Лекция 5. Предполные классы. Сохранение функцией множества функций. Описание предполных классов в P_k. Теорема Кузнецова.

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

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Теорема Поста

Для проверки полноты множеств функций из P_2 можно применять теорему **Поста**.

Теорема Поста. *Пусть $A \subseteq P_2$. Множество A является полной системой тогда и только тогда, когда оно не содержится ни в одном из классов T_0, T_1, L, S, M.*

При этом T_0, T_1, L, S, M являются всеми **предполными** классами в P_2.

Можно ли в P_k при $k \geqslant 3$ доказать теорему, аналогичную теореме Поста в P_2? Да, это теорема **Кузнецова**.

Сначала рассмотрим свойства **предполных классов** в P_k.

Предполный класс

Пусть $A \subseteq P_k$. Множество A называется **предполным классом** (в P_k), если

1) $[A] \neq P_k$, т. е. множество A не является полной системой;

2) для любой функции $f \in P_k \setminus A$ верно $[A \cup \{f\}] = P_k$, т. е. при добавлении к A любой новой функции получается полная система.

Предполный класс называется также **максимальным классом**.

Замкнутость предполного класса

Предложение 1. *Любой предполный класс в P_k является замкнутым классом.*

Доказательство проведем от обратного: пусть $A \subseteq P_k$ — предполный класс, но $[A] \neq A$.

Значит, найдется функция $f \in [A] \setminus A$. Получаем:

$$[A \cup \{f\}] = [A].$$

По п. 1 определения предполного класса $[A] \neq P_k$, но по п. 2 определения предполного класса $[A \cup \{f\}] = [A] = P_k$. Приходим к противоречию.

Значит, A — замкнутый класс.

$\square$

Свойства предполных классов

Предложение 2. *Если $A, B \subseteq P_k$ — предполные классы и $A \neq B$, то $A \not\subseteq B$ и $B \not\subseteq A$.*

Доказательство проведем от обратного: пусть, например, $A \subseteq B$, $A \neq B$.

Значит, найдется функция $f \in B \setminus A$. Получаем:

$$[A \cup \{f\}] \subseteq [B].$$

По п. 1 определения предполного класса $[B] \neq P_k$, но по п. 2 определения предполного класса $[A \cup \{f\}] = P_k \subseteq [B]$. Приходим к противоречию.

Значит, $A \not\subseteq B$ и аналогично $B \not\subseteq A$.

$\square$

Критериальная система

Предложение 3. *Множество всех предполных классов в P_k является критериальной системой, т. е. для любого множества $A \subseteq P_k$ верно: множество A является полной системой в P_k тогда и только тогда, когда оно не содержится ни в одном из предполных классов.*

Критериальная система

Доказательство. Пусть $A \subseteq P_k$.

1. *Необходимость*. Если A — полная система и предположить, что $A \subseteq B$, где B — некоторый предполный класс, то

$$[A] \subseteq [B] = B \neq P_k \; -$$

противоречие.

Значит, A не содержится ни в одном из предполных классов.

2. *Достаточность*. Если A — не содержится ни в одном из предполных классов и предположить, что $[A] \neq P_k$, то $[A] \subseteq B$, где B — некоторый предполный класс — противоречие.

Значит, A — полная система.

$\square$

Предполные классы

Каждый предполный класс в P_k, $k \geqslant 2$, можно описать как множество всех полиморфизмов некоторого множества S, $S \subseteq P_k^{(m)}$.

Сохранение функцией множества функций

Пусть $S \subseteq P_k^{(m)}$ — множество k-значных функций переменных $z_1, \ldots, z_m$.

Функция $f(x_1, \ldots, x_n)$ **сохраняет** множество S, если для любых функций $g_1, \ldots, g_n \in S$ верно

$$h(z_1, \ldots, z_m) = f(g_1(z_1, \ldots, z_m), \ldots, g_n(z_1, \ldots, z_m)) \in S.$$

Т. е. функция f сохраняет множество S, если при подстановке вместо переменных функции f любых функций из S получается функция из S.

Если функция f сохраняет множество S, то функцию f назовем **полиморфизмом** множества S.

Сохранение функцией множества функций

Пример. Пусть $S = \{0, 1, z\} \subseteq P_2^{(1)}$.

