

Лекция 9. Полиномы Жегалкина

Произвольная логическая функция может быть представлена в виде некоторой эквивалентной ей композиции конъюнкции и сложения по модулю 2, называемой *полиномом Жегалкина*.

Пример 1. Рассмотрим, например, логические функции

$$\begin{cases} 1 \oplus x_1 \oplus (x_1 \wedge x_2), \\ x_2 \oplus (x_1 \wedge x_3) \oplus (x_1 \wedge x_2 \wedge x_3), \end{cases}$$

которые напоминают по структуре алгебраические полиномы (многочлены) нескольких переменных, только вместо умножения в них используется конъюнкция (логическое умножение), а вместо обычного сложения – сложение mod 2. Эти функции относятся к так называемым *полиномам Жегалкина*. Однако, логические функции

$$\begin{cases} x_1 \oplus (x_2 \wedge x_2), \\ x_1 \oplus x_1 \oplus (x_1 \wedge x_2) \end{cases}$$

не входят в класс полиномов Жегалкина.

Чтобы дать формальное определение полиномов Жегалкина, введем несколько вспомогательных обозначений.

Обозначения.

$$\sum_{i=1}^n \oplus x_i \stackrel{\text{def}}{=} x_1 \oplus \cdots \oplus x_n. \quad (1)$$

Аналогично

$$\sum_{j=1}^{j_{\max}} \oplus f_j(x_{i_1}, \dots, x_{i_k}) \stackrel{\text{def}}{=} f_1(x_{i_1}, \dots, x_{i_k}) \oplus \cdots \oplus f_{j_{\max}}(x_{i_1}, \dots, x_{i_k}) \quad (k \in \mathbb{N}). \quad (2)$$

Далее будем рассматривать функции f_j определенного вида, что обозначается

$$f_j(x_{i_1}, \dots, x_{i_k}) = (x_{i_1} \wedge \cdots \wedge x_{i_k})_j \quad (k \geq 1), \quad (3)$$

для которых полагаем, что:

а) каждая из переменных x_{i_1}, \dots, x_{i_k} входит в каждую из функций $f_j(x_{i_1}, \dots, x_{i_k})$ не более чем по одному разу:

$$i_l \neq i_m \quad (1 \leq l \leq k, 1 \leq m \leq k, l \neq m) \quad (4)$$

(например, функция $f_1(x_1) = x_1 \wedge x_1$ недопустима, так как здесь $l = 1 \neq 2 = m$, но $i_l = i_1 = 1 = i_2 = i_m$);

б) все функции f_j различны между собой:

$$f_p(x_{i_1}, \dots, x_{i_k}) \neq f_s(x_{i_1}, \dots, x_{i_k}) \quad (1 \leq p \leq j_{\max}, 1 \leq s \leq j_{\max}, p \neq s) \quad (5)$$

(например, недопустима ситуация, когда $f_1(x_1, x_2) = f_2(x_1, x_2) = x_1 \wedge x_2$, так как здесь $p = 1 \neq 2 = s$, но $f_p(x_1, x_2) = f_1(x_1, x_2) = x_1 \wedge x_2 = f_2(x_1, x_2) = f_s(x_1, x_2)$).

Замечание 1. При $k = 1$ в (3) имеем $f_j(x_{i_{m_j}}) = x_{i_{m_j}}$.

Определение 1. *Полиномом Жегалкина* от n логических переменных называется полином, являющийся суммой по mod 2 некоторой константы $a \in \{0, 1\}$ и некоторых функций $f_j(x_{i_1}, \dots, x_{i_k})$ вида (3), удовлетворяющих условиям (4) и (5):

$$a \oplus \sum_{j=1}^{j_{\max}} \oplus f_j(x_{i_1}, \dots, x_{i_k}) = a \oplus \sum_{j=1}^{j_{\max}} \oplus (x_{i_1} \wedge \dots \wedge x_{i_k})_j,$$

где

$$\begin{cases} j_{\max} \in \mathbb{N}, \\ k \in \mathbb{N}, \\ m \in \mathbb{N}, \\ 1 \leq m \leq k, \\ i_m \in \mathbb{N}, \\ 1 \leq i_m \leq n. \end{cases}$$

Пример 2. Докажем, что

$$\bar{x} = 1 \oplus x. \quad (6)$$

Доказательство.

Таблица 1

x	\bar{x}	$1 \oplus x$
0	1	1
1	0	0

Упражнение 1 (д/з). Доказать:

$$x \vee y = x \oplus y \oplus (x \wedge y). \quad (7)$$

Доказательство.

Таблица 2

x	y	$x \vee y$	$x \oplus y$	$x \wedge y$	$x \oplus y \oplus (x \wedge y)$
0	0	0	0	0	0
0	1	1	1	0	1
1	0	1	1	0	1
1	1	1	0	1	1

Замечание 2. Известно, что любую композицию логических функций всегда можно представить в виде полинома Жегалкина, причем единственным образом. Для этого нужно:

1) заменить логические функции на соответствующие эквивалентные функции, являющиеся полиномами Жегалкина (см. (6), (7)),

2) произвести упрощения в полученной формуле, используя следующие свойства функций \wedge (см. лекции) и \oplus :

Группа I.

1. $x \wedge y = y \wedge x$;
2. $x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge y \wedge z$;
3. $x \wedge x = x$;
4. $x \wedge 0 = 0$;
5. $x \wedge 1 = x$.

Группа II.

1. $x \oplus y = y \oplus x$;
2. $(x \oplus y) \oplus z = x \oplus (y \oplus z) = x \oplus y \oplus z$;
3. $x \oplus x = 0$;
4. $x \oplus 0 = x$.

Группа III.

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

(8)

Результат операций 1)–2) и будет полиномом Жегалкина для данной композиции.

Замечание 3. Соотношения (8) легко проверить табличным способом.

Пример 3. Проверим соотношение II.3 из (8).

Решение.

Таблица 3

x	$x \oplus x$
0	0
1	0

Упражнение 2 (д/з). Проверить другие соотношения из (8).

Пример 4. Представить в виде полинома Жегалкина функцию $f(x, y) = \bar{x} \oplus (x \vee y)$.

Решение. $f(x, y) \stackrel{(6),(7)}{=} 1 \oplus x \oplus x \oplus y \oplus (x \wedge y) \stackrel{(8):II.3}{=} 1 \oplus 0 \oplus y \oplus (x \wedge y) \stackrel{(8):II.4}{=} 1 \oplus y \oplus (x \wedge y)$.

Упражнение 3 (д/з). Представить в виде полинома Жегалкина функцию $f(x, y) = (x \vee \bar{y}) \oplus (\bar{x} \vee y)$.

Теорема (без док-ва). *Любая логическая функция может быть представлена в виде полинома Жегалкина и притом единственным образом.*

Замечание 4. Полином Жегалкина также можно найти методом неопределенных коэффициентов. Рассмотрим этот метод на следующем примере.

Пример 5. Представить в виде полинома Жегалкина функцию двух переменных, заданную таблицей 4.

Таблица 4

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

Решение. Полином Жегалкина для функции двух переменных ищем в следующем виде:

$$f(x, y) = a_0 \oplus a_1 \wedge x \oplus a_2 \wedge y \oplus a_3 \wedge x \wedge y, \quad (9)$$

где $a_i \in \{0, 1\}$, $i = 0, \dots, 3$. Очевидно, если $a_i = 0$, то соответствующее слагаемое фактически не входит в полином, а если $a_i = 1$, то входит.

Для определения коэффициентов полинома нужно подставить значения неизвестных и соответствующее значение функции в (9) согласно таблице 4. Последовательно подставляя все возможные наборы значений переменных в (9), получим:

$$\begin{cases} (0, 0) : 0 = a_0 \oplus a_1 \wedge 0 \oplus a_2 \wedge 0 \oplus a_3 \wedge 0 \wedge 0 \Rightarrow a_0 = 0; \\ (0, 1) : 1 = 0 \oplus a_1 \wedge 0 \oplus a_2 \wedge 1 \oplus a_3 \wedge 0 \wedge 1 \Rightarrow a_2 = 1; \\ (1, 0) : 1 = 0 \oplus a_1 \wedge 1 \oplus 1 \wedge 0 \oplus a_3 \wedge 1 \wedge 0 \Rightarrow a_1 = 1; \\ (1, 1) : 0 = 0 \oplus 1 \wedge 1 \oplus 1 \wedge 1 \oplus a_3 \wedge 1 \wedge 1 \Rightarrow a_3 = 0. \end{cases}$$

Подставляя в (9) найденные значения коэффициентов, получим искомым полином Жегалкина для данной функции: $f(x, y) = x \oplus y$.

Замечание 6. Сравним результат примера 5 и упражнения 3. Для комбинации функций и эквивалентной ей функции, заданной табличным способом, мы получаем один и тот же полином Жегалкина, что согласуется с утверждением теоремы о его единственности.

Упражнение 4 (д/з). Представить в виде полинома Жегалкина функцию двух переменных, заданную таблицей 5.

Таблица 5

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

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

Замечание 7. Результат примера 4 и упражнения 4 совпадают аналогично замечанию 6.