Лекция 4. Полиномы Жегалкина. Теорема Жегалкина. Быстрый способ построения полинома Жегалкина. Полные системы.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте https://mk.cs.msu.ru

Монотонные элементарные конъюнкции

Элементарная конъюнкция, не содержащая отрицаний переменных, называется **монотонной** (ЭК), или **мономом**, или **одночленом**.

Например, 1, x_2, $x_1x_2x_4$ — монотонные ЭК.

Полиномы Жегалкина

Полиномом (или **многочленом**) **Жегалкина** длины l, $l \geqslant 1$, назовем сумму по модулю два l различных монотонных ЭК.

Полиномом (или **многочленом**) **Жегалкина** длины 0 назовем константу 0.

Другими словами, полиномом Жегалкина называется выражение вида

$$K_1 \oplus \ldots \oplus K_l,$$

где K_j — различные монотонные ЭК, $l \geqslant 1$, или константа 0.

Например, 0, 1, $x_1x_2 \oplus x_1$, $x_2 \oplus x_3 \oplus 1$, $x_1x_2 \oplus x_1 \oplus x_3$ — полиномы Жегалкина.

Считаем, что два полинома Жегалкина совпадают, если они отличаются только порядком входящих в них монотонных ЭК.

Каждый полином Жегалкина с переменными $x_1, \ldots, x_n$ определяет какую-то функцию $f(x_1, \ldots, x_n) \in P_2^{(n)}$.

Полином Жегалкина

Теорема 4.1 (И. И. Жегалкина). *Каждая функция* $f(x_1, \ldots, x_n) \in P_2$ *может быть единственным образом представлена в виде полинома Жегалкина* P_f.

Полином Жегалкина

Доказательство. 1. Существование. Применим полиномиальное разложение функции $f(x_1, \ldots, x_n)$ по всем n переменным:

$$f(x_1, \ldots, x_n) = \bigoplus_{\sigma \in E_2^n} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma).$$

Затем пользуясь тождеством $x^\sigma = x \oplus \sigma \oplus 1$ везде в правой части заменим выражение $x_i^{\sigma_i}$ на выражение $x_i \oplus \sigma_i \oplus 1$.

Далее по правилам коммутативности и ассоциативности $\&$ и $\oplus$ и дистрибутивности вида $x(y \oplus z) = xy \oplus xz$ перемеожим все скобки.

После этого приведем подобные слагаемые по правилам $x \oplus x = 0$, $x \oplus 0 = x$.

В итоге получим полином Жегалкина, который представляет исходную функцию f.

Полином Жегалкина

Доказательство. 2. Единственность. Покажем, что число полиномов Жегалкина над переменными $x_1, \ldots, x_n$ совпадет с числом функций из $P_2^{(n)}$.

Монотонных элементарных конъюнкций над переменными $x_1, \ldots, x_n$ всего найдется 2^n, т. к. каждая переменная x_i, $i = 1, \ldots, n$, может либо входить, либо не входить в такую монотонную ЭК.

Далее, полиномов Жегалкина над переменными $x_1, \ldots, x_n$ всего найдется 2^{2^n}, т. к. каждая из 2^n монотонных ЭК может либо входить, либо не входить в такой полином Жегалкина.

Значит, учитывая п. 1, каждая функция f из $P_2^{(n)}$ может быть представлена ровно одним полиномом Жегалкина над переменными $x_1, \ldots, x_n$.

□

Построение полиномов Жегалкина

По теореме Жегалкина для каждой функции $f \in P_2$ найдется единственный полином Жегалкина, который ее задает.

Если задана функция $f \in P_2$, то как можно построить ее полином Жегалкина?

Рассмотрим несколько способов построения:

1) метод **из доказательства** теоремы;

2) метод **неопределенных коэффициентов**;

3) **быстрый способ**.

Метод из доказательства теоремы

Пример. По методу из **доказательства теоремы** найдем полином Жегалкина для функции $f(x_1, x_2) = x_1 \vee x_2$:

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	1

Найдем полиномиальное разложение функции f по всем переменным:

$$f(x_1, x_2) = \bar{x}_1 x_2 \oplus x_1 \bar{x}_2 \oplus x_1 x_2.$$

Метод из доказательства теоремы

Пример (продолжение). Теперь везде заменим выражение $\bar{x}$ на выражение $x \oplus 1$ и выполним преобразования:

$$\begin{aligned} f(x_1, x_2) &= \bar{x}_1 x_2 \oplus x_1 \bar{x}_2 \oplus x_1 x_2 = \\ &= (x_1 \oplus 1) x_2 \oplus x_1 (x_2 \oplus 1) \oplus x_1 x_2 = \\ &= (x_1 x_2 \oplus x_2) \oplus (x_1 x_2 \oplus x_1) \oplus x_1 x_2 = \\ &= x_1 x_2 \oplus x_1 \oplus x_2. \end{aligned}$$

Получаем полином Жегалкина функции f:

$$f(x_1, x_2) = x_1 x_2 \oplus x_1 \oplus x_2.$$

Метод неопределенных коэффициентов

Пример. Методом **неопределенных коэффициентов** найдем полином Жегалкина для функции $f(x_1, x_2) = x_1 \vee x_2$:

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	1

Запишем ее полином Жегалкина с неопределенными коэффициентами:

$$f(x_1, x_2) = c_{1,2}x_1x_2 \oplus c_1x_1 \oplus c_2x_2 \oplus c_0,$$

где $c_{1,2}, c_1, c_2, c_0 \in E_2$ — неизвестные коэффициенты.