Тогда функция $f_1(x, y) = x \vee y \in P_2$ **сохраняет** множество S, т. к. для любой функции $g \in S$ верно:

$$\begin{aligned} &0 \vee g = g \vee 0 = g, \\ &1 \vee g = g \vee 1 = 1, \\ &z \vee z = z. \end{aligned}$$

Функция $f_2(x, y) = x \oplus y \in P_2$ **не сохраняет** множество S , т. к.

$$1 \oplus z = \bar{z} \notin S.$$

Сохранение функцией множества функций

Множество всех функций из P_k, сохраняющий множество S, обозначаем $Pol(S)$.

Считаем, что любая функция из P_k сохраняет пустое множество функций, т. е. $Pol(\emptyset) = P_k$.

Кроме того, тождественная функция сохраняет любое множество функций, поэтому для любого множества S, $S \subseteq P_k^{(m)}$, верно $I_k \subseteq Pol(S)$.

Сохранение функцией множества функций

Пример. Пусть $S = \{0\} \subseteq P_k^{(1)}$.

Если функция $f(x_1, \ldots, x_n) \in P_k$ сохраняет S, то верно

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

Значит, функции, сохраняющие S, — в точности функции из P_k, сохраняющие 0, т. е. $Pol(S) = T_0$.

Сохранение функцией множества функций

Пример. Пусть $S = \{z\} \subseteq P_k^{(1)}$.

Если функция $f(x_1, \ldots, x_n) \in P_k$ сохраняет S, то верно

$$f(z, \ldots, z) = z,$$

или

$$\begin{aligned} &f(0, \ldots, 0) = 0,\\ &f(1, \ldots, 1) = 1,\\ &\ldots,\\ &f(k-1, \ldots, k-1) = k-1. \end{aligned}$$

Значит, функции, сохраняющие S, — в точности функции из P_k, сохраняющие любой $a \in E_k$, т. е. $Pol(S) = \bigcap\limits_{a \in E_k} T_a$.

Сохранение функцией множества функций

Пример. Пусть $S = \{z, \bar{z}\} \subseteq P_2^{(1)}$.

Если функция $f(x_1, \ldots, x_n) \in P_2$ сохраняет S, то верно

$$f(z^{\sigma_1}, \ldots, z^{\sigma_n}) = z^{\sigma_0},$$

где $\sigma_0, \sigma_1, \ldots, \sigma_n \in E_2$.

Значит, функции, сохраняющие S, — в точности функции из P_2, которые на всех парах противоположных наборов принимают противоположные значения, т. е. $Pol(S)$ — класс самодвойственных функций.

Замкнутость множества полиморфизмов

Предложение 4. *Если* $S \subseteq P_k^{(m)}$, *то* $Pol(S)$ *— замкнутый класс.*

Доказательство. Пусть $S \subseteq P_k^{(m)}$. Отметим, что $I_k \subseteq Pol(S)$. Пусть $f_0(y_1, \ldots, y_t) \in Pol(S)$ и $f_i(x_1, \ldots, x_n) \in Pol(S)$, где $i = 1, \ldots, t$.

Рассмотрим функцию

$$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_t(x_1, \ldots, x_n)).$$

Если $g_1, \ldots, g_n \in S$, то

$$\begin{aligned} f(g_1, \ldots, g_n) &= f_0(f_1(g_1, \ldots, g_n), \ldots, f_t(g_1, \ldots, g_n)) = \\ &= f_0(h_1, \ldots, h_t) = h \in S, \end{aligned}$$

т. к. в силу $f_1, \ldots, f_t \in Pol(S)$ верно $h_1, \ldots, h_t \in S$ и в силу $f_0 \in Pol(S)$ верно $h \in S$.

Значит, $f \in Pol(S)$.

Неполнота системы $\{0, 1, \dots, k-1, x \cdot y\}$ в P_k

Пример. Докажем, что $A = \{0, 1, \dots, k-1, x \cdot y\}$ — неполная система в P_k при простых k. Ясно, что при составных k эта система не полна, т. к. $A \subseteq Polyn_k$.

