Лекция 15. Функции конечно-значных логик. Элементарные функции k-значной логики. Способы задания функций k-значной логики: таблицы, формулы, I-я и II-я формы, полиномы. Полнота.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по “Избранным вопросам дискретной математики”.
3-й курс, группа 318,
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mathcyb.cs.msu.su

Конечнозначные функции

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$.
Функция $f(x_1, \ldots, x_n)$ называется k-**значной**, если

$$f^n : E_k^n \to E_k,$$

где $n = 1, 2, \ldots$.

Множество всех k-значных функций обозначим как P_k, множество всех k-значных функций, зависящих от переменных $x_1, \ldots, x_n$, обозначим как P_k^n.

При $k = 2$ функции называются **булевыми**, при $k \geq 3$ – многозначными.

Аналогично булеву случаю равенство k-значных функций $(k \geq 3)$ рассматривается с точностью до несущественных (фиктивных) переменных.

Конечнозначные функции

Переменная x_i называется **существенной** для функции $f(x_1, \ldots, x_n) \in P_k$, если найдутся такие элементы $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in E_k$, что

$$\varphi(x_i) = f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n) \neq Const.$$

Переменная x_i является существенной, если все другие переменные можно так зафиксировать, полученная новая функция одной этой переменной принимает хотя бы два различных значения.

Переменная, не являющаяся существенной, называется **несущественной**, или **фиктивной**.
Фиктивные переменные можно удалять и добавлять.

Конечнозначные функции

Функции f и g называются **равными**, если при помощи конечного числа удалений или добавлений фиктивных переменных они их можно сделать совпадающими.

Функции f и g называются **конгруэнтными**, если равные им функции осуществляют одинаковые отображения, т.е. отличаются только именами переменных.

Примеры.

1. Функции $f_1(x) = 0$ и $f_2 = 0$ – равны.

2. Функции $g(x) = x$ и $h(y) = y$ – конгруэнтны.

Таблицы значений

Как можно задавать k-значные функции?
1. Таблицы значений. Упорядочим все наборы множества E_k^n в **лексико-графическом**, или **алфавитном** порядке (в алфавите $0, 1, \dots, k-1$), сопоставим каждому набору – значение функции на нем.

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

Таблицы значений

Теорема 1. *Пусть* $k \geq 2$. *При* $n \geq 1$ *верно* $|P_k^n| = k^{k^n}$.

Доказательство.
Для каждой функции $f(x_1, \ldots, x_n) \in P_k^n$ – в ее таблице k^n строк.
В каждой строке вне зависимости от других строк – ее значение на этом наборе из k возможных.
Откуда $|P_k^n| = k^{k^n}$.

$\square$

Элементарные функции

2. Формулы.

Элементарные k-значные функции ($k \geq 3$).

$\mathbf{n = 0}$:

константы $0, 1, \ldots, k-1$.

$\mathbf{n = 1}$:

x	x	$\bar{x}$	$\sim x$	$-x$
0	0	1	$k-1$	0
1	1	2	$k-2$	$k-1$
$\ldots$				
$k-2$	$k-2$	$k-1$	1	2
$k-1$	$k-1$	0	0	1

x – тождественно x;

$\bar{x} = x + 1 (\mathrm{mod}\ k)$ – отрицание Поста x;

$\sim x = (k-1) - x$ – отрицание Лукасевича x;

$-x = k - x (\mathrm{mod}\ k)$ – минус x.

Элементарные функции

Характеристические функции выделенного значения $J_i(x)$, $j_i(x)$, $i = 0, 1, \ldots, k-1$:

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

$$j_i(x) = \begin{cases} 1, & x = i; \\ 0, & x \neq i. \end{cases}$$

Элементарные функции

n = 2:

$x + y (\mathrm{mod}\ k)$, $x - y (\mathrm{mod}\ k)$, $x \cdot y (\mathrm{mod}\ k)$ – сложение, вычитание и умножение по модулю k;

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

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

$x \dot{-} y = \begin{cases} x - y, & x \geq y; \\ 0, & x < y. \end{cases}$ – усеченная разность;

$x \supset y = \begin{cases} k - 1, & x \leq y; \\ (k-1) - (x - y), & x > y. \end{cases}$ – импликация.

