Лекция 2. Полиномы. Теорема о представлении функций k-значной логики полиномами по модулю k. Полнота в P_k. Теорема о полноте системы Поста. Функция Вебба.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Моном

Выражение вида

$$x_{i_1}^{s_1} \cdot \ldots \cdot x_{i_r}^{s_r},$$

где все переменные различны, $s_1, \ldots, s_r \geqslant 1$, назовем **мономом** (или **одночленом**) ранга r, $r \geqslant 1$.

Мономом (или **одночленом**) ранга 0 назовем константу 1.

Мономы считаются совпадающими, если они отличаются только порядком своих сомножителей.

Полином по модулю k

Выражение вида

$$c_1 K_1 + \ldots + c_l K_l,$$

где $K_1, \ldots, K_l$ — различные мономы, $c_1, \ldots, c_l \in E_k \setminus \{0\}$ — коэффициенты, назовем **полиномом** (или **многочленом**) по модулю k длины l, $l \geqslant 1$.

Полиномом (или **многочленом**) по модулю k длины 0 назовем константу 0.

Полиномы по модулю k

Теорема 1 (о представлении k-значных функций полиномами по модулю k) *Пусть $k \geqslant 2$. Каждая функция $f(x_1, \ldots, x_n) \in P_k$ может быть представлена полиномом по модулю k тогда и только тогда, когда k — простое число.*

Полиномы

Доказательство. 1. Сначала рассмотрим случай, когда k — простое число. Пусть $f(x_1, \ldots, x_n) \in P_k$.

Запишем ее во 2-й форме:

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

Заметим, что $j_i(x) = j_0(x - i)$ при $i \in E_k$, поэтому:

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in E_k^n} j_0(x_1 - \sigma_1) \cdot \ldots \cdot j_0(x_n - \sigma_n) \cdot f(\sigma).$$

Полиномы по модулю k

Доказательство. Если k — простое число, то по малой теореме Ферма верно $a^{k-1} = 1 (\mathrm{mod}\ k)$ при $1 \leqslant a \leqslant k-1$.

Поэтому $j_0(x) = 1 - x^{k-1}$, а значит,

$$f = \sum_{\sigma \in E_k^n} (1 - (x_1 - \sigma_1)^{k-1}) \cdot \ldots \cdot (1 - (x_n - \sigma_n)^{k-1}) \cdot f(\sigma).$$

Затем перемножаем скобки по свойствам дистрибутивности, коммутативности и ассоциативности, далее приводим подобные слагаемые. Получим полином по модулю k для функции f.

Значит, существование полинома по модулю k для каждой k-значной функции при простых k доказано.

Полиномы по модулю k

Доказательство. 2. Теперь рассмотрим случай, когда k — составное число. Значит, $k = k_1 \cdot k_2$, где $1 < k_1 \leqslant k_2 < k$.

Докажем от обратного, что в этом случае функция $j_0(x) \in P_k$ не задается никаким полиномом по модулю k.

Полиномы по модулю k

Доказательство. Предположим, что функция $j_0(x)$ задается полиномом по модулю k:

$$j_0(x) = c_s x^s + c_{s-1} x^{s-1} + \ldots + c_1 x + c_0,$$

где $c_s, c_{s-1}, \ldots, c_1, c_0 \in E_k$ — коэффициенты, $c_s \neq 0$.
Тогда $j_0(0) = c_0 = 1$ и

$$j_0(k_1) = c_s {k_1}^s + c_{s-1} {k_1}^{s-1} + \ldots + c_1 k_1 + 1 = 0.$$

Поэтому

$$k_1 \cdot (c_s k_1^{s-1} + c_{s-1} k_1^{s-2} + \ldots + c_1) = k - 1 (\mathrm{mod}\ k).$$

Число k_1 — делитель числа k, поэтому для того, чтобы равенство выполнялось по модулю k, число $k - 1$ обязано делиться на k_1, где $k_1 > 1$. Приходим к противоречию.

Значит, при составных k никакой полином по модулю k не задает функцию $j_0(x)$.

