Лекция 2. Функции k-значной логики. Формулы. Нормальные формы: 1-я и 2-я формы, полиномы по модулю k. Полнота.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Формула

Пусть $A \subseteq P_k$, причем каждая функция из A имеет свое, отличное от других функций, обозначение.
Формула над множеством A определяется по индукции.

1. *Базис индукции*. Если x — переменная, то выражение x — формула.

2. *Индуктивный переход*. Если f — обозначение m-местной функции из A и $F_1, \ldots, F_m$ — уже построенные формулы или переменные (не обязательно различные), то выражение $f(F_1, \ldots, F_m)$ — формула.

3. Других формул нет, т. е. каждая формула построена либо по базису индукции, либо по индуктивному переходу.

Формулы

Пример. Пусть $A = \{0, 1, \ldots, k-1, x, \bar{x}, \sim x, -x, x^s\} \subseteq P_5$.
Тогда:

$F_1 = x$	формула по базису индукции для переменной x;
$F_2 = x^2$	формула по индуктивному переходу для функции $x^2 \in A$ и уже построенной формулы F_1;
$F_3 = 3$	формула по индуктивному переходу для функции $3 \in A$;
$F_4 = 3 \cdot x^2$	формула по индуктивному переходу для функции $x \cdot y \in A$ и уже построенных формул F_3, F_2;
$F_5 = \sim (3 \cdot x^2)$	формула по индуктивному переходу для функции $\sim x \in A$ и уже построенной формулы F_4;
	и т. д.

Функция, определяемая формулой

Каждая формула над множеством $A \subseteq P_k$ задает некоторую *k-значную функцию*.

Функция f_F, задаваемая формулой F, определяется по индукции.

1. *Базис индукции*. Если $F = x$, где x — переменная, то $f_F(x) = x$, т. е. функция f_F тождественно равна переменной x.

2. *Индуктивный переход*. Если $F = f(F_1, \ldots, F_m)$, где f — обозначение m-местной функции из A и $F_1, \ldots, F_m$ — формулы или переменные, причем формула F_i определяет функцию $f_{F_i}(x_1, \ldots, x_1)$ (возможно, зависящую не от всех переменных существенно), $i = 1, \ldots, m$, то

$$f_F(x_1, \ldots, x_n) = f(f_{F_1}(x_{1,1}, \ldots, x_{1,n_1}), \ldots, f_{F_m}(x_{m,1}, \ldots, x_{m,n_m})).$$

Здесь пользуемся тем, что f обозначает какую-то функцию из A.

Функции, определяемые формулами

Пример. Найдем функцию $f_{F_5}(x) \in P_5$, которая задается формулой F_5:

x	x^2	$3 \cdot x^2$	$\sim (3 \cdot x^2)$
0	0	0	4
1	1	3	1
2	4	2	2
3	4	2	2
4	1	3	1

Функция f_{F_5}, определяемая формулой F_5, записана в самом правом столбце.

Тождественные формулы

Формулы F_1 и F_2 называются **эквивалентными**, или **тождественными**, если они определяют равные функции, т. е. функции f_{F_1} и f_{F_2} равны.
Обозначение тождественных формул: $F_1 = F_2$

Верны следующие свойства:
1) коммутативность связок $\cdot, +, \min, \max$;
2) ассоциативность связок $\cdot, +, \min, \max$;
3) дистрибутивность умножения относительно сложения:

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

И многие другие.

Доказательство тождеств

Примеры.

1. Докажем тождество: $-(\bar{x}) = \sim x$.

$$-(\bar{x}) = -(x+1) = (k-1) - x = \sim x.$$

2. Докажем тождество: $\sim \max(\sim x, \sim y) = \min(x, y)$.

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

$$= (k-1) - \begin{cases} (k-1) - x, & (k-1) - x \geqslant (k-1) - y, \\ (k-1) - y, & (k-1) - x < (k-1) - y, \end{cases} =$$

$$= \begin{cases} x, & x \leqslant y, \\ y, & x > y, \end{cases} = \min(x, y).$$

1-я форма

Теорема 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,

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

1-я форма

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

x	f
0	1
1	2
2	0

Запишем 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 2 (о 2-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:*

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

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

Запишем 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:

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

Моном

Выражение вида

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

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

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 3 (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

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

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

Неполиномиальные функции

Функции

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

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

Полиномы по модулю k

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

Следствие 3.1.
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 — составное число

Если k — составное число, то можно применять метод **неопределенных коэффициентов** для проверки, задается 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.

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, и найден один из ее полиномов по модулю 4:

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

Замыкание множества

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

Замыканием $[A]$ множества A называется множество всех функций, выразимых формулами над множеством A.

Если $A = [A]$, то множество A называется **замкнутым классом**.

Примеры: P_k, $Polyn_k$.

Полные системы

Если $[A] = P_k$, то множество A называется **полной системой**.

Примеры.
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 4. *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 $J_i(x)$, $i \in E_k$.
Проверим, что

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

Если $x = i$, то

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

Если $x \neq i$, то

$$0 = J_i(x) = 1 + \max_{t \neq (k-1)-i}(x + t) = 1 + (k - 1) = 0.$$

Т. е. все $J_i(x)$, $i \in E_k$, получены.

Система Поста

.

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

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

Если $x = i$, то

$$a = a \cdot j_i(i) = (a+1) + \max(J_i(i), (k-1) - a) = (a+1) + (k-1) = a.$$

Если $x \neq i$, то

$$0 = a \cdot j_i(x) = (a+1) + \max(J_i(x), (k-1) - a) = (a+1) + (k-1) - a = 0.$$

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 4.1. *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 4.2. *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 4.3. *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 $g_1, \ldots, g_t$, что функция Вебба $V_k(x, y)$ выражается формулой над ними.
Тогда подсистема $A' = \{g_1, \ldots, g_t\} \subseteq A$ 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.