Конспект по дискретной математике

September 24, 2019

Определение. Арифметический базис — $\oplus, \wedge, 1$

Полином Жегалкина

Пример: $f(x, y, z) = (x \oplus y) \wedge (x \oplus x \wedge y \oplus 1) \leftrightarrow (x+y)(x+xy+1) = x^2+x^2y+x+xy+xy^2+y$. Можно заметить, что $x^2 = x (mod\, 2)$. $x^2 + x^2y + x + xy + xy^2 + y = x + xy + x + xy + xy = xy + y \leftrightarrow x \wedge y \oplus y$

Определение. Приведенный полином Жегалкина: $\oplus_{\alpha_1, \alpha_2 \dots \alpha_n} x_1^{\alpha_1}, x_2^{\alpha_2} \dots x_n^{\alpha_n}$

Теорема 1. Любая булева функция, кроме 0, имеет представление в виде приведенного полинома Жегалкина, и только одно.

Доказательство. Существование тривиально - любую функцию записываем в арифметическом базисе и создаем приведенный полином Жегалкина. Докажем единственность. Всего существует $2^{2^n} - 1$ функций от n аргументов, кроме 0. Кроме того, столько же существует полиномов Жегалкина от n аргументов. Если некоторой функции соответствует больше чем один полином Жегалкина, то некоторой функции не соответствует такой полином — противоречие. $\square$

Определение. Булева функция называется линейной, если в её полиноме Жегалкина не используется $\wedge$.

Примечание. От n переменных существует 2^{n+1} линейных функций.

Для 3 аргументов:

$$F_0 \quad f(0, 0 \dots, 0) = 0 - \text{всего } 2^{2^n - 1}$$
$$F_1 \quad f(1, 1 \dots, 1) = 1 - \text{всего } 2^{2^n - 1}$$
$$F_l \quad f(x_1, x_2 \dots, x_n) = \oplus_{i \in \{1 \dots n\}} x_i - \text{всего } 2^{n+1}$$
$$F_s \quad f(\neg x_1 \dots \neg x_n) = \neg f(x_1 \dots x_n) - \text{всего } 2^{2^n - 1}$$
$$F_m \quad x_1 \dots x_n, y_1 \dots y_n, x_i \leq y_i \Rightarrow f(x_1, x_2 \dots, x_n) \leq f(y_1, y_2 \dots, y_n)$$

Определение. Эти пять множеств функций называются классы Пирса

Лемма 1. *Классы Поста замкнуты относительно композиции*

Лемма 2. *Для любого класса Поста существует функция, не принадлежащая этому классу*

Доказательство. $\Uparrow$ - стрелка Пирса не принадлежит ни одному классу Поста. $\square$

Определение. Замыкание $\overline{F} = \{g\}$, где g можно записать формулой в системе связок F.

Определение. F — базис, если замыкание на нем - все булевы функции.

Теорема 2. Множество функций F является базисом базис тогда и только тогда, когда в этом классе содержатся функции всех пяти классов Поста. Другой способ записи: F - базис $\Leftrightarrow \forall i \in \{0, 1, s, m, l\}$ $F \not\subset F_i$

Доказательство. Докажем “$\Rightarrow$”. $F \subset F_i \Rightarrow^{L1} \overline{F} \subset F_i \Rightarrow^{L2} \downarrow \neq \overline{F} \rightarrow F$ — не базис.

Докажем в другую сторону.

Здесь $f_0, f_1, f_l, f_m, f_s \quad f_i \neq F_i$, то есть рассматриваются функции, не лежащие в соответствующих классах Поста.

Рассмотрим $f_0(0, 0, \ldots 0)$.

1. $f_0(1, 1, \ldots, 1) = 0$

   $f_0(x, x, \ldots, x) = \neg x$

2. $f_0(1, 1, \ldots, 1) = 1$

   $f_0(x, x, \ldots, x) = 1$

Если сделать то же самое для f_2, то получим $\neg$ и 0.

Выпишем все возможные аргументы для f_m:

$$\begin{cases} x_1 \; x_2 \; x_3 \; \ldots x_n \quad f_m(X) = 1 \\ y_1 \; x_2 \; x_3 \; \ldots x_n \quad f_m(X) = 1 \\ y_1 \; y_2 \; x_3 \; \ldots x_n \quad f_m(X) = 1 \\ \vdots \\ y_1 \; y_2 \; y_3 \; \ldots y_n \quad f_m(X) = 0 \end{cases}$$

Заметим, что для некоторого i-того набора переменных $f_m(X_i) = 0$, а $f_m(X_{i-1}) = 1$.
$f_m(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots x_n) = 1$
$f_m(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots x_n) = 0$. Зафиксируем такие x. Тогда $f_m(x_1, x_2, \ldots, x_{i-1}, x, x_{i+1}, \ldots x_n) = \neg x$

Итого, мы получили $\neg x$ из f_m

Рассмотрим f_s. $\exists x_1, x_, 2 \dots x_n f_s(x_1 \dots x_n) = f_s(\neg x_1, \dots x_n)$. С помощью этого каким-то образом получается одна из констант. Другая константа получается отрицанием.

Рассмотрим $f_l = x \wedge y \wedge z_3 \wedge z_4 \wedge \dots \wedge z_k \oplus \dots \oplus x \oplus \dots \oplus z_i \oplus \dots \oplus u_j$. Мы выбрали нелинейный член с наименьшим числом элементов, его элементы обозначили за $x, y, z_3, z_4, \dots, z_k$. Не встречающиеся в этом члене переменные обозначили за $u_1, u_2, \dots, u_j$. Если подставить вместо z_i 1, вместо u_j 0, то $f(x, y, 1, \dots, 1, 0 \dots, 0) = x \wedge y[\oplus x][\oplus y][\oplus 1] = g(x, y)$. Члены с u_j обратились в ноль.

Если в g есть $\oplus 1$, то от него можно избавиться, взяв $\neg g$. Если есть $\oplus x$ (или y), то берем $g(\not x, y)$ или наоборот. $x \wedge y \oplus x \oplus y = x \vee y$

$\square$

	сохр. 0	сохр. 1	мон.	сам.	лин.
$\wedge$	.	.	.	нет	нет
$\vee$	.	.	.	нет	нет
$\neg$	нет	нет	нет	.	.
$\wedge$	.	.	.	нет	нет
$\oplus$	.	нет	нет	нет	.
1	нет	.	.	нет	.
$\rightarrow$	нет	.	нет	нет	нет
0	.	нет	.	нет	.