

## Лекция 1. Конечнзначные функции.

Элементарные  $k$ -значные функции. Способы задания  $k$ -значных функций: таблицы, формулы, 1-я и 2-я формы, полиномы. Полнота. 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>

# Конечнозначные функции

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

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

где  $n = 1, 2, \dots$

Множество всех  $k$ -значных функций обозначим  $P_k$ ,  
множество всех  $k$ -значных функций, зависящих от переменных  
 $x_1, \dots, x_n$ , обозначим  $P_k^{(n)}$ .

При  $k = 2$  функции называются функциями *алгебры логики*,  
или *булевыми* функциями, при  $k \geq 3$  — *многозначными*  
функциями.

Аналогично двузначному случаю равенство многозначных  
функций ( $k \geq 3$ ) рассматривается с точностью до  
несущественных (фиктивных) переменных.

# Существенные и несущественные переменные

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

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

Т.е. переменная  $x_i$  является существенной, если все другие переменные можно так определить, что полученная функция одной переменной  $x_i$  принимает хотя бы два различных значения.

Переменная, не являющаяся существенной, называется **несущественной**, или **фиктивной**.

Несущественные переменные можно удалять и добавлять, при этом получается функция, равная исходной, но зависящая от другого набора переменных.

# Равенство и конгруэнтность функций

Функции  $f$  и  $g$  называются **равными**, если конечным числом удалений или добавлений несущественных переменных их можно сделать совпадающими.

Функции  $f$  и  $g$  называются **конгруэнтными**, если равные им функции 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.

# Применение

Конечнозначные функции применяются для построения моделей решения прикладных задач, в которых можно выделить исходное множество, состоящее из конечного числа элементов.

Не столь широкое применение  $k$ -значных функций при  $k \geq 3$  по сравнению с двузначными связано, в первую очередь, с физической реализацией вычислительной техники на двузначной основе.

Проводятся исследования, относящиеся к разработке физических схем, построенных на многозначных функциях; существуют промышленные цифровые устройства на многозначной основе.

# 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	$f(k-1, \dots, k-1, 0)$
	$\dots$			
$k-1$	$\dots$	$k-1$	$k-2$	$f(k-1, \dots, k-1, k-2)$
$k-1$	$\dots$	$k-1$	$k-1$	$f(k-1, \dots, k-1, k-1)$

# Число $k$ -значных функций

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

**Доказательство.**

Каждую функцию  $f(x_1, \dots, x_n) \in P_k^{(n)}$  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  $|P_k^{(n)}| = k^{k^n}$ .



# Элементарные функции

## 2. Формулы.

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

$n = 0$ :

константы  $0, 1, \dots, k - 1$ .

$n = 1$ :

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

$x$  — тождественно равна  $x$ ;

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

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

$-x = k - x(\text{mod } k)$  — минус  $x$ .



# Элементарные функции

Характеристические функции выделенного значения  $J_i(x)$ ,  $j_i(x)$ , где  $i \in E_k$ :

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

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

# Элементарные функции

$n = 2$ :

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

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

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

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

$$x \rightarrow y = \begin{cases} k - 1, & x \leq y, \\ (k - 1) - (x - y), & x > y, \end{cases} \quad \text{— импликация.}$$

**обобщения:**

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

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

$$x^m = \underbrace{x \cdot \dots \cdot x}_m \quad \text{— степень.}$$

# Элементарные функции

Как двузначные функции обобщаются на многозначные функции?

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

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

# Формула

Понятия *формулы* и *функции, определяемой формулой*, вводятся аналогично двузначному случаю.

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  $F_1, \dots, F_m$  — уже построенные формулы или переменные (не обязательно различные), то выражение  $f(F_1, \dots, F_m)$  — формула.
3. Других формул нет, т. е. каждая формула построена либо по базису индукции, либо по индуктивному переходу.