обобщения:

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

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

$x^m = \underbrace{x \cdot \cdots \cdot x}_{m}$ – степень.

Элементарные функции

Как булевы функции обобщаются на многозначные функции?

n	P_2	$P_k,\ k \geq 3$	пояснения
$n = 0$	$0,\ 1$	$0,\ 1,\ \ldots,\ k-1$	константы
$n = 1$	x	x	тождественная функция
	$\bar{x}$	$\bar{x},\ \sim x$	отрицание
$n = 2$	$x \& y$	$\min(x, y)$	конъюнкция или минимум
	$x \vee y$	$\max(x, y)$	дизъюнкция или максимум
	$x \oplus y$	$x + y \pmod{k}$	сложение по модулю k
	$x \to y$	$x \supset y$	импликация

В связи с расширением исходного множества значений появляются элементарные функции, не имеющие явного элементарного прообраза в булевом случае: $-x$, $J_i(x)$, $j_i(x)$, $x \dot{-} y$.

Формулы

Понятия **формулы** и **функции, реализуемой формулой**, вводятся аналогично булеву случаю.
Пусть $A \subseteq P_k$.
Формула над множеством A определяется по индукции.
1. Базис индукции. Если $f^n \in A$ – n-местная функция и $u_1, \ldots, u_n$ – набор из n произвольных имен переменных, то выражение $f(u_1, \ldots, u_n)$ – формула.
2. Индуктивный переход. Если $F_1, \ldots, F_n$ – уже построенные формулы или имена переменных и $f^n \in A$ – n-местная функция, то выражение $f(F_1, \ldots, F_n)$ – формула.
3. Других формул нет, т.е. каждая формула или построена по по базису индукции, или построена по индуктивному переходу.

Формулы

Пример. Пусть $A \subseteq P_5$ – множество элементарных функций. Тогда

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

Формулы

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

Функция f_F, реализуемая формулой F, определяется по индукции.

1. Базис индукции. Если $F = u$, где u – имя переменной, то $f_F = u$, т.е. функция f_F тождественно равна переменной u.

2. Индуктивный переход. Если $F = f(F_1, \ldots, F_n)$, где $F_1, \ldots, F_n$ – формулы или имена переменных и $f^n \in A$, то $f_F = f(f_{F_1}, \ldots, f_{F_n})$.

Формулы

Пример. Найдем функцию $f_{F_4}(x) \in P_5$, которая реализуется формулой F_4:

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

Функция f_{F_4}, реализуемая формулой F_4, записана в самом правом столбце.

Эквивалентные формулы

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

Верны следующие эквивалентности:
1) коммутативность связок $\cdot, +, \min, \max$;
2) ассоциативность связок $\cdot, +, \min, \max$;
3) дистрибутивность $(x + y) \cdot z = x \cdot z + y \cdot z$.
И многие другие.

Эквивалентные формулы

Примеры.

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

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

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

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

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

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

I-я форма

Теорема 2 (о I-й форме). *Пусть $k \geq 2$. Каждая k-значная функция $f(x_1, \ldots, x_n) \in P_k$ может быть задана формулой вида:*

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

Доказательство.
Рассмотрим произвольный набор $\alpha = (a_1, \ldots, a_n) \in E_k^n$. Тогда

$$f(a_1, \ldots, a_n) = \max_{(\sigma_1,\ldots,\sigma_n)\in E_k^n} \min\left(J_{\sigma_1}(a_1), \ldots, J_{\sigma_n}(a_n), f(\sigma_1, \ldots, \sigma_n)\right) =$$

$$= \max(0, \ldots, 0, f(a_1, \ldots, a_n), 0, \ldots, 0) = f(a_1, \ldots, a_n).$$

$\square$

I-я форма

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

x	f
0	1
1	2
2	0

Найдем ее I-ю форму:

$$f(x) = \max(\min(J_0(x), f(0)), \min(J_1(x), f(1)), \min(J_2(x), f(2))) =$$

$$= \max(\min(J_0(x), 1), \min(J_1(x), 2), \min(J_2(x), 0)) =$$

$$= \max(\min(J_0(x), 1), J_1(x)).$$

II-я форма

Теорема 3 (о II-й форме) *Пусть $k \geq 2$. Каждая k-значная функция $f(x_1, \ldots, x_n) \in P_k$ может быть задана формулой вида:*

