

Функции k -значных логик. Теоремы о представимости функций k -значных логик 1-й и 2-й формами. Теорема о представимости функций k -значных логик полиномами по модулю k .

Селезнева Светлана Николаевна
selezn@cs.msu.ru

факультет ВМК МГУ имени М.В. Ломоносова

Функции k -значной логики

Пусть $E_k = \{0, 1, \dots, k - 1\}$, где $k \geq 2$.

Функция $f(x_1, \dots, x_n)$, $n \geq 1$, называется **функцией k -значной логики**, или **k -значной функцией**, если

$$f : E_k^n \rightarrow E_k.$$

Множество всех функций k -значной логики обозначим P_k .

Функции k -значной логики

Некоторые функции k -значной логики:

$n = 1$:

- 1) константы $0, 1, \dots, k - 1$;
- 2) x — тождественно равная x ;
- 3) характеристические функции $J_i(x), j_i(x)$, где $i \in E_k$:

$$J_i(x) = \begin{cases} k - 1, & x = i, \\ 0, & x \neq i, \end{cases} \quad j_i(x) = \begin{cases} 1, & x = i, \\ 0, & x \neq i. \end{cases}$$

Функции k -значной логики

$n = 2$:

1) $x + y$, $x - y$, $x \cdot y$ — сложение, вычитание и умножение по модулю k ;

2) $\min(x, y) = \begin{cases} x, & x \leq y, \\ y, & x > y, \end{cases}$ — минимум из x и y ;

3) $\max(x, y) = \begin{cases} x, & x \geq y, \\ y, & x < y, \end{cases}$ — максимум из x и y .

1-я форма

Теорема (о 1-й форме). Пусть $k \geq 2$. При $n \geq 1$ каждая функция $f(x_1, \dots, x_n) \in P_k$ может быть представлена в виде:

$$f(x_1, \dots, x_n) = \max_{\sigma \in E_k^n} \min (J_{\sigma_1}(x_1), \dots, J_{\sigma_n}(x_n), f(\sigma)).$$

Доказательство. Рассмотрим произвольный набор $\alpha \in E_k^n$ и подставим его в левую и правую части равенства из утверждения теоремы:

$$f(\alpha) = \max_{\sigma \in E_k^n} \min (J_{\sigma_1}(\alpha_1), \dots, J_{\sigma_n}(\alpha_n), f(\sigma)).$$

1-я форма

Доказательство. Набор σ пробегает все значения из множества E_k^n , а набор α — какой-то набор из E_k^n .

1. Если $\sigma \neq \alpha$, то найдется такое i , $1 \leq i \leq n$, что $\sigma_i \neq \alpha_i$.
Значит, $J_{\sigma_i}(\alpha_i) = 0$, откуда в этом случае:

$$\min(J_{\sigma_1}(\alpha_1), \dots, J_{\sigma_{i-1}}(\alpha_{i-1}), 0, J_{\sigma_{i+1}}(\alpha_{i+1}), \dots, J_{\sigma_n}(\alpha_n), f(\sigma)) = 0.$$

2. Если $\sigma = \alpha$, то для всех i , $i = 1, \dots, n$, верно $\sigma_i = \alpha_i$, а значит, $J_{\sigma_i}(\alpha_i) = k - 1$. Поэтому в этом случае:

$$\min(k - 1, \dots, k - 1, f(\alpha)) = f(\alpha).$$

Следовательно,

$$f(\alpha) = \max(0, \dots, 0, f(\alpha), 0, \dots, 0) = f(\alpha).$$

1-я форма

Пример. Рассмотрим функцию $f(x) = \bar{x} \in P_3$:

x	f
0	1
1	2
2	0

Представим ее в 1-й форме:

$$\begin{aligned} f(x) &= \max(\min(J_0(x), f(0)), \min(J_1(x), f(1)), \min(J_2(x), f(2))) = \\ &= \max(\min(J_0(x), 1), \min(J_1(x), 2), \min(J_2(x), 0)) = \\ &= \max(\min(J_0(x), 1), J_1(x)). \end{aligned}$$

2-я форма

Теорема (о 2-й форме) Пусть $k \geq 2$. При $n \geq 1$ каждая функция $f(x_1, \dots, x_n) \in P_k$ может быть представлена в виде:

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

Доказательство повторяет доказательство предыдущего утверждения.

2-я форма

Пример. Рассмотрим функцию $f(x) = J_2(x + x^2) \in P_4$:

x	x^2	$x + x^2$	f
0	0	0	0
1	1	2	3
2	0	2	3
3	1	0	0

Представим ее во 2-й форме:

$$\begin{aligned} f(x) &= j_0(x) \cdot f(0) + j_1(x) \cdot f(1) + j_2(x) \cdot f(2) + j_3(x) \cdot f(3) = \\ &= j_0(x) \cdot 0 + j_1(x) \cdot 3 + j_2(x) \cdot 3 + j_3(x) \cdot 0 = 3j_1(x) + 3j_2(x). \end{aligned}$$

1-я и 2-я формы

Пример. Рассмотрим функцию $f(x, y) = \min(x^2, y) \in P_3$
($f(x, y)$ указано на пересечении строки x и столбца y):

$x \setminus y$	0	1	2
0	0	0	0
1	0	1	1
2	0	1	1

1-я форма для f :

$$f(x, y) = \max(\min(J_1(x), J_1(y), 1), \min(J_1(x), J_2(y), 1), \min(J_2(x), J_1(y), 1), \min(J_2(x), J_2(y), 1)).$$

2-я форма для f :

$$f(x, y) = j_1(x)j_1(y) + j_1(x)j_2(y) + j_2(x)j_1(y) + j_2(x)j_2(y).$$

Полином по модулю k

Выражение вида

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

где $s_1, \dots, s_k \geq 1$, или константу 1 назовем **мономом** (или **одночленом**).

Выражение вида

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

где K_1, \dots, K_l — мономы, $c_1, \dots, c_l \in E_k$ — коэффициенты, назовем **полиномом** (или **многочленом**) по модулю k .

Полиномы по модулю k

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

Полиномы по модулю k

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

Запишем ее во 2-й форме:

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

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

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

Полиномы по модулю k

Доказательство. Если k — простое число, то по малой теореме Ферма верно $a^{k-1} = 1 \pmod{k}$ при $1 \leq a \leq k-1$.

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

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

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 $1 < k_1 \leq k_2 < k$.

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 :

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

где $c_s, c_{s-1}, \dots, c_1, c_0 \in E_k$ — коэффициенты, $c_s \neq 0$.

Тогда $j_0(0) = c_0 = 1$ и

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

Поэтому

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

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 $j_0(x)$.

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