Рассмотрим множество

$$S = \{0, 1, \dots, k-1, j_0(x), 2 \cdot j_0(x), \dots, (k-1) \cdot j_0(x)\} \subseteq P_k^{(1)}.$$

Отметим, что $A \subseteq Pol(S)$. Но $x + y \notin Pol(S)$, т. к.

$$1 + j_0(x) \notin S.$$

Значит, $Pol(S) \neq P_k$. Получаем:

$$[A] \subseteq [Pol(S)] = Pol(S) \neq P_k.$$

Т. е. при простых $k \geqslant 3$ система A не полна в P_k.

При $k = 2$ система $A = \{0, 1, x \cdot y\} \subseteq M$ не полна в P_2.

Предполные классы

Покажем, что любой предполный класс в P_k можно описать как множество всех функций, сохраняющих некоторое множество функций S, $S \subseteq P_k^{(m)}$.

Предполные классы

Если A — замкнутый класс и $n \geqslant 1$, то положим $A^{(n)} = A \cap P_k^{(n)}$.

Теорема 1. *Пусть $k \geqslant 2$, A — замкнутый класс в P_k, $m \geqslant 1$ и $A^{(m)} \neq \emptyset$, $A^{(m)} \neq P_k^{(m)}$. Тогда для множества функций*

$$S = A^{(m)} \subseteq P_k^{(m)}$$

верно:

1) $A \subseteq Pol(S)$;

2) *если A — предполный класс, то $A = Pol(S)$.*

Предполные классы

Доказательство. 1. Пусть A — замкнутый класс и $f(x_1, \dots, x_n) \in A$.

Если $g_1, \dots, g_n \in S$, то

$$f(g_1(z_1, \dots, z_m), \dots, g_n(z_1, \dots, z_m)) \in [A],$$

Но A — замкнутый класс, поэтому $[A] = A$.

Получаем: $f(g_1, \dots, g_n) \in S$ и $f \in Pol(S)$.

Значит, $A \subseteq Pol(S)$.

Предполные классы

Доказательство. 2. Пусть теперь A — предполный класс и $h(x_1, \ldots, x_m) \notin A$ (такая функция h найдется).

В силу $z_1, \ldots, z_m \in S$ верно

$$h(z_1, \ldots, z_m) \notin S,$$

т. к. $h \notin A$. Значит, $h \notin Pol(S)$ и $Pol(S) \neq P_k$.

Из п. 1 получаем:

$$A \subseteq Pol(S) \neq P_k.$$

Значит, $A = Pol(S)$.

$\square$

Основной инвариант предполного класса

Пусть $k \geqslant 2$, $A \subseteq P_k$ и A — предполный класс, для которого верно следующее:

1) для числа m, $m \geqslant 1$, класс A содержит какие-то функции m переменных, но не **не все** (т. е. $A^{(m)} \neq \emptyset$, $A^{(m)} \neq P_k^{(m)}$);
2) для любого числа l, $l = 1, \ldots, m-1$, класс A содержит **все** функции l переменных (т. е. $A^{(l)} = P_k^{(l)}$).

Тогда **основным инвариантом** класса A назовем множество

$$S_A = A^{(m)} \subseteq P_k^{(m)}.$$

Из теоремы 1 следует, что

$$A = Pol(S_A).$$

Предполные классы в P_2

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

A	$A \cap P_2^{(1)}$
T_0	$0, x$
T_1	$1, x$
L	$0, 1, x, \bar{x} = x \oplus 1$
S	$x, \bar{x}$
M	$0, 1, x$

Предполный класс T_0 в P_2

Предполный класс T_0 функций, сохраняющих 0.

Рассмотрим $T_0 \subseteq P_2$. Тогда:

$$S_{T_0} = T_0^{(1)} = \{0, z\}.$$

Поэтому

$$T_0 = Pol(S_{T_0}) = Pol(\{0, z\}).$$

Предполный класс T_1 в P_2

Предполный класс T_1 функций, сохраняющих 1.

Рассмотрим $T_1 \subseteq P_2$. Тогда:

$$S_{T_1} = T_1^{(1)} = \{1, z\}.$$

Поэтому

$$T_1 = Pol(S_{T_1}) = Pol(\{1, z\}).$$

Предполный класс S в P_2

Предполный класс S самодвойственных функций.

Рассмотрим $S \subseteq P_2$. Тогда:

$$S_S = S^{(1)} = \{z, \bar{z}\}.$$

Поэтому

$$S = Pol(S_S) = Pol(\{z, \bar{z}\}).$$

Предполный класс M в P_2

Предполный класс M монотонных функций.