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

II-я форма

Пример. Пусть $g(x) = J_2(x + x^2) \in P_4$:

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

Найдем ее II-ю форму:

$$g(x) = j_0(x) \cdot g(0) + j_1(x) \cdot g(1) + j_2(x) \cdot g(2) + j_3(x) \cdot g(3) =$$

$$= j_0(x) \cdot 0 + j_1(x) \cdot 3 + j_2(x) \cdot 3 + j_3(x) \cdot 0 = 3j_1(x) + 3j_2(x).$$

Полиномы

Формула вида

$$x_{i_1}^{m_1} \cdot \ldots \cdot x_{i_r}^{m_r},$$

где все переменные попарно различны и $m_1, \ldots, m_r \geq 1$, называется **мономом**.

Число его сомножителей r, $r \geq 1$, называется его **рангом**, сумма степеней его сомножителей $d = \sum\limits_{i=1}^{r} m_i$, $d \geq 1$, называется его **степенью**.

По определению будем считать константу 1 мономом ранга $r = 0$ и степени $d = 0$.

Полиномы

Формула вида

$$c_1X_1 + \dots + c_lX_l,$$

где X_i – попарно различные мономы и $c_i \in E_k \setminus \{0\}$ – коэффициенты, $i = 1, \dots, l$, называется **полиномом по модулю k**.

Число l, $l \geq 1$, его слагаемых X_i называется его **длиной**.

По определению будем считать константу 0 (пустым) полиномом по модулю k с длиной $l = 0$.

Будем полагать, что в полином можно добавлять слагаемые с нулевыми коэффициентами. Примем, что полученное выражение (формулу) будем также называть полиномом. Такой полином будем считать совпадающим с полиномом без всех слагаемых с нулевыми коэффициентами.

Полиномы

Теорема 4 (о задании k-значных функций полиномами)
Пусть $k \geq 2$. Каждая k-значная функция $f(x_1, \ldots, x_n) \in P_k$ задается полиномом по модулю k тогда и только тогда, когда k – простое число.

Полиномы

Доказательство.
Пусть $f(x_1, \ldots, x_n) \in P_k$. Запишем ее во II-й форме:

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

Заметим, что $j_\sigma(x) = j_0(x - \sigma)$. Тогда

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

Полиномы

Доказательство.

1. Если k – простое число, то по малой теореме Ферма $a^{k-1} = 1 (\mathrm{mod}\ k)$ при $1 \leq a \leq k-1$.
Тогда $j_0(x) = 1 - x^{k-1}$ и

$$f(x_1, \ldots, x_n) =$$

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

Затем перемножаем скобки по свойствам дистрибутивности, коммутативности и ассоциативности; приводим подобные слагаемые. Получим полином по модулю k для функции $f(x_1, \ldots, x_n)$.
Существование полинома по модулю k для каждой k-значной функции при простых k доказано.

Полиномы

Доказательство.
2. Пусть k – составное число. Тогда $k = k_1 \cdot k_2$, где $k_1 \geq k_2 > 1$. Докажем от противного, что в этом случае функция $j_0(x)$ не задается полиномом по модулю k.

Полиномы

Доказательство.
Пусть функция $j_0(x)$ задается полиномом по модулю k:

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

$c_s, c_{s-1}, \ldots, c_1, c_0 \in E_k$ – коэффициенты, $c_s \neq 0$.
Тогда

$$j_0(0) = c_0 = 1;$$

$$j_0(k_2) = c_s k_2^s + c_{s-1}k_2^{s-1} + \cdots + c_1 k_2 + 1 = 0.$$

Откуда

$$k_2 \cdot (c_s k_2^{s-1} + c_{s-1}k_2^{s-2} + \cdots + c_1) = k - 1 (\mathrm{mod}\ k).$$

Т.к. число k_2 – делитель числа k, число $k-1$ обязано делиться на $k_2 > 1$ – противоречие.
Т.е. при составных k никакой полином по модулю k не задает функцию $j_0(x)$. $\square$

Полиномы

Элементарные 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 значениях k – и простых, и составных.

Полиномы

Элементарные функции

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

являются полиномиальными при простых k и НЕ ЯВЛЯЮТСЯ полиномиальными при всех составных k (будет доказано далее).

Полиномы

Множество всех k-значных функций, задающихся полиномами по модулю k, обозначается как Pol_k.

Следствие 4.1.
Если k – простое число, то $Pol_k = P_k$;
если k – составное число, то $Pol_k \neq P_k$.

Вопросы:
Как строить полиномы для k-значных функций при простых k?
Как выяснить, задается ли полиномом заданная k-значная функция, если k – составное?

Если k – простое число

Методы построения полиномов k-значных функций при простых k:

1. метод из доказательства теоремы 4 – по II-й форме;
2. метод **неопределенных коэффициентов**;
3. **быстрый** метод.

Если k – простое число

Теорема 5 (о выражении коэффициентов полинома функции через ее значения) *Пусть* $k \geq 2$ *– простое число,* $f(x) \in P_k^1$*, и*

$$f(x) = c_{k-1}x^{k-1} + \cdots + c_1 x + c_0,$$

где $c_{k-1}, \ldots, c_1, c_0 \in E_k$*. Тогда*

$$\begin{aligned} c_0 &= f(0); \\ c_i &= -\sum_{j=1}^{k-1} f(j) j^{k-1-i}, \ i = 1, \ldots, k-2; \\ c_{k-1} &= -\sum_{j=0}^{k-1} f(j). \end{aligned}$$

Если k – простое число

Доказательство. По теореме 3 о II-й форме, малой теореме Ферма и по свойству $C_{k-1}^i = (-1)^i (\mathrm{mod}\ k)$, если k – простое число, получаем:

$$\begin{aligned} f(x) &= \sum_{j=0}^{k-1} f(j) \cdot j_i(x) = \sum_{j=0}^{k-1} f(j)(1-(x-j)^{k-1}) = \\ &= f(0)(1-x^{k-1}) - \sum_{j=1}^{k-1} f(j) \sum_{i=1}^{k-1} C_{k-1}^i x^i (-j)^{k-1-i} = \\ &= f(0)(1-x^{k-1}) - \sum_{i=1}^{k-1} x^i \sum_{j=1}^{k-1} f(j) j^{k-1-i}. \end{aligned}$$

$\square$

Если k – простое число

Пример. Построим быстрым методом полином для функции $f(x) = \max(x, 2x) \in P_3$:

x	f
0	0
1	2
2	2

Тогда $f(x) = c_2x^2 + c_1x + c_0$, и

$$\begin{aligned} c_0 &= f(0) = 0; \\ c_1 &= -(f(1)1^1 + f(2)2^1) = -(2 + 2 \cdot 2) = 0; \\ c_2 &= -(f(0) + f(1) + f(2)) = -(0 + 2 + 2) = 2. \end{aligned}$$

Откуда

$$f(x) = 2x^2.$$

Если k – составное число

Если k – составное число, то можно применять метод **неопределенных коэффициентов** для выяснения, задается ли данная k-значная функция полиномом по модулю k.

Если k – составное число

Примеры.
1. Пусть $f(x) = J_1(x) + J_2(x) \in P_4$.
Выясним, задается ли функция $f(x) \in P_4$ полиномом по модулю 4 **методом неопределенных коэффициентов**.
Предположим, что функция $f(x)$ задается полиномом по модулю 4.
Сначала построим таблицу степеней x^m:

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

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

Если k – составное число

Тогда
$$f(x) = ax^3 + bx^2 + cx + d,$$
где $a, b, c, d \in E_4$ – неизвестные коэффициенты.
Для определения коэффициентов составим систему уравнений по значениям данной функции $f(x) = J_1(x) + J_3(x) \in P_4$:

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

Если k – составное число

Из первого и третьего уравнения получаем:

$$2c = 3.$$

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

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

Следовательно, система не имеет решений (по модулю 4), и

$$f(x) = J_1(x) + J_2(x) \notin Pol_4.$$

Если k – составное число

2. Пусть $g(x) = 2(J_1(x) + J_2(x)) \in P_4$.
Аналогично, выясним, задается ли функция $g(x) \in P_4$ полиномом по модулю 4.
Тогда

$$g(x) = a'x^3 + b'x^2 + c'x + d',$$

где $a', b', c', d' \in E_4$ – неизвестные коэффициенты.
Составляем систему уравнений:

$$\begin{aligned} g(0) &= d' = 0; \\ g(1) &= a' + b' + c' + d' = 2; \\ g(2) &= 2c' + d' = 2; \\ g(3) &= 3a' + b' + 3c' + d' = 0. \end{aligned}$$

Если k – составное число

Из первого и третьего уравнения получаем:

$$2c' = 2, \; c' = 1.$$

Тогда

$$\begin{aligned} a' + b' &= 1; \\ 3a' + b' &= 1. \end{aligned}$$

Откуда

$$a' = 0, \; b' = 1.$$

Следовательно, функция $g(x)$ задается полиномом по модулю 4, и один из ее полиномов по модулю 4

$$g(x) = 2(J_1(x) + J_2(x)) = x^2 + x \in Pol_4.$$

Операция замыкания

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

Замыканием множества A называется множество всех функций, реализуемых формулами над множеством A. Обозначение: $[A]$.

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

Примеры: $\emptyset$, P_k, Pol_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 Россера-Туркетта.
2. $\{0, 1, \ldots, k-1, j_0(x), j_1(x), \ldots, j_{k-1}(x), x+y, x \cdot y\}$ – система II-й формы.
3. $\{0, 1, \ldots, k-1, x+y, x \cdot y\}$, если k – простое число, – система полиномов.

Система Поста

Теорема 6. *Пусть $k \geq 3$. Система Поста* $\{\bar{x}, \max(x, y)\}$ *является полной системой в* P_k.

Доказательство. Построим формулами на системой Поста все функции из системы Россера-Туркетта.

1. Построение констант.

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

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

Откуда $(k - 1) + 1 = 0$; $0 + 1 = 1$; $1 + 1 = 2$; $\ldots$; $(k - 2) + 1 = k - 1$.

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

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

Все $J_i(x)$, $i \in E_k$, получены.

Система Поста

.

Доказательство.

3. Построение $\min(x, y)$.

Проверим, что

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

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 получена каждая функция $f(x) \in P_k^1$, так как

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

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

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

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

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

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

Функция $\min(x, y)$ получена.
Все функции системы Россера-Туркетта построены формулами над функциями системы Поста. Система Поста – полна. $\square$

Функция Вебба

Следствие 6.1. *Пусть $k \geq 3$. Множество, состоящее из одной функции Вебба $V_k(x, y) = \max(x, y) + 1$, является полной системой в P_k.*

Доказательство. Построим из функции Вебба функции из системы Поста.

$$\bar{x} = V_k(x, x) = \max(x, x) + 1 = x + 1;$$

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

$\square$

Неполиномиальность максимума

Следствие 6.2. *Пусть k – составное число. Тогда* $\max(x, y) \notin Pol_k$.

Доказательство проведем от противного. Пусть $\max(x, y) \in Pol_k$ при некотором составном k.
Но $\bar{x} = x + 1 \in Pol_k$.
Тогда $\{\bar{x}, \max(x, y)\} \subseteq Pol_k$.
Но система Поста полна в P_k, следовательно, каждая функция из P_k задается полиномом по модулю k при составном k – противоречие.
Откуда, $\max(x, y) \notin Pol_k$.

$\square$

Бесконечные полные системы в P_k

Следствие 6.3. *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 $g_1, \ldots, g_s$, что функция Вебба $V_k(x, y)$ выражается формулой над ними.

Тогда подсистема $A' = \{g_1, \ldots, g_s\}$ – полна в P_k (почему?).

$\square$

Задачи для самостоятельного решения

1. Гл. III 1.11, 2.7, 2.12, 2.23.

Литература к лекции 15

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001.
2. Гаврилов Г.П., сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.

Конец лекции 15