x \vee y$
1000: $\overline{x \vee y}$, $x \downarrow y$
1001: $x \equiv y$, $x \Leftrightarrow y$
1010: $\overline{y}$
1011: $x \vee \overline{y}$
1100: $\overline{x}$
1101: $\overline{x} \vee y$, $x \Rightarrow y$
1110: $\overline{x \wedge y}$, $x \overline{\wedge} y$, $x'y$, $x|y$
1111: $\top$

Запись логических функций

Мы можем задать одну и ту же логическую функцию несколькими способами.

1. С помощью таблицы истинности.
2. С помощью комбинации логических функций. Мы уже убедились, что одна и та же функция может быть записана по-разному.
3. Векторный. $f(x, y) = (0001)$. Элементы вектора соответствуют аргументам, расположенным в *лексикографическом* порядке.

- Функции тождественны, если их таблицы истинности идентичны.

Коммутативность и ассоциативность

Определение: Для бинарной функции $\circ$ имеет место *коммутативность*, если для любых $x, y \in \{0, 1\}$ выполняется:

$$x \circ y = y \circ x.$$

Например, функции $\{\wedge, \vee, \oplus, \equiv, |, \downarrow\}$ являются коммутативными.

Определение: Для бинарной функции $\circ$ имеет место *ассоциативность*, если для любых $x, y, z \in \{0, 1\}$ выполняется:

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

Например, функции $\{\wedge, \vee, \oplus, \equiv\}$ являются ассоциативными.

Дистрибутивность

Определение: Для бинарной функций $\circ$ имеет место *дистрибутивность* относительно функции $\diamond$, если для любых $x, y, z \in \{0, 1\}$ выполняется:

$$x \circ (y \diamond z) = (x \circ y) \diamond (z \circ z).$$

Некоторые из пар, для которых выполняется дистрибутивность:
$\{\wedge, \vee\}; \{\vee, \wedge\}; \{\rightarrow, \rightarrow\}, \{\wedge, \oplus\}$

Стрелка Пирса и штрих Шеффера.

Они интересны тем, что через них можно выразить все остальные, включая одноместную.

Задача. Выразить все элементарные ФАЛ через штрих Шеффера.
Решение:

- Операция отрицания.

$$\overline{x} = \overline{x \& x} = x|x$$

- Операция конъюнкции:

$$x \& y = \overline{\overline{x \& y}} = \overline{x|y} = (x|y)|(x|y)$$

Здесь мы воспользовались формулой двойного отрицания, формулой для отрицания дизъюнкции и уже выведенной формулой для выражения отрицания через штрих Шеффера.

Выражение операций через штрих Шеффера

- Операция дизъюнкции.

$$x \vee y = \overline{\overline{x \vee y}} = \overline{\overline{x} \& \overline{y}} = \overline{x} | \overline{y} = (x|x)|(y|y)$$

- Операция импликации.

$$x \to y = \overline{\overline{\overline{x} \vee y}} = \overline{x \& \overline{y}} = x | \overline{y} = x|(y|y)$$

СКНФ и СДНФ

Введём обозначение:

$$x^\sigma = \begin{cases} x, \text{ если } \sigma = 1, \\ \overline{x}, \text{ если } \sigma = 0. \end{cases}$$

Для любой функции имеет место разложение СДНФ:

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

Для любой функции имеет место разложение СКНФ:

$$f(x_1, \ldots, x_n) = \bigwedge_{\substack{(\sigma_1,\ldots,\sigma_n) \\ f(\sigma_1,\ldots,\sigma_n)=0}} x_1^{\overline{\sigma}_1} \vee \cdots \vee x_n^{\overline{\sigma}_n}.$$

Задача на разложения

Задача Построить СКНФ и СДНФ для функции с вектором (0110).

- СДНФ. Наборы, при которых функция равна 1 — $(0,1)$ и $(1,0)$.

$$f(x,y) = (x^0 \wedge y^1) \vee (x^1 \wedge y^0) = \overline{x} \wedge y \vee x \wedge \overline{y}. \tag{30}$$

- СКНФ. Нужны наборы, при которых функция равна 0. Это $(0,0)$ и $(1,1)$.

$$f(x,y) = (x^{\overline{0}} \vee y^{\overline{0}}) \wedge (x^{\overline{1}} \vee y^{\overline{1}}) = (x \vee y) \wedge (\overline{x} \vee \overline{y}). \tag{31}$$