Рассмотрим $M \subseteq P_2$. Тогда:

$$S_M = M^{(1)} = \{0, 1, z\}.$$

Поэтому

$$M = Pol(S_M) = Pol(\{0, 1, z\}).$$

Предполный класс L в P_2

Предполный класс L линейных функций.

Рассмотрим $L \subseteq P_2$. Тогда:

$$S_L = L^{(2)} = \{0, 1, z_1, \bar{z}_1, z_2, \bar{z}_2, z_1 \oplus z_2, \overline{z_1 \oplus z_2}\}.$$

Поэтому

$$L = Pol(S_L) = Pol(\{0, 1, z_1, \bar{z}_1, z_2, \bar{z}_2, z_1 \oplus z_2, \overline{z_1 \oplus z_2}\}).$$

Описание предполных классов

Следствие 1.2. *Пусть $k \geqslant 2$. Любой предполный класс A в P_k может быть описан как $A = Pol(S)$, где $S = A^{(m)}$ для некоторого числа m, где $m \leqslant 2$.*

Доказательство. По теореме 1 верно $A = Pol(S)$, где $S = A^{(m)}$ для любого такого числа m, что $A^{(m)} \neq \emptyset$, $A^{(m)} \neq P_k^{(m)}$.

Заметим, что для любого предполного класса A верно $I_k \subseteq A$, а также верно $A^{(2)} \neq P_k^{(2)}$, т. к. функция Вебба $V_k(x_1, x_2)$ образует полную систему, т. е. $V_k \notin A$.

Значит, для любого предполного класса A верно $A = Pol(S)$ для $S = A^{(m)}$, где $m \leqslant 2$.

$\square$

Описание предполных классов

Мы показали, что в P_k любой предполный класс может быть описан как множество всех полиморфизмов некоторого множества S, $S \subseteq P_k^{(m)}$, где $m \leqslant 2$.

Далее мы установим, что в P_k при $k \geqslant 3$ любой предполный класс может быть описан множеством S, $S \subseteq P_k^{(m)}$, где $m = 1$.

Перестановки

Пусть $f(x) \in P_k$.

Функция f называется **перестановкой** (на E_k), если f является взаимно однозначным отображением (т. е. принимает все k значений из E_k).

Пусть S_k обозначает множество всех перестановок из P_k.

Пусть CS_k обозначает множество всех функций одной переменной из P_k, которые не являются перестановками.

Перестановки

Пример. Пусть $k = 5$.

x	f_1	f_2
0	1	0
1	2	1
2	3	4
3	4	4
4	0	1

Тогда $f_1(x) = \bar{x} \in S_5$ и $f_2(x) = x^2 \in CS_5$.

Предполные классы

Теорема 2. *Пусть* $k \geqslant 3$, $A \subseteq P_k$ *— замкнутый класс,* $A \neq P_k$ *и* $A^{(1)} = P_k^{(1)}$. *Тогда*

1) $A \subseteq Pol(CS_k)$;

2) *если* A *— предполный класс, то* $A = Pol(CS_k)$.

Предполные классы

Доказательство. 1. 1) Пусть $f(x) \in P_k^{(1)}$.

Если $g \in CS_k$, то $f(g(z)) = h(z) \in CS_k$, т. к. g принимает не все значения из E_k.

2) Пусть $f(x_1, \ldots, x_n) \in A$ — существенная функция. Тогда f принимает не более $(k-1)$ значений, т. к. иначе по критерию Яблонского (или критерию Слупецкого) $A = [A] = P_k$, что не так.

Если $g_1, \ldots, g_n \in CS_k$, то

$$f(g_1(z), \ldots, g_n(z)) = h(z) \in CS_k,$$

т. к. f принимает не все значения из E_k.

Значит, в обоих случаях $f \in Pol(CS_k)$, поэтому $A \subseteq Pol(CS_k)$.

Предполные классы

Доказательство. 2. Пусть теперь A — предполный класс.

Пусть $h(x_1, \ldots, x_m) \in P_k$ — произвольная существенная функция, принимающая все k значений. Тогда $h \notin A$.