# Формулы

**Пример.** Пусть  $A \subseteq P_5$  — множество элементарных функций.

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  $F = f(F_1, \dots, F_m)$ , где  $f$  — обозначение  $m$ -местной функции из  $A$  и  $F_1, \dots, F_m$  — формулы или переменные, причем формула  $F_i$  определяет функцию  $f_{F_i}(x_{i,1}, \dots, x_{i,n_i})$ , где  $\bigcup_{i=1}^m \{x_{i,1}, \dots, x_{i,n_i}\} = \{x_1, \dots, x_n\}$ , то

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

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	3
3	4	2	3
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:  $\sim \max(\sim x, \sim y) = \min(x, y)$ .

$$\begin{aligned} & \sim \max(\sim x, \sim y) = \\ & = (k - 1) - \begin{cases} (k - 1) - x, & (k - 1) - x \geq (k - 1) - y, \\ (k - 1) - y, & (k - 1) - x < (k - 1) - y, \end{cases} = \\ & = \begin{cases} x, & x \leq y, \\ y, & x > y, \end{cases} = \min(x, y). \end{aligned}$$

# 1-я форма

**Теорема 1 (о 1-й форме).** Пусть  $k \geq 2$ . Каждая  $k$ -значная функция  $f(x_1, \dots, x_n) \in P_k$  может быть задана формулой вида:

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

**Доказательство.**

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

$$\begin{aligned} f(\alpha) &= \max_{\sigma=(\sigma_1, \dots, \sigma_n) \in E_k^n} \min(J_{\sigma_1}(a_1), \dots, J_{\sigma_n}(a_n), f(\sigma)) = \\ &= \max(0, \dots, 0, f(\alpha), 0, \dots, 0) = f(\alpha). \end{aligned}$$

□

## 1-я форма

**Пример.**

Пусть  $f(x) = \bar{x} \in P_3$ :

$x$	$f$
0	1
1	2
2	0

Найдем ее 1-ю форму:

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

## 2-я форма

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

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

## 2-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 2-ю форму:

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

# Моном

**Мономом** ранга  $r$ ,  $r \geq 1$ , назовем формулу вида

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

где все переменные различны и  $s_1, \dots, s_r \geq 1$ .

**Мономом** ранга 0 назовем константу 1.

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

# Полином

**Полиномом** по модулю  $k$  длины  $l$ ,  $l \geq 1$ , назовем формулу вида

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

где  $K_1, \dots, K_l$  — различные мономы и  $c_1, \dots, c_l \in E_k \setminus \{0\}$  — коэффициенты.

**Полиномом** по модулю  $k$  длины 0 назовем константу 0.

Полиномы, отличающиеся только порядком своих слагаемых, считаем совпадающими.

Примем, что в полином можно добавлять слагаемые с нулевыми коэффициентами. Полученное выражение (формулу) будем также считать полиномом по модулю  $k$ . Полагаем, что такой полином совпадает с полиномом без всех слагаемых с нулевыми коэффициентами.

# Полиномы

**Теорема 3 (о задании  $k$ -значных функций полиномами по модулю  $k$ )** Пусть  $k \geq 2$ . Каждая  $k$ -значная функция  $f(x_1, \dots, x_n) \in P_k$  задается полиномом по модулю  $k$  тогда и только тогда, когда  $k$  — простое число.



# Полиномы

**Доказательство.** 1. Сначала рассмотрим случай, когда  $k$  — простое число.

Пусть  $f(x_1, \dots, x_n) \in P_k$ . Запишем ее во 2-й форме:

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

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

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

# Полиномы

## Доказательство.

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

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

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

Затем перемножаем скобки по свойствам дистрибутивности, коммутативности и ассоциативности; 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

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

# Полиномы

**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

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

Т. к. число  $k_1$  — делитель числа  $k$ , число  $k - 1$  обязано делиться на  $k_1 > 1$  — противоречие.

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

# Полиномиальные функции

## Элементарные функции

$$x,$$

$$\bar{x} = x + 1,$$

$$\sim x = (k - 1) - x = (k - 1)x + (k - 1),$$

$$-x = k - x = (k - 1)x,$$

$$x + y,$$

$$x - y = x + (k - 1)y,$$

$$x \cdot y,$$

$$x^m$$

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

# Неполиномиальные функции

## Элементарные функции

$$j_i(x), i \in E_k,$$

$$J_i(x), i \in E_k,$$

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

$$\min(x, y),$$

$$x \dot{-} y,$$

$$x \rightarrow y$$

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

# Полиномиальные функции

Множество всех  $k$ -значных функций, задающихся полиномами по модулю  $k$ , обозначается  $Polyn_k$ .

## Следствие 3.1.

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

## Вопросы:

Как 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 — по 2-й форме;
- 2) метод *неопределенных коэффициентов*.



## 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  $x^s$ :

$x$	$x^2$	$x^3$	$x^4$
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

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  $f(x) = J_1(x) + J_2(x) \in P_4$ :

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

## 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  $c \in E_4$ :

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

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

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

## Если $k$ — составное число

2. Пусть  $g(x) = 2 \cdot f(x) = 2(J_1(x) + J_2(x)) \in P_4$ .

Аналогично, выясним, задается ли функция  $g(x) \in P_4$  полиномом по модулю 4.

Тогда

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

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

Составляем систему уравнений:

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

## Если $k$ — составное число

Из первого и третьего уравнения получаем:

$$2c = 2,$$

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

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

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

Следовательно, функция  $g(x)$  задается полиномом по модулю 4, и найден 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, определяемых формулами над множеством  $A$  (с возможным добавлением или удалением несущественных переменных).

Обозначение:  $[A]$ .

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

**Примеры:**  $P_k$ ,  $Polyn_k$ ,  $\{x\}$ .

# Полные системы

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

**Примеры.**

1.  $\{0, 1, \dots, k-1, J_0(x), J_1(x), \dots, J_{k-1}(x), \max(x, y), \min(x, y)\}$  — система 1-й формы.
2.  $\{0, 1, \dots, k-1, j_0(x), j_1(x), \dots, j_{k-1}(x), x+y, x \cdot y\}$  — система 2-й формы.
3.  $\{0, 1, \dots, k-1, x+y, x \cdot y\}$  при простых  $k$  — система полиномов.



# Система Поста

**Теорема 4.** Пусть  $k \geq 3$ . Система Поста  $\{\bar{x}, \max(x, y)\}$  является полной системой в  $P_k$ .

**Доказательство.** Построим формулами над системой Поста все функции из системы 1-й формы.

1. Построение констант.

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

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

Далее  $(k - 1) + 1 = 0$ ;  $0 + 1 = 1$ ;  $1 + 1 = 2$ ; ...;  
 $(k - 2) + 1 = k - 1$ .

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.

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

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

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

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 построены формулами над функциями системы Поста. Значит, система Поста полна.



# Функция Вебба

**Следствие 4.1.** 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:

$$\begin{aligned}\bar{x} &= V_k(x, x) = \max(x, x) + 1 = x + 1, \\ \max(x, y) &= V_k(x, y) + \underbrace{1 + \dots + 1}_{k-1}.\end{aligned}$$

□

# Неполиномиальность максимума

**Следствие 4.2.** Если  $k$  — составное число, то  $\max(x, y) \notin \text{Polyn}_k$ .

**Доказательство** проведем от противного.

Предположим, что при некотором составном  $k$  выполняется  $\max(x, y) \in \text{Polyn}_k$ .

Но  $\bar{x} = x + 1 \in \text{Polyn}_k$ , поэтому  $\{\bar{x}, \max(x, y)\} \subseteq \text{Polyn}_k$ .

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,  $\max(x, y) \notin \text{Polyn}_k$ .



# Бесконечные полные системы в $P_k$

**Следствие 4.3.** *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  $g_1, \dots, g_t$ , что функция Вебба  $V_k(x, y)$  выражается формулой над ними.

Тогда подсистема  $A' = \{g_1, \dots, g_t\} \subseteq A$  полна в  $P_k$ .

□

# Литература к лекции

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001. Ч. I, гл. 2, стр. 43–50.
2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004. Гл. III 1.1, 1.11, 1.12, 2.7, 2.12, 2.22.



Конец лекции