Метод неопределенных коэффициентов

Пример (продолжение). Подставляя поочередно все наборы из E_2^2 в левую и правую части полученного равенства, составляем систему линейных уравнений с неизвестными $c_{1,2}, c_1, c_2, c_0$:

$$\begin{cases} f(0,0) = c_0 = 0, \\ f(0,1) = c_2 \oplus c_0 = 1, \\ f(1,0) = c_1 \oplus c_0 = 1, \\ f(1,1) = c_{1,2} \oplus c_1 \oplus c_2 \oplus c_0 = 1. \end{cases}$$

Решаем полученную систему и находим:

$$c_{1,2} = 1, \ c_1 = 1, \ c_2 = 1, \ c_0 = 0.$$

Получаем полином Жегалкина функции f:

$$f(x_1, x_2) = x_1 x_2 \oplus x_1 \oplus x_2.$$

Полином Жегалкина

Если $f \in P_2^{(n)}$, то ее полином Жегалкина P_f однозначно определяется своими коэффициентами при всех возможных монотонных ЭК над переменными $x_1, \ldots, x_n$.

Монотонные ЭК над $x_1, \ldots, x_n$

Набору $\alpha \in E_2^n$, $n \geqslant 2$, **взаимно однозначно сопоставим** монотонную ЭК над переменными $x_1, \ldots, x_n$:

$$x^\alpha = \begin{cases} 1, & \alpha = (0, \ldots, 0), \\ \prod\limits_{\alpha_i = 1} x_i, & \alpha \neq (0, \ldots, 0). \end{cases}$$

Будем говорить, что набор $\alpha \in E_2^n$ и монотонная ЭК x^α соответствуют друг другу.

Монотонные ЭК над $x_1, \ldots, x_n$

Если α пробегает по всем возможным наборам из E_2^n, то x^α перечисляет все возможные монотонные ЭК над $x_1, \ldots, x_n$.

Например, если $n = 2$, то

$$x^\alpha = \begin{cases} 1, & \alpha = (0,0), \\ x_2, & \alpha = (0,1), \\ x_1, & \alpha = (1,0), \\ x_1 x_2, & \alpha = (1,1). \end{cases}$$

Коэффициенты полинома Жегалкина

Пусть $c_f(\alpha)$ обозначает **коэффициент** при мономе x^α, $\alpha \in E_2^n$, в полиноме Жегалкина функции $f \in P_2^{(n)}$.

Тогда

$$f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in E_2^n} c_f(\alpha) \cdot x^\alpha.$$

Для нахождения полинома Жегалкина функции f нужно найти коэффициенты $c_f(\alpha)$ для всех $\alpha \in E_2^n$.

Вычисление коэффициентов при $n = 1$

Если $f(x) \in P_2^{(1)}$, то

$$\begin{aligned} f(x) &= \bar{x} \cdot f(0) \oplus x \cdot f(1) = (x \oplus 1) \cdot f(0) \oplus x \cdot f(1) = \\ &= x \cdot f(0) \oplus f(0) \oplus x \cdot f(1) = (f(0) \oplus f(1)) \cdot x \oplus f(0). \end{aligned}$$

Поэтому

$$\begin{aligned} c_f(0) &= f(0), \\ c_f(1) &= f(0) \oplus f(1). \end{aligned}$$

Например, если $f(x) = \bar{x}$, то

$$\begin{aligned} c_f(0) &= f(0) = 1, \\ c_f(1) &= f(0) \oplus f(1) = 1 \oplus 0 = 1. \end{aligned}$$

Поэтому

$$\bar{x} = c_f(1) \cdot x \oplus c_f(0) \cdot 1 = x \oplus 1.$$

Вычисление коэффициентов полинома Жегалкина

Теорема 4.2 (вычисление коэффициентов). *Если* $n \geqslant 1$, $f(y, x_1, \ldots, x_n) \in P_2^{(n+1)}$, $f_a(x_1, \ldots, x_n) = f(a, x_1, \ldots, x_n)$, *где* $a \in E_2$, *то для каждого* $\alpha \in E_2^n$ *верны равенства:*

$$c_f(0, \alpha_1, \ldots, \alpha_n) = c_{f_0}(\alpha),$$
$$c_f(1, \alpha_1, \ldots, \alpha_n) = c_{f_0}(\alpha) \oplus c_{f_1}(\alpha).$$