□

Полиномиальные функции

Функции

$$
\begin{aligned}
&x,\\
&\bar{x} = x + 1,\\
&\sim x = (k-1) - x = (k-1)x + (k-1),\\
&-x = k - x = (k-1)x,\\
&x + y,\\
&x - y = x + (k-1)y,\\
&x \cdot y,\\
&x^s
\end{aligned}
$$

являются полиномиальными при всех k — и простых, и составных.

Неполиномиальные функции

Функции

$$j_i(x),\ i \in E_k,$$
$$J_i(x),\ i \in E_k,$$
$$\min(x, y),$$
$$\max(x, y),$$
$$x \dot{-} y,$$
$$x \to y$$

являются полиномиальными при простых k и не являются полиномиальными при всех составных k (покажем далее).

Полиномы по модулю k

Множество всех k-значных функций, представимых полиномами по модулю k, обозначим $Polyn_k$.

Следствие 1.1.
Если k — простое число, то $Polyn_k = P_k$; если k — составное число, то $Polyn_k \neq P_k$.

Вопросы:

Как найти полином по модулю k для заданной k-значной функции, если k — простое число?

Как выяснить, задается ли полиномом по модулю k заданная k-значная функция, если k — составное число?

Если k — простое число

Способы построения полиномов k-значных функций при простых k:

1) метод из доказательства теоремы — по 2-й форме;

2) метод **неопределенных коэффициентов**.

Если k — простое число

Пример. Пусть $f(x) = 4J_2(x) + 3J_3(x) \in P_5$:

x	f
0	0
1	0
2	1
3	2
4	0

По 2-й форме найдем для функции f полином по модулю 5.

Запишем функцию f во 2-й форме:

$$f(x) = j_2(x) + 2 \cdot j_3(x).$$

Если k — простое число

Пример (продолжение). Далее получаем:

$$\begin{aligned} f(x) &= j_2(x) + 2 \cdot j_3(x) = j_0(x-2) + 2j_0(x-3) = \\ &= (1-(x-2)^4) + 2 \cdot (1-(x-3)^4). \end{aligned}$$

Применим тождество:

$$\begin{aligned} (x+y)^4 &= x^4 + 4x^3y + x^2y^2 + 4xy^3 + y^4 (\mathrm{mod}\ 5) = \\ &= x^4 - x^3y + x^2y^2 - xy^3 + y^4 (\mathrm{mod}\ 5). \end{aligned}$$

Находим:

$$1-(x-2)^4 = 1-(x^4+2x^3+4x^2+3x+1) = 4x^4+3x^3+x^2+2x,$$
$$1-(x-3)^4 = 1-(x^4-2x^3+4x^2-3x+1) = 4x^4+2x^3+x^2+3x.$$

Поэтому

$$\begin{aligned} f(x) &= (4x^4+3x^3+x^2+2x) + 2 \cdot (4x^4+2x^3+x^2+3x) = \\ &= 2x^4+2x^3+3x^2+3x. \end{aligned}$$

Значит,

$$f(x) = 2x^4+2x^3+3x^2+3x.$$

Если k — составное число

Если k — составное число, то можно применять метод **неопределенных коэффициентов** для проверки, представима ли заданная k-значная функция полиномом по модулю k.

Если k — составное число

Пример. Пусть $f(x) = j_1(x) + j_2(x) \in P_4$:

x	f
0	0
1	1
2	1
3	0

Методом неопределенных коэффициентов проверим, задается ли функция f полиномом по модулю 4.

Если k — составное число

Пример (продолжение). Сначала построим таблицу степеней x^s по модулю 4:

x	x^2	x^3	x^4
0	0	0	0
1	1	1	1
2	0	0	0
3	1	3	1

Т. к. $x^4 = x^2$, степени в полиноме по модулю 4 можно записывать только до третьей.

Если k — составное число

Пример (продолжение). Предположим, что функция $f(x)$ задается полиномом по модулю 4, т. е. пусть

$$f(x) = ax^3 + bx^2 + cx + d,$$

где $a, b, c, d \in E_4$ — неизвестные коэффициенты.

