Лекция 21. Функции k-значной логики. Таблицы значений. Представление функций k-значной логики в 1-й и 2-й формах. Представление функций k-значной логики полиномами по модулю k.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Функции k-значной логики

Пусть $E_k = \{0, 1, \ldots, k-1\}$, где $k \geqslant 2$ — целое число.

Функцией k-значной логики (или **k-значной функцией**) называем произвольное отображение из E_k^n в E_k, $n \geqslant 1$.

Т. е. если $f : E_k^n \to E_k$, то f — *n-местная функция k-значной логики*.

При этом если $f = f(x_1, \ldots, x_n)$, то говорим, что f — функция n переменных $x_1, \ldots, x_n$.

Иногда константы $0, 1, \ldots, k-1$ считаем 0-*местными функциями k-значной логики* (функциями без переменных).

Функции алгебры логики

Множество всех функций k-значной логики, зависящих от n переменных, обозначим $P_k^{(n)}$.

Множество всех функций k-значной логики обозначаем P_k, т. е. $P_k = \bigcup\limits_{n \geqslant 1} P_k^{(n)}$.

При $k \geqslant 3$ функции k-значной логики называются **функциями многозначной логики**.

Таблицы значений

Функции k-значной логики можно задавать таблицами значений.

Упорядочим все наборы множества E_k^n в *лексико-графическом*, или *алфавитном* порядке (в алфавите $0, 1, \ldots, k-1$), сопоставим каждому набору значение функции на нем.

x_1	$\ldots$	x_{n-1}	x_n	$f(x_1, \ldots, x_{n-1}, x_n)$
0	$\ldots$	0	0	$f(0, \ldots, 0, 0)$
0	$\ldots$	0	1	$f(0, \ldots, 0, 1)$
	$\ldots$			
0	$\ldots$	0	$k-1$	$f(0, \ldots, 0, k-1)$
	$\ldots$			
$k-1$	$\ldots$	$k-1$	0	$f(k-1, \ldots, k-1, 0)$
	$\ldots$			
$k-1$	$\ldots$	$k-1$	$k-2$	$f(k-1, \ldots, k-1, k-2)$
$k-1$	$\ldots$	$k-1$	$k-1$	$f(k-1, \ldots, k-1, k-1)$

Функции k-значной логики

Рассмотрим некоторые важные k-значные функции:

1. $n = 0$: **константы** $0, 1, \ldots, k-1$.

2. $n = 1$:

1) x — **тождественно равная** x;

2) **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

3. $n = 2$:

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

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

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

4. обобщения:

1) $\min(x_1, x_2, \ldots, x_n) = \min(x_1, \min(x_2, \ldots, x_n))$;

2) $\max(x_1, x_2, \ldots, x_n) = \max(x_1, \max(x_2, \ldots, x_n))$;

3) $x^s = \underbrace{x \cdot \ldots \cdot x}_{s}$ — степень, $s \geqslant 1$.

Функции k-значной логики

Каким функциям алгебры (двузначной) логики соответствуют функции k-значной логики при $k \geqslant 3$?

n	$P_k, k \geqslant 3$	P_2
$n = 0$	$0, 1, \ldots, k-1$	$0, 1$
$n = 1$	x	x
	$J_0(x), j_0(x)$	$\bar{x}$
	$J_{k-1}(x), j_{k-1}(x)$	x
$n = 2$	$\min(x, y)$	$x \& y$
	$\max(x, y)$	$x \vee y$
	$x + y$	$x \oplus y$
	$x \cdot y$	$x \cdot y$

Функции k-значной логики

В k-значной логике аналогично двузначной логике вводятся понятия существенной и несущественной переменных, равенства функций с точностью до несущественных переменных; понятия формулы над множеством функций и функции, определяемой формулой.

Число k-значных функций n переменных

Предложение 21.1. *Пусть* $k \geqslant 2$*. При* $n \geqslant 1$ *верно равенство:* $|P_k^{(n)}| = k^{k^n}$.

Доказательство.

Каждую функцию $f(x_1, \ldots, x_n) \in P_k^{(n)}$ можно задать таблицей с k^n строками.

В каждой строке этой таблицы — значение этой функции на соответствующем наборе из k возможных значений из E_k.

При этом разные таблицы определяют различные функции.

Поэтому $|P_k^{(n)}| = k^{k^n}$.

$\square$

1-я форма

Теорема 21.1 (о 1-й форме). *Пусть $k \geqslant 2$. При $n \geqslant 1$ каждая функция $f(x_1, \ldots, x_n) \in P_k$ может быть представлена в виде:*

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

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

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

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, $1 \leqslant i \leqslant n$, что $\sigma_i \neq \alpha_i$. Значит, $J_{\sigma_i}(\alpha_i) = 0$, откуда в этом случае:

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

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

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

Следовательно,

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

$\square$

1-я форма

Пример. Рассмотрим функцию $f(x) = x + 1 \in P_3$:

x	f
0	1
1	2
2	0

Представим ее в 1-й форме:

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

2-я форма

Теорема 21.2 (о 2-й форме) *Пусть* $k \geqslant 2$. *При* $n \geqslant 1$ *каждая функция* $f(x_1, \dots, x_n) \in P_k$ *может быть представлена в виде:*

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

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:

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

2-я форма для f:

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

Моном

Выражение вида

$$x_{i_1}^{s_1} \cdot \ldots \cdot x_{i_m}^{s_m},$$

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

Мономом 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 по модулю k длины 0 назовем константу 0.

Полиномы по модулю k

Теорема 21.3 (о представлении k-значных функций полиномами по модулю k) *Пусть $k \geqslant 2$. 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

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 $j_0(x)$. □

Полиномы по модулю k

Вопросы:

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

Как проверить, можно ли записать полиномом по модулю k заданную k-значную функцию, если k — составное число?

Если k — простое число

Методы 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:

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

Находим:

$$\begin{aligned} 1-(x-2)^4 = 1-(x^4+2x^3+4x^2+3x+1) = 4x^4+3x^3+x^2+2x, \\ 1-(x-3)^4 = 1-(x^4-2x^3+4x^2-3x+1) = 4x^4+2x^3+x^2+3x. \end{aligned}$$

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, можно ли записать заданную k-значную функцию 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.

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). 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.

Составляем систему уравнений:

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

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, и найден один из ее полиномов по модулю 4:

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

Задачи для самостоятельного решения

1. Докажите теорему 21.2.

2. Представьте в 1-й и 2-й формах функцию $f \in P_k$, если
1) $k = 6$, $f(x) = J_0(x^2 - x)$;
2) $k = 3$, $f(x, y) = x \cdot y$.

3. Найдите полином по модулю k для функции $f \in P_k$, если
1) $k = 5$, $f(x) = \min(x^2, x^3)$;
2) $k = 3$, $f(x, y) = \min(x^2, y)$.

4. Проверьте, можно ли представить полиномом по модулю k функцию $f \in P_k$, если
1) $k = 4$, $f(x) = j_0(x) + j_2(x)$;
2) $k = 6$, $f(x) = j_0(x) + j_2(x)$;
3) k — любое составное число, $f = \max(x, y) + \min(x, y)$;
4) k — любое составное число, $f = (\max(x, y) - \min(x, y))^2$.

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, 20121. С. 11–12, 14–121.
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.