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.ru

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Алгоритм распознавания полноты

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

$$A = \{f_1, \ldots, f_t\} \subseteq P_k, \ \ t \geqslant 1,$$

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 $x_1, \ldots, x_n$.

Алгоритм распознавания полноты

Доказательство. По индукции построим последовательность множеств

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots \subseteq P_k^{(2)}.$$

Базис индукции. $N_0 = \{x_1, x_2\}$.

Индуктивные переход. Пусть множество $N_r \subseteq P_k^{(2)}$ уже построено. Для каждой функции $f_j \in A$, $j = 1, \ldots, t$, рассмотрим все функции, которые получаются подстановкой вместо ее переменных функций из множества N_r. Положим

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

где $i = 1, \ldots, n$, $j = 1, \ldots, t$.

Например, множество N_1 содержит все функции, которые можно построить, если вместо переменных функций $f_j \in A$, $j = 1, \ldots, t$, 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. множество $P_k^{(2)}$ — конечно, найдется такое r^*, $r^* \geqslant 1$, что

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

Алгоритм распознавания полноты

Покажем, что $N_{r^*} = [A]_{x_1,x_2}$, где $[A]_{x_1,x_2} = [A] \cap P_k^{(2)}$.

Другими словами, покажем, что в множестве N_{r^*} содержатся в точности все те функции переменных x_1, x_2, которые можно выразить формулами над A.

1. Если $f \in N_{r^*}$, то по построению $f \in [A]_{x_1,x_2}$ (почему?). Значит, $N_{r^*} \subseteq [A]_{x_1,x_2}$.

Алгоритм распознавания полноты

Доказательство.
2. Пусть теперь $f(x_1, x_2) \in [A]$.

По определению это означает, что функцию $f(x_1, x_2)$ можно выразить некоторой формулой F над A, причем в этой формуле F встречаются только переменные x_1, x_2.

Докажем индукцией по числу d вхождений в формулу F функций из A, что $f \in N_{r^*}$.

1) *Базис индукции*: $d = 0$. Если $F = x_1$ или $F = x_2$, то $f \in N_0$, а значит, $f \in N_{r^*}$.

Алгоритм распознавания полноты

2) *Индуктивный переход.* Пусть любая функция переменных x_1, x_2 из $[A]$, которая может быть выражена формулой с не более, чем d_0, вхождениями функций из A, содержится также и в N_{r^*}.

Рассмотрим функцию $f(x_1, x_2) \in [A]$, которая выражается формулой F с $d_0 + 1$ вхождениями функций из A.

Тогда $F = f_j(F_1, \ldots, F_n)$, где $f_j \in A$, а F_i — формула с не более, чем d_0, вхождениями функций из A, $i = 1, \ldots, n$.

По предположению индукции $f_{F_i} \in N_{r^*}$, $i = 1, \ldots, n$.

Следовательно, по построению $f \in N_{r^*+1}$. Но $N_{r^*+1} = N_{r^*}$. Поэтому $f \in N_{r^*}$. Значит, $[A]_{x_1,x_2} \subseteq N_{r^*}$.

Равенство $N_{r^*} = [A]_{x_1,x_2}$ обосновано.

Алгоритм распознавания полноты

Доказательство.
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. $[A]$ не содержит даже все функции от двух переменных (в силу доказанного равенства $[A]_{x_1,x_2} = N_{r^*}$).

$\square$

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 $k \geqslant 3$ доказать теорему, аналогичную теореме Поста в P_2?
Да, это теорема Кузнецова. Мы ее докажем чуть позже.

Замкнутый класс

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

Замкнутые классы

Утверждение 1. *Пусть* $k \geqslant 2$ *и* $A \subseteq P_k$. *Если* $x \in A$ *и для любых* $f_0(y_1, \ldots, y_m) \in A$, $f_i(x_{i,1}, \ldots, x_{i,n_i}) \in A$, $i = 1, \ldots, m$, *выполняется*

$$f_0(f_1(x_{1,1}, \ldots, x_{1,n_1}), \ldots, f_1(x_{m,1}, \ldots, x_{m,n_m})) \in A,$$

то множество A *является замкнутым классом.*

Замкнутые классы

Доказательство. Рассмотрим произвольную формулу F над A, которая выражает некоторую функцию $f \in P_k$.

Докажем индукцией по числу d вхождений в формулу F функций из A, не равных тождественной функции, что $f \in A$.

1) *Базис индукции*: $d = 0$. Если $F = x$, то $f \in A$.

Замкнутые классы

2) *Индуктивный переход.* Пусть любая функция, которая может быть выражена формулой с не более, чем d_0, вхождениями функций из A, не равных тождественной функции, содержится в A.

Рассмотрим функцию $f(x_1, \ldots, x_n) \in [A]$, которая выражается формулой F с $d_0 + 1$ вхождениями функций из A, не равных тождественной функции.

Тогда $F = f_0(F_1, \ldots, F_m)$, где $f_0 \in A$, а F_i — формула с не более, чем d_0, вхождениями функций из A, не равных тождественной функции, $i = 1, \ldots, m$.

По предположению индукции $f_{F_i} \in A$, $i = 1, \ldots, n$.

Далее по условию утверждения $f \in A$. $\square$

Функция, сохраняющая множество

Пусть $E \subseteq E_k$. Функция $f(x_1, \ldots, x_n) \in P_k$ **сохраняет множество** E, если для любых $a_1, \ldots, a_n \in E$ выполняется $f(a_1, \ldots, a_n) \in E$.

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

Класс функций, сохраняющих множество

Утверждение 2. *Пусть* $k \geqslant 2$. *Для каждого множества* $E \subseteq E_k$ *множество* $T_k(E)$ *— замкнутый класс.*

Доказательство. Пусть $E \subseteq E_k$. Заметим, что $x \in T_k(E)$.

Пусть $f_0(y_1, \ldots, y_m) \in T_k(E)$ и $f_i(x_1, \ldots, x_n) \in T_k(E)$, где $i = 1, \ldots, m$.

Рассмотрим функцию
$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$.

Далее если $a_1, \ldots, a_n \in E$, то

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

т. к. $b_1, \ldots, b_m \in E$. Значит, $f \in T_k(E)$. $\square$

Классы функций, сохраняющих множество

Утверждение 3. *Пусть $k \geqslant 2$ 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 $f(x) \notin T_k(E)$.

$\square$

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 $k \geqslant 3$

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

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

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

Значит, $A \subseteq T_k(E)$.
Получаем:

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

Т. е. система $\{\sim x, \max(x, y)\}$ — неполна в P_k при $k \geqslant 3$.
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) $\bigcup\limits_{i=1}^{s} D_i = E_k$.

Функция, сохраняющая разбиение

Пусть $D = \{D_1, \ldots, D_s\}$ — 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 $\alpha = (a_1, \ldots, a_n), \beta = (b_1, \ldots, b_n) \in E_k^n$ называются **эквивалентными** по разбиению D, если $a_i \sim_D b_i$ для всех $i = 1, \ldots, n$. Обозначение: $\alpha \sim_D \beta$.

Функция $f(x_1, \ldots, x_n) \in P_k$ **сохраняет разбиение** D, если для любых пар наборов $\alpha, \beta \in E_k^n$ из $\alpha \sim_D \beta$ следует $f(\alpha) \sim_D f(\beta)$.

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

Класс функций, сохраняющих разбиение

Утверждение 4. *Пусть $k \geqslant 2$. Для каждого разбиения D множества E_k множество $U_k(D)$ — замкнутый класс.*

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

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

Рассмотрим функцию $f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$.

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

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

и $f(\alpha) \sim_D f(\beta)$, т. к. $\gamma \sim_D \delta$. Значит, $f \in U_k(D)$. $\square$

Классы функций, сохраняющих разбиение

Утверждение 5. *Пусть $k \geqslant 2$ и $D = \{D_1, \ldots, D_s\}$ — 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 $f(x) \in P_k$, что $f(a) = a$, $f(b) = c$. Тогда $f(x) \notin U_k(D)$.

□

В P_2 нет не совпадающих в ним классов, сохраняющих разбиение.

Неполнота одной системы в P_k при $k \geqslant 3$

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

Рассмотрим $D = \{D_1, D_2\}$ — разбиение E_k, где $D_1 = \{0, 1\}$, $D_2 = \{2, \ldots, k-1\}$, при этом $s = 2$.
Отметим, что $1 < s < k$ при $k \geqslant 3$.
Каждая константа, $j_i(x)$, $i \in E_k$, $\max(x, y)$, $\min(x, y)$ сохраняют разбиение D. Значит, $A \subseteq U_k(D)$.
Получаем:

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

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

Пример. Докажите, что система
$A = \{0, 1, \ldots, k-1, J_0(x), J_1(x), \ldots, J_{k-1}(x), x+y, x \cdot y\}$ —
полна в P_k при всех $k \geqslant 3$.

Теорема Кузнецова

Теорема 2 (А.В. Кузнецова о функциональной полноте). *Пусть $k \geqslant 3$. 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 $M_1, \dots, M_{s(k)}$.

Теорема Кузнецова

Доказательство.

1. Построение классов. Пусть $N \subseteq P_k^{(2)}$ и

$n1)$ $N \neq P_k^{(2)}$;
$n2)$ $x_1 \in N$, $x_2 \in N$;
$n3)$ $[N]_{x_1,x_2} = [N] \cap P_k^{(2)} = N$.

Пусть $M(N) \subseteq P_k$ и

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

Другими словами, в $M(N)$ содержатся все такие функции, что при подстановке вместо их переменных любых функций из N получается снова функция из N.

Теорема Кузнецова

1.1) Покажем, что $M(N)$ — замкнутый класс.

Заметим, что $x \in M(N)$. Пусть $f_0(z_1, \ldots, z_t) \in M(N)$, $f_i(y_1, \ldots, y_m) \in M(N)$, где $i = 1, \ldots, t$.

Рассмотрим функцию
$f(y_1, \ldots, y_m) = f_0(f_1(y_1, \ldots, y_m), \ldots, f_t(y_1, \ldots, y_m))$.

Тогда для любых функций $g_1, \ldots, g_m \in N$ получаем

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

т. к. $h_1(x_1, x_2), \ldots, h_t(x_1, x_2) \in N$. Значит, $f \in M(N)$.

Теорема Кузнецова

1.2) Покажем, что $M(N) \cap P_k^{(2)} = N$.

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 $f(g_1(x_1, x_2), g_2(x_1, x_2)) \in [N]_{x_1, x_2}$, а значит, по свойству $n3$ для множества N верно $f(g_1(x_1, x_2), g_2(x_1, x_2)) \in N$. Поэтому $f(x_1, x_2) \in M(N)$.

Теорема Кузнецова

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

Теорема Кузнецова

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 по доказанному и не содержатся друг в друге по построению.

Теорема Кузнецова

2. Обоснование критерия. Докажем, что построенные классы

$$M_1, \ldots, M_{s(k)} \ -$$

искомые.

Теорема Кузнецова

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) Предположим, что A не содержится ни в одном классе M_j, $j = 1, \ldots, s(k)$, но система A не полна.

Положим $N_0 = ([A] \cap P_k^{(2)})$.

Тогда
$n1)$ $N_0 \neq P_k^{(2)}$;
$n2)$ $x_1, x_2 \in N_0$;
$n3)$ $[N_0]_{x_1,x_2} = [N_0] \cap P_k^{(2)} = N_0$, т. к.
$N_0 \subseteq [N_0] \cap P_k^{(2)} \subseteq ([A] \cap P_k^{(2)}) = N_0$.

Значит, $M(N_0) \in \mathcal{S}(P_k)$.

Теорема Кузнецова

Итак, получено, что $M(N_0) \in \mathcal{S}(P_k)$.

Но если $f(x_1, \dots, x_n) \in A$, то для любых функций $g_1, \dots, g_n \in N_0$

$$f(g_1(x_1, x_2), \dots, g_n(x_1, x_2)) \in [A] \cap P_k^{(2)} \subseteq N_0.$$

Поэтому $A \subseteq M(N_0)$. Следовательно, $A \subseteq M(N_0) \subseteq M_j$ для некоторого j — противоречие.

Значит, система A — полна. $\square$

Предполный класс

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

1) $[A] \neq P_k$;

2) для любой функции $f \in P_k \setminus A$ выполняется $[A \cup \{f\}] = P_k$.

Предполные классы в P_2

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

Предполные классы в P_k

Утверждение 6. *Пусть $k \geqslant 2$. Классы $M_1, \ldots, M_{s(k)}$ из теоремы Кузнецова — все предполные классы в P_k.*

Доказательство.

1. Докажем, что каждый из классов M_j — предполный.

1) $[M_j] = M_j \neq P_k$.

2) Если $f \in P_k \setminus M_j$, то множество $M_j \cup \{f\}$ не содержится ни в одном из классов $M_1, \ldots, M_{s(k)}$. Значит, по теореме Кузнецова $[M_j \cup \{f\}] = P_k$.

Предполные классы в P_k

Доказательство.
2. Докажем от противного, что других предполных классов в P_k нет.

Пусть $M \subseteq P_k$ — предполный класс и $M \neq M_j$ для всех $j = 1, \ldots, s(k)$.

1) Если M не содержится ни в одном из классов $M_1, \ldots, M_{s(k)}$, то по теореме Кузнецова $[M] = P_k$ — противоречие с п. 1 определения предполного класса.

2) Пусть $M \subseteq M_j$ для некоторого j, $1 \leqslant j \leqslant s(k)$. Рассмотрим функцию $f \in M_j \setminus M$. Тогда $[M \cup \{f\}] \subseteq [M_j] = M_j \neq P_k$ — противоречие с п. 2 определения предполного класса. $\square$

Предполные классы

Для каждого $k \geqslant 2$ 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 $k \geqslant 3$ **все** предполные классы описаны.

Часть предполных классов в P_k, $k \geqslant 3$, найдены С.В. Яблонским, А.А. Мартыненко, Ло Чжу Каем. Завершил описание предполных классов в P_k, $k \geqslant 3$, 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