Вычисление коэффициентов полинома Жегалкина

Доказательство. Применим полиномиальное разложение функции $f(y, x_1, \ldots, x_n)$ по переменной y:

$$\begin{aligned} f(y, x_1, \ldots, x_n) &= \bar{y} \cdot f(0, x_1, \ldots, x_n) \oplus y \cdot f(1, x_1, \ldots, x_n) = \\ &= \bar{y} \cdot f_0 \oplus y \cdot f_1 = (y \oplus 1) \cdot f_0 \oplus y \cdot f_1 = \\ &= y \cdot f_0 \oplus f_0 \oplus y \cdot f_1 = y \cdot (f_0 \oplus f_1) \oplus f_0. \end{aligned}$$

Но

$$\begin{aligned} f_0 &= \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha, \\ f_1 &= \bigoplus_{\alpha \in E_2^n} c_{f_1}(\alpha) \cdot x^\alpha. \end{aligned}$$

Вычисление коэффициентов полинома Жегалкина

Доказательство. Поэтому:

$$f = y \cdot \left(\bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha \oplus \bigoplus_{\alpha \in E_2^n} c_{f_1}(\alpha) \cdot x^\alpha \right) \oplus \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha.$$

Значит,

$$f = \bigoplus_{\alpha \in E_2^n} (c_{f_0}(\alpha) \oplus c_{f_1}(\alpha)) \cdot y \cdot x^\alpha \oplus \bigoplus_{\alpha \in E_2^n} c_{f_0}(\alpha) \cdot x^\alpha.$$

Перепишем следующим образом:

$$f = \bigoplus_{(1,\alpha) \in E_2^{n+1}} (c_{f_0}(\alpha) \oplus c_{f_1}(\alpha)) \cdot (y^1 \cdot x^\alpha) \oplus \bigoplus_{(0,\alpha) \in E_2^{n+1}} c_{f_0}(\alpha) \cdot (y^0 \cdot x^\alpha).$$

Вычисление коэффициентов полинома Жегалкина

Итак,

$$f = \bigoplus_{(1,\alpha)\in E_2^{n+1}} (c_{f_0}(\alpha) \oplus c_{f_1}(\alpha)) \cdot (y^1 \cdot x^\alpha) \oplus \bigoplus_{(0,\alpha)\in E_2^{n+1}} c_{f_0}(\alpha) \cdot (y^0 \cdot x^\alpha).$$

Из полученного выражения находим:

$$c_f(0, \alpha_1, \ldots, \alpha_n) = c_{f_0}(\alpha),$$
$$c_f(1, \alpha_1, \ldots, \alpha_n) = c_{f_0}(\alpha) \oplus c_{f_1}(\alpha).$$

□

Быстрый способ

Пример. Пользуясь формулами предыдущей теоремы, найдем полином Жегалкина функции $f(x_1, x_2, x_3)$:

x_1	x_2	x_3	f
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

Быстрый способ

Пример (продолжение). На шаге 1 вычисляем коэффициенты полиномов Жегалкина всех подфункций $f_\sigma(x_3)$, $\sigma \in E_2^2$, функции $f(x_1, x_2, x_3)$ по переменным x_1, x_2:

x_1	x_2	x_3	f	1
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	0

Быстрый способ

Пример (продолжение). На шаге 2, пользуясь полученными значениями на шаге 1, вычисляем коэффициенты полиномов Жегалкина всех подфункций $f_\delta(x_2, x_3)$, $\delta \in E_2^1$, функции $f(x_1, x_2, x_3)$ по переменной x_1:

x_1	x_2	x_3	f	1	2
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	1

Быстрый способ

Пример (продолжение). Наконец, на шаге 3, пользуясь полученными значениями на шаге 2, вычисляем коэффициенты полиномов Жегалкина функции $f(x_1, x_2, x_3)$:

x_1	x_2	x_3	f	1	2	$3(c_f)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	0	1	0

Быстрый способ

Пример (продолжение).

x_1	x_2	x_3	f	1	2	$3(c_f)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	1	1	1	1
1	0	0	0	0	0	0
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	0	1	0

Получаем:

$$f(x_1, x_2, x_3) = x_2x_3 \oplus x_1x_3 \oplus x_1x_2.$$

Полная система

Пусть $A \subseteq P_2$. Множество A называется **полной системой**, если формулами над A можно выразить любую функцию алгебры логики.

Полнота системы $\{x \cdot y, x \oplus y, 1\}$

Предложение 4.1. *Система* $A = \{x \cdot y, x \oplus y, 1\}$ *является полной*.

Доказательство. Рассмотрим произвольную функцию $f \in P_2$.

1. Если $f = 0$, то $f = x \oplus x$.

2. Если $f \neq 0$, то представим f ее полиномом Жегалкина.

□

Литература к лекции

1. Алексеев В. Б. Лекции по дискретной математике. М.: Инфра-М, 2012.

2. Марченков С. С. Основы теории булевых функций. М.: Физматлит, 2014.

3. Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2001.

4. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.