По основной лемме для существенной функции h найдутся такие k наборов $\delta_0, \delta_1, \ldots, \delta_{k-1} \in E_k^n$, что

1) $h(\delta_a) = a$, где $a \in E_k$ (на наборах $\delta_0, \delta_1, \ldots, \delta_{k-1}$ функция h принимает k различных значений $0, 1, \ldots, k-1$);

2) для множества $G_i = \{\delta_{0,i}, \delta_{1,i}, \ldots, \delta_{k-1,i}\}$ верно $|G_i| \leqslant k-1$, где $i = 1, \ldots, n$.

Предполные классы

Рассмотрим такие функции $g_a \in P_k^{(1)}$, где $a \in E_k$, что $\alpha_{g_a} = (\delta_{0,i}, \delta_{1,i}, \ldots, \delta_{k-1,i}) \in E_k^k$ (т. е. вектор значений функции g_a — в точности набор $(\delta_{0,i}, \delta_{1,i}, \ldots, \delta_{k-1,i}) \in E_k^k$).

δ_a	$a \in E_k$	g_1	g_2	$\ldots$	g_n	$h(\delta_a)$
δ_0	0	$\delta_{0,1}$	$\delta_{0,2}$	$\ldots$	$\delta_{0,n}$	0
δ_1	1	$\delta_{1,1}$	$\delta_{1,2}$	$\ldots$	$\delta_{1,n}$	1
$\ldots$						
δ_{k-1}	$k-1$	$\delta_{k-1,1}$	$\delta_{k-2,2}$	$\ldots$	$\delta_{k-1,n}$	$k-1$
		G_1	G_2	$\ldots$	G_n	E_k

Тогда $g_0, g_1, \ldots, g_{k-1} \in CS$, но

$$h(g_0(z), g_1(z), \ldots, g_{k-1}(z)) = z \notin CS,$$

а значит, $h \notin Pol(CS)$ и $Pol(CS) \neq P_k$.

Предполные классы

Из п. 1 получаем:

$$A \subseteq Pol(CS) \neq P_k.$$

Значит, $A = Pol(CS)$.

$\square$

Предполный класс, содержащий $P_k^{(1)}$

Из теоремы 2 получаем, что в P_k существует **ровно один** предполный класс, содержащий все функции одной переменной.

При $k \geqslant 3$ опишем его я явном виде.

Класс Слупецкого в P_k

В P_k при $k \geqslant 3$ рассмотрим замкнутый класс A, состоящий в точности из

1) **всех** функций одной переменной и

2) **всех** функций любого числа переменных, принимающих не более $(k-1)$ различных значений.

Он называется **класс Слупецкого**.

Предполный класс Слупецкого в P_k

Предложение 5. *Класс Слупецкого является предполным классом в P_k при $k \geqslant 3$.*

Доказательство.
1. $[A] = A \neq P_k$, т. е. A — неполная система в P_k.

2. Если $f \notin A$, то f — существенная функция, принимающая все k значений.

Тогда по критерию Слупецкого $[A \cup \{f\}] = P_k$, т. е. при добавлении к множеству A любой не принадлежащей ему функции получается полная система.

Т. е. A — предполный класс.

$\square$

Теорема Кузнецова

Теорема 3 (А. В. Кузнецова о предполных классах в P_k). *Пусть $k \geqslant 3$. В P_k существует конечное число предполных классов. Более того, если A — предполный класс в P_k, то*

1) *при $A^{(1)} \neq P_k^{(1)}$ выполняется $A = Pol(A^{(1)})$;*

2) *при $A^{(1)} = P_k^{(1)}$ выполняется $A = Pol(CS)$, и в этом случае A — предполный класс Слупецкого.*

Доказательство. Теорема следует из теорем 1 и 2 и предложения 5.

$\square$

Явное описание предполных классов

Можно ли явно описать свойства функций, составляющих каждых предполный класс в P_k (например, как в P_2)?

Да, для каждого $k \geqslant 3$ каждый предполный класс в P_k можно задать как множество функций, сохраняющих определенный предикат.

Явное описание предполных классов

Классы сохранения множества $T_k(E)$ и сохранения разбиения $U_k(D)$, не совпадающие с P_k, являются предполными в P_k.

Но это не все предполные классы в P_k.

Явное описание предполных классов

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

Завершил описание предполных классