

Лекция 2. Алгоритм распознавания полноты в  $P_k$ . Замкнутые классы. Классы функций, сохраняющих множество и сохраняющих разбиение, их замкнутость. Теорема Кузнецова о функциональной полноте. Предполные классы.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <http://mk.cs.msu.su>

# Алгоритм распознавания полноты

**Теорема 1** (о существовании алгоритма, распознающего полноту в  $P_k$ ). Пусть  $k \geq 3$ . Существует детерминированный алгоритм, которому на вход подается конечная система функций

$$A = \{f_1, \dots, f_m\} \subseteq P_k,$$

и который всегда через конечное число шагов останавливается и выдает ответ «Да», если система  $A$  — полна, и выдает ответ «Нет», если система  $A$  не является полной.

**Доказательство.**

Т.к. можно добавлять несущественные переменные, будем считать, что все функции  $f_j$  зависят от одного и того же набора переменных  $x_1, \dots, x_n$ .

# Алгоритм распознавания полноты

**Доказательство.** По индукции построим последовательность множеств

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \dots \subseteq P_k^2.$$

*Базис индукции.*  $N_0 = \emptyset$ .

*Индуктивный переход.* Пусть множество  $N_r \subseteq P_k^2$  уже построено. Для каждой функции  $f_j \in A$ ,  $j = 1, \dots, m$ , рассмотрим все функции, которые получаются подстановкой вместо ее переменных функций из множества  $N_r$  или переменных  $x_1, x_2$ . Положим

$$N_{r+1} = N_r \cup \{f_j(g_1(x_1, x_2), \dots, g_n(x_1, x_2)) \mid g_i \in N_r \cup \{x_1, x_2\}\},$$

где  $i = 1, \dots, n$ ,  $j = 1, \dots, m$ .

Например, множество  $N_1$  содержит все функции, которые можно построить, если вместо переменных функций  $f_j \in A$ ,  $j = 1, \dots, m$ , подставлять только переменные  $x_1$  и  $x_2$ .

# Алгоритм распознавания полноты

**Доказательство.** Т.к.  $N_r \subseteq P_k^2$  для всех  $r$ , и  $|P_k^2| = k^{k^2}$ , т.е.  $|P_k^2|$  — конечное число, найдется такое  $r^*$ , что

$$N_0 \subset N_1 \subset \dots \subset N_{r^*-1} \subset N_{r^*} = N_{r^*+1} = \dots$$

Пусть алгоритм останавливается, когда построено такое множество  $N_{r^*}$ , что  $N_{r^*} = N_{r^*+1}$ .

Тогда

- 1) если  $V_k(x_1, x_2) \in N_{r^*}$ , то ответ «Да» в силу полноты системы  $\{V_k\}$ ;
- 2) если  $V_k(x_1, x_2) \notin N_{r^*}$ , то ответ «Нет», т.к. замыкание  $[A]$  не содержит даже все функции от двух переменных.

□

Что можно сказать о сложности алгоритма из теоремы 1?

Он крайне трудоемок и не годится для применения на практике.

# Полнота в $P_k$

А есть ли алгоритм распознавания полноты в  $P_2$ ? Да, он основан на теореме Поста и заключается в проверке свойств сохранения констант, линейности, самодвойственности и монотонности для функций из исходной системы  $A \subseteq P_2$ .

Можно ли в  $P_k$  при  $k \geq 3$  доказать теорему, аналогичную теореме Поста в  $P_2$ ?

Да, это теорема Кузнецова. Мы ее докажем чуть позже.

# Замкнутый класс

Пусть  $A \subseteq P_k$ ,  $k \geq 2$ . Множество  $A$  называется **замкнутым** классом в  $P_k$ , если  $[A] = A$ .

## Функция, сохраняющая множество

Пусть  $E \subseteq E_k$ . Функция  $f(x_1, \dots, x_n) \in P_k$  **сохраняет множество  $E$** , если для всех  $a_1, \dots, a_n \in E$  верно  $f(a_1, \dots, a_n) \in E$ .

Множество функций из  $P_k$ , сохраняющих множество  $E \subseteq E_k$ , обозначим как  $T_k(E)$ .

# Класс функций, сохраняющих множество

**Теорема 2.** Пусть  $k \geq 2$ . Для каждого множества  $E \subseteq E_k$  класс  $T_k(E)$  замкнут.

**Доказательство.** Пусть  $E \subseteq E_k$ . Заметим, что  $x \in T_k(E)$ . Пусть  $f_0(y_1, \dots, y_m) \in T_k(E)$ , и  $f_i(x_1, \dots, x_n) \in T_k(E)$ , где  $i = 1, \dots, m$ .

Рассмотрим функцию

$$f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

Тогда если  $a_1, \dots, a_n \in E$ , то

$$\begin{aligned} f(a_1, \dots, a_n) &= f_0(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) = \\ &= f_0(b_1, \dots, b_m) \in E, \end{aligned}$$

т.к.  $b_1, \dots, b_m \in E$ . □



# Классы функций, сохраняющих множество

**Теорема 3.** Пусть  $k \geq 2$  и  $E \subseteq E_k$ .

Тогда  $T_k(E) = P_k$ , если и только если  $E = \emptyset$  или  $E = E_k$ .

**Доказательство.**

- 1) Если  $E = \emptyset$ , то  $T_k(E) = P_k$ , т.к. никаких условий нет.
- 2) Если  $E = E_k$ , то  $T_k(E) = P_k$ , т.к. для всех функций условие выполнено.
- 3) Если  $E \neq \emptyset$  и  $E \neq E_k$ , то пусть  $a \in E$  и  $b \in E_k \setminus E$ . Рассмотрим такую функцию  $f(x) \in P_k$ , что  $f(a) = b$ . Тогда  $f(x) \notin T_k(E)$ .

□

Пусть  $k = 2$ .

Тогда  $T_2(\{0\}) = T_0$  и  $T_2(\{1\}) = T_1$  — классы, сохраняющие константу ноль и константу один соответственно.

Неполнота системы  $\{\sim x, \max(x, y)\}$  в  $P_k$  при  $k \geq 3$ 

**Пример.** Докажем, что система  $A = \{\sim x, \max(x, y)\}$  — неполна в  $P_k$  при  $k \geq 3$ .

Рассмотрим  $E = \{0, k - 1\} \subseteq E_k$ . Отметим, что  $E \neq E_k$  при  $k \geq 3$ . Кроме того,

$$\begin{aligned}\sim 0 &= k - 1, \quad \sim (k - 1) = 0, \\ \max(a, b) &\in \{0, k - 1\} \text{ при } a, b \in \{0, k - 1\}.\end{aligned}$$

Значит,  $A \subseteq T_k(E)$ .

По теоремам 2 и 3 получаем:

$$[A] \subseteq T_k(E) \neq P_k.$$

Т.е. система  $\{\sim x, \max(x, y)\}$  — неполна в  $P_k$  при  $k \geq 3$ .

При  $k = 2$  система  $\{\sim x = \bar{x}, \max(x, y) = x \vee y\}$  — полна.

# Разбиение множества

Семейство  $D = \{D_1, \dots, D_s\}$  называется **разбиением** множества  $E_k$ , если

1)  $D_i \neq \emptyset$  при  $i = 1, \dots, s$ ;

2)  $D_i \cap D_j = \emptyset$  при  $i \neq j$ ;

3)  $\bigcup_{i=1}^s D_i = E_k$ .

## Функция, сохраняющая разбиение

Пусть  $D = \{D_1, \dots, D_s\}$  — разбиение множества  $E_k$ . Элементы  $a, b \in E_k$  называются **эквивалентными** по разбиению  $D$ , если найдется такое подмножество  $D_i \in D$ , что  $a, b \in D_i$ .

Обозначение:  $a \sim_D b$ .

Наборы  $\alpha = (a_1, \dots, a_n), \beta = (b_1, \dots, b_n) \in E_k^n$  называются **эквивалентными** по разбиению  $D$ , если  $a_i \sim_D b_i$  для всех  $i = 1, \dots, n$ . Обозначение:  $\alpha \sim_D \beta$ .

Функция  $f(x_1, \dots, x_n) \in P_k$  **сохраняет разбиение  $D$** , если для всех пар наборов  $\alpha, \beta \in E_k^n$  если  $\alpha \sim_D \beta$ , то  $f(\alpha) \sim_D f(\beta)$ .

Множество функций из  $P_k$ , сохраняющих разбиение  $D$ , обозначим как  $U_k(D)$ .

# Класс функций, сохраняющих разбиение

**Теорема 4.** Пусть  $k \geq 2$ . Для каждого разбиения  $D$  класс  $U_k(D)$  замкнут.

**Доказательство.** Пусть  $D$  — разбиение множества  $E_k$ .  
Заметим, что  $x \in U_k(D)$ .

Пусть  $f_0(y_1, \dots, y_m) \in U_k(D)$ , и  $f_i(x_1, \dots, x_n) \in U_k(D)$ , где  $i = 1, \dots, m$ .