Для нахождения коэффициентов составим систему уравнений, последовательно подставляя все значения из E_4 в левую и правую части равенства:

$$\begin{cases} f(0) = d = 0, \\ f(1) = a + b + c + d = 1, \\ f(2) = 2c + d = 1, \\ f(3) = 3a + b + 3c + d = 0. \end{cases}$$

Если k — составное число

Пример (продолжение). Из первого и третьего уравнения получаем:

$$2c = 1.$$

Подставляя все возможные значения $c \in E_4$, выясняем, что это равенство не выполняется ни при каких $c \in E_4$:

$$2 \cdot 0 = 0,\ 2 \cdot 1 = 2,\ 2 \cdot 2 = 0,\ 2 \cdot 3 = 2.$$

Следовательно, система не имеет решений (по модулю 4), поэтому функция $f(x) = j_1(x) + j_2(x)$ не может быть представлена полиномом по модулю 4, т. е. $f \notin Polyn_4$.

Если k — составное число

Пример. Пусть $f(x) = 2 \cdot j_0(x) \in P_4$:

x	f
0	2
1	0
2	0
3	0

Проверим, задается ли функция f полиномом по модулю 4.

Если k — составное число

Пример (продолжение). Пусть

$$f(x) = ax^3 + bx^2 + cx + d,$$

где $a, b, c, d \in E_4$ — неизвестные коэффициенты.

Составляем систему уравнений:

$$\begin{cases} g(0) = d = 2, \\ g(1) = a + b + c + d = 0, \\ g(2) = 2c + d = 0, \\ g(3) = 3a + b + 3c + d = 0. \end{cases}$$

Если k — составное число

Пример (продолжение). Из первого и третьего уравнения получаем:

$$2c = 2,$$

и $c = 1$ — одно из решений этого уравнения. Тогда

$$\begin{cases} a + b = 1, \\ 3a + b = 3, \end{cases}$$

и $a = 1$, $b = 0$ — одно из решений этой системы уравнений.

Следовательно, функция $f(x)$ может быть представлена полиномом по модулю 4, т. е. $f \in Polyn_4$, и найден один из ее полиномов по модулю 4:

$$f(x) = 2 \cdot j_0(x) = x^3 + x + 2.$$

Полная система

Пусть $A \subseteq P_k$ — множество k-значных функций.

Множество A называется **полной системой**, если формулами над A можно выразить любую функцию из P_k.

Полные системы

Примеры полных систем.

1. $\{0, 1, \ldots, k-1, J_0(x), J_1(x), \ldots, J_{k-1}(x), \max(x, y), \min(x, y)\}$ — система 1-й формы.

2. $\{0, 1, \ldots, k-1, j_0(x), j_1(x), \ldots, j_{k-1}(x), x + y, x \cdot y\}$ — система 2-й формы.

3. $\{0, 1, \ldots, k-1, x + y, x \cdot y\}$ при простых k — система полиномов.

Система Поста

Теорема 2. *Пусть* $k \geqslant 3$. *Система Поста* $\{\bar{x}, \max(x, y)\}$ *является полной системой в* P_k.

Доказательство. Выразим формулами над системой Поста все функции из системы 1-й формы.
1. Построение констант.

$\bar{x} = x + 1$; $(x + 1) + 1 = x + 2$; $\ldots$; $(x + (k - 1)) + 1 = x$. Тогда

$$\max(x, x + 1, x + 2, \ldots, x + (k - 1)) = k - 1.$$

Далее $(k - 1) + 1 = 0$; $0 + 1 = 1$; $1 + 1 = 2$; $\ldots$;
$(k - 2) + 1 = k - 1$.
Т. е. все константы получены.

Система Поста

Доказательство. **2**. Построение $J_a(x)$, $a \in E_k$.
Проверим, что

$$J_a(x) = 1 + \max_{t \neq (k-1)-a} (x + t).$$

Пусть $b \in E_k$.
Если $b = a$, то

$$k - 1 = J_a(a) = 1 + \max_{t \neq (k-1)-a} (a + t) = 1 + (k - 2) = k - 1.$$

Если $b \neq a$, то

$$0 = J_a(b) = 1 + \max_{t \neq (k-1)-a} (b + t) = 1 + (k - 1) = 0.$$

Т. е. все $J_a(x)$, $a \in E_k$, получены.

Система Поста

.

Доказательство. 3. Построение $\min(x, y)$.
Рассмотрим функции $g_{a,c}(x) = c \cdot j_a(x)$, где $a, c \in E_k$.
Проверим, что

$$g_{a,c}(x) = (c+1) + \max(J_a(x), (k-1) - c).$$

Пусть $b \in E_k$.
Если $b = a$, то

$$c = c \cdot j_a(a) = (c+1) + \max(J_a(a), (k-1) - c) = (c+1) + (k-1) = c.$$

Если $b \neq a$, то

$$0 = c \cdot j_a(b) = (c+1) + \max(J_a(b), (k-1) - c) = (c+1) + (k-1) - c = 0.$$

Система Поста

.

Доказательство. Тогда можно построить каждую функцию $f(x) \in P_k^{(1)}$, т. к.

$$f(x) = \max(g_{0,f(0)}(x), g_{1,f(1)}(x), \ldots, g_{k-1,f(k-1)}(x)).$$

Действительно, для каждого значения $b \in E_k$ верно

$$\begin{aligned} f(b) &= \max(g_{0,f(0)}(b), \ldots, g_{b,f(b)}(b), \ldots, g_{k-1,f(k-1)}(b)) = \\ &= \max(0, \ldots, 0, f(b), 0, \ldots, 0) = f(b). \end{aligned}$$

В частности, получена функция $f(x) =\sim x$.
Тогда

$$\min(x, y) =\sim \max(\sim x, \sim y).$$

Т. е. функция $\min(x, y)$ получена.

Все функции системы 1-й формы можно выразить формулами над функциями системы Поста. Значит, система Поста полна.
□

Функция Вебба

Следствие 2.1. *Пусть $k \geqslant 3$. Множество, состоящее из одной функции Вебба $V_k(x, y) = \max(x, y) + 1$, является полной системой в P_k.*

Доказательство. Выразим через функцию Вебба все функции системы Поста:

$$\bar{x} = V_k(x, x) = \max(x, x) + 1 = x + 1,$$
$$\max(x, y) = V_k(x, y) + \underbrace{1 + \ldots + 1}_{k-1}.$$

□

Неполиномиальность максимума

Следствие 2.2. *Если k — составное число, то* $\max(x, y) \notin Polyn_k$.

Доказательство проведем от обратного.
Предположим, что при некотором составном k верно $\max(x, y) \in Polyn_k$.
Но $\bar{x} = x + 1 \in Polyn_k$, поэтому $\{\bar{x}, \max(x, y)\} \subseteq Polyn_k$.
Система Поста полна в P_k, следовательно, получаем, что каждая функция из P_k задается полиномом по модулю k при этом составном k — противоречие.
Значит, $\max(x, y) \notin Polyn_k$.

□

Бесконечные полные системы в P_k

Следствие 2.3. *При $k \geqslant 3$ из каждой бесконечной полной в P_k системы можно выделить конечную полную подсистему*.

Доказательство. Пусть $A \subseteq P_k$ — бесконечная полная система.
Т. к. система A — полна, в ней найдутся функции такие $f_1, \ldots, f_t$, что функция Вебба $V_k(x, y)$ выражается формулой над ними.
Тогда подсистема $B = \{f_1, \ldots, f_t\} \subseteq A$ полна в P_k.

□

Литература к лекции

1. Алексеев В. Б. Лекции по дискретной математике. М.: Инфра-М, 2012. С. 24–25.

2. Марченков С. С. Избранные главы дискретной математики. М.: МАКС Пресс, 2016. С. 11–12, 14–16.

3. Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2001. С. 43–45, 48, 69–71.

4. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004. Гл. III 1.11, 1.12, 2.7, 2.12.