Определение

Булевой функцией называется функция вида

$$f : \{0,1\}^n \to \{0,1\}.$$

(Иначе говоря, булева функция сопоставляет каждому кортежу длины n из 0 и 1 одно из двух значений, 0 или 1.)

Интерпретация в логике: 0 — ложь, 1 — истина.

Основные функции:

- **Конъюнкция** (логическое "и") $x \wedge y$ (также обозн. $x \& y$, xy):
  $x \wedge y = 1 \Leftrightarrow$ оба $x = 1$ и $y = 1$
- **Дизъюнкция** (логическое "или") $x \vee y$:
  $x \vee y = 1 \Leftrightarrow$ хотя бы один из аргументов $= 1$ ($x = 1$ или $y = 1$)
- **Импликация** (логическое "следует") $x \to y$:
  $x \to y = 1 \Leftrightarrow$ верно хотя бы одно из $x = 0$ или $y = 1$
- **Симметрическая разность** (сумма по модулю 2) $x \oplus y$:
  $x \oplus y = 1 \Leftrightarrow x \neq y$
- **Отрицание** $\neg x$ (также обозн. $\overline{x}$): $\neg x = 1 \Leftrightarrow x = 0$

Представление булевых функций

Сколько всего булевых функций от n переменных? 2^{2^n}

Булеву функцию можно задать *таблицей истинности*:

x	$\neg x$
0	1
1	0

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0

Или же *вектором истинности*:

- упорядочим все 2^n кортежей в лексикографическом порядке
- i-я компонента вектора истинности равна значению функции на i-м кортеже
- какой номер у кортежа $(\sigma_1, \ldots, \sigma_n)$?

$$\Sigma_{i=1}^{n} \sigma_i 2^{n-i}$$

Например, $x \wedge y = (0001)$.

Формулы

Базис $\mathcal{F}$ — некоторое подмножество булевых функций

Определение

Формула над базисом $\mathcal{F}$ определяется по индукции.

- База: всякая функция $f \in \mathcal{F}$ является формулой над $\mathcal{F}$;
- Индуктивный переход: Если $f(x_1, \ldots, x_n)$ — формула над базисом $\mathcal{F}$, а $\Phi_1, \ldots, \Phi_n$ — либо формулы над $\mathcal{F}$, либо переменные, то тогда $f(\Phi_1, \ldots, \Phi_n)$ — формула над базисом $\mathcal{F}$.

Пример

$(x \vee y) \wedge (z \vee x)$ — формула над базисом $\{\vee, \wedge\}$

ДНФ

Обозначение для переменной x или ее отрицания $\neg x$:

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

Простой конъюнкцией называется конъюнкция одной или нескольких переменных или их отрицаний, причем каждая переменная встречается не более одного раза.

Дизъюнктивная нормальная форма (ДНФ) — представление БФ в виде дизъюнкции простых конъюнкций.

Пример: $(x \wedge \neg y) \vee z$

Если в каждой конъюнкции участвуют все переменные, это совершенная ДНФ (СДНФ).

Построение СДНФ по таблице истинности

- В таблице истинности отмечаем все наборы переменных, на которых функция равна 1.
- Для каждого такого набора $(\sigma_1, \dots, \sigma_n)$ берем конъюнкцию $(x_1^{\sigma_1} \wedge \dots \wedge x_n^{\sigma_n})$
- Включаем в СДНФ все полученные конъюнкции:

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

По построению: выражение справа принимает значение 1 $\Leftrightarrow f = 1$. Мы доказали:

Теорема

Для любой булевой функции, не равной тождественно нулю, существует СДНФ, ее задающая.

КНФ и СКНФ

Аналогично определяется и строится СКНФ:
Простой дизъюнкцией называется дизъюнкция одной или нескольких переменных или их отрицаний, причем каждая переменная встречается не более одного раза.

Конъюнктивная нормальная форма (КНФ) — представление БФ в виде конъюнкции простых дизъюнкций.

Пример: $(x \vee \neg y) \wedge z$

Если в каждой дизъюнкции участвуют все переменные, это совершенная КНФ (СКНФ).

Строится аналогично по таблице истинности:

$$f(x_1, \ldots, x_n) = \bigwedge_{f(\sigma_1, \ldots, \sigma_n) = 0} (x_1^{\neg \sigma_1} \vee \cdots \vee x_n^{\neg \sigma_n})$$

Многочлен Жегалкина

Многочлен Жегалкина: сумма по модулю 2 конъюнкций переменных (также допускается слагаемое-единица) без повторений слагаемых, а также константа 0.

Например, $f(x, y, z) = 1 \oplus x \oplus x \wedge y \wedge z$.

Общий вид:

$$f(x_1, \dots, x_n) = a \oplus \bigoplus_{\substack{1 \le i_1 < \dots < i_k \le n \\ k \in \{1, \dots, n\}}} a_{i_1 \dots i_k} \wedge x_{i_1} \wedge \dots \wedge x_{i_k},$$

где $\quad a, a_{i_1 \dots i_k} \in \{0, 1\}$.

Или, что то же самое: $f(x_1, \dots, x_n) =$

$$a \oplus a_1 x_1 \oplus \dots a_n \wedge x_n \oplus a_{12} \wedge x_1 \wedge x_2 \oplus \dots a_{1 \dots n} \wedge x_1 \wedge \dots \wedge x_n$$

Примечание: Зачастую константу 0 не считают полиномом Жегалкина, то есть в выражении допускаются только конъюнкции, сложения и константа 1.

Многочлен Жегалкина

Теорема

Для каждой функции существует единственное представление многочленом Жегалкина.

Доказательство. **Существование**. Преобразуем ДНФ:

- замена дизъюнкции: $x \vee y = x \oplus y \oplus x \wedge y$ (Д/З)
- замена отрицаний: $\neg x = x \oplus 1$
- раскрываем скобки по тождеству: $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$ (Д/З)
- сокращаются одинаковые слагаемые: $x \oplus x = 0$.

Единственность: всего многочленов Жегалкина 2^{2^n}; функций столько же — следовательно, представление единственно.