Рассмотрим функцию

$$f(x_1, \dots, x_n) = f_0(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

Тогда если  $\alpha, \beta \in E_k^n$  и  $\alpha \sim_D \beta$ , то

$$\begin{aligned} f(\alpha) &= f_0(f_1(\alpha), \dots, f_m(\alpha)) = f_0(\gamma), \\ f(\beta) &= f_0(f_1(\beta), \dots, f_m(\beta)) = f_0(\delta), \end{aligned}$$

и  $f(\alpha) \sim_D f(\beta)$ , т.к.  $\gamma \sim_D \delta$ . □

# Классы функций, сохраняющих разбиение

**Теорема 5.** Пусть  $k \geq 2$  и  $D = \{D_1, \dots, D_s\}$  — разбиение множества  $E_k$ .

Тогда  $U_k(D) = P_k$ , если и только если  $s = 1$  или  $s = k$ .

**Доказательство.**

1) Если  $s = 1$ , то  $U_k(D) = P_k$ , т.к. все элементы  $E_k$  эквивалентны по разбиению.

2) Если  $s = k$ , то  $U_k(D) = P_k$ , т.к. эквивалентность по разбиению обозначает равенство элементов  $E_k$ .

3) Если  $1 < s < k$ , то найдется подмножество  $D_i \in D$ , в котором не менее двух элементов, т.е.  $a, b \in D_i$ ,  $a \neq b$ , и найдется еще хотя бы одно подмножество  $D_j \in D$ ,  $i \neq j$ , и пусть  $c \in D_j$ . Рассмотрим такую функцию  $g(x) \in P_k$ , что  $g(a) = a$ ,  $g(b) = c$ . Тогда  $g(x) \notin U_k(D)$ .

□

В  $P_2$  нет не совпадающих в нем классов, сохраняющих разбиение.

# Неполнота одной системы в $P_k$ при $k \geq 3$

**Пример.** Докажем, что система  $A = \{0, 1, \dots, k-1, j_0(x), j_1(x), \dots, j_{k-1}(x), \max(x, y), \min(x, y)\}$  — неполна в  $P_k$  при  $k \geq 3$ .

Рассмотрим  $D = \{D_1, D_2\}$  — разбиение  $E_k$ , где  $D_1 = \{0, 1\}$ ,  $D_2 = \{2, \dots, k-1\}$ , при этом  $s = 2$ .

Отметим, что  $1 < s < k$  при  $k \geq 3$ .

Каждая константа,  $j_i(x)$ ,  $i \in E_k$ ,  $\max(x, y)$ ,  $\min(x, y)$  сохраняют разбиение  $D$ . Значит,  $A \subseteq U_k(D)$ .

По теоремам 4 и 5 получаем:

$$[A] \subseteq U_k(D) \neq P_k.$$

Т.е. система  $A$  — неполна в  $P_k$  при  $k \geq 3$ .

При  $k = 2$  система

$\{0, 1, j_0(x) = \bar{x}, j_1(x) = x, \max(x, y) = x \vee y, \min(x, y) = xy\}$  — полна.

# Полнота некоторой системы в $P_k$ при $k \geq 3$

**Пример.** Докажите, что система

$A = \{0, 1, \dots, k-1, J_0(x), J_1(x), \dots, J_{k-1}(x), x+y, x \cdot y\}$  —  
полна в  $P_k$  при всех  $k \geq 3$ .



# Теорема Кузнецова

**Теорема 6 (А.В. Кузнецова о функциональной полноте).**  
 Пусть  $k \geq 3$ . Существует такое конечное семейство замкнутых и не содержащихся друг в друге классов в  $P_k$

$$M_1, \dots, M_{s(k)},$$

что для любого  $A \subseteq P_k$  система  $A$  полна в  $P_k$  тогда и только тогда, когда она не содержится ни в одном из классов  $M_1, \dots, M_{s(k)}$ .

**Доказательство.**

**1. Построение классов.** Пусть  $N \subseteq P_k^2$  и

n1)  $N \neq P_k^2$ ;

n2)  $x_1 \in N, x_2 \in N$ ;

n3)  $[N] \cap P_k^2 = N$ .

Пусть  $M(N) \subseteq P_k$  и

$$M(N) = \{f(y_1, \dots, y_m) \in P_k \mid f(g_1(x_1, x_2), \dots, g_m(x_1, x_2)) \in N \text{ для всех } g_1, \dots, g_m \in N\}.$$

# Теорема Кузнецова

1.1) Класс  $M(N)$  — замкнут.

Заметим, что  $x \in M(N)$ .

Если  $f_0(z_1, \dots, z_t) \in M(N)$ ,  $f_i(y_1, \dots, y_m) \in M(N)$ , где  $i = 1, \dots, t$ , и

$f(y_1, \dots, y_m) = f_0(f_1(y_1, \dots, y_m), \dots, f_t(y_1, \dots, y_m))$ , то для любых функций  $g_1, \dots, g_m \in N$  получаем

$$\begin{aligned} f(g_1(x_1, x_2), \dots, g_m(x_1, x_2)) &= f_0(f_1(g_1(x_1, x_2), \dots, g_m(x_1, x_2)), \dots, \\ & f_t(g_1(x_1, x_2), \dots, g_m(x_1, x_2))) = \\ &= f_0(h_1(x_1, x_2), \dots, h_t(x_1, x_2)) \in N, \end{aligned}$$

т.к.  $h_1(x_1, x_2), \dots, h_t(x_1, x_2) \in N$ .

# Теорема Кузнецова

$$1.2) M(N) \cap P_k^2 = N.$$

Если  $f(x_1, x_2) \in M(N)$ , то для  $x_1, x_2 \in N$  получаем  $f(x_1, x_2) \in N$ .

Если  $f(x_1, x_2) \in N$  и  $g_1, g_2 \in N$ , то  $f(g_1(x_1, x_2), g_2(x_1, x_2)) \in [N] \cap P_k^2$ , а значит по свойству  $n3$  для множества  $N$ ,  $f(g_1(x_1, x_2), g_2(x_1, x_2)) \in N$ . Т.е.  $f(x_1, x_2) \in M(N)$ .

1.3)  $M(N) \neq P_k$  по п. 1.2) и свойству  $n1$  для множества  $N$ .

Выберем из семейства замкнутых классов

$$\mathcal{S}(P_k) = \{M(N) \mid N \subseteq P_k^2, \text{ для } N \text{ верны свойства } n1, n2, n3\}$$

все максимальные (по включению) классы.

Обозначим их как  $M_1, \dots, M_{s(k)}$ .

Они замкнуты и не содержатся друг в друге по построению.

# Теорема Кузнецова

2. Обоснование критерия. Докажем, что построенные классы

$$M_1, \dots, M_{s(k)}$$

искомые.

Пусть  $A \subseteq P_k$ .

2.1) Если  $A \subseteq M_j$  для некоторого  $j$ , то по п.п. 1.1) и 1.3)

$$[A] \subseteq [M_j] = M_j \neq P_k.$$

Т.е. система  $A$  — не полна.

# Теорема Кузнецова

2.2) Пусть  $A$  не содержится ни в одном классе  $M_j$ ,

$j = 1, \dots, s(k)$ , но система  $A$  не полна.

Положим  $N = ([A] \cap P_k^2) \cup \{x_1, x_2\}$ .

Тогда

n1)  $N \neq P_k^2$ ;

n2)  $x_1, x_2 \in N$ ;

n3)  $N = [N] \cap P_k^2$ , т.к.  $N \subseteq [N] \cap P_k^2 \subseteq ([A] \cap P_k^2) \cup \{x_1, x_2\} = N$ .

Отсюда  $M(N) \in \mathcal{S}(P_k)$ .

Но если  $f(x_1, \dots, x_n) \in A$ , то для любых функций  $g_1, \dots, g_n \in N$

$$f(g_1(x_1, x_2), \dots, g_n(x_1, x_2)) \in [A] \cap P_k^2 \subseteq N.$$

Поэтому  $A \subseteq M(N)$ .

Отсюда  $A \subseteq M(N) \subseteq M_j$  для некоторого  $j$  — противоречие.

Т.е. система  $A$  полна. □

# Предполный класс

Пусть  $A \subseteq P_k$ ,  $k \geq 2$ . Множество  $A$  называется **предполным классом** в  $P_k$ , если

- 1)  $[A] \neq P_k$ ;
- 2) для любой функции  $f \in P_k \setminus A$  верно  $[A \cup \{f\}] = P_k$ .

# Предполные классы

В  $P_2$  пять предполных классов:  $T_0$ ,  $T_1$ ,  $L$ ,  $S$ ,  $M$ .

В  $P_k$  каждый из классов  $M_1, \dots, M_{s(k)}$  в теореме Кузнецова является предполным.

Из доказательства  $s(k) \leq 2^{k^2} - 2$ .

# Предполные классы

Для каждого  $k \geq 2$  классы сохранения множества  $T_k(E)$  и сохранения разбиения  $U_k(D)$ , если они не совпадают с  $P_k$ , являются предполными в  $P_k$ .

Но это не все предполные классы в  $P_k$ .



# Предполные классы

При каждом  $k \geq 3$  все предполные классы конструктивно описаны.

Часть предполных классов в  $P_k$ ,  $k \geq 3$ , описаны

С.В. Яблонским, А.А. Мартыненко, Ло Чжу Каем.

Завершил описание предполных классов в  $P_k$ ,  $k \geq 3$ , и доказал, что других предполных классов нет, И. Розенберг.

## Литература к лекции

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001. Ч. I, гл. 2, стр. 51–56.
2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004. Гл. III 2.1–2.5, 2.13, 2.19.

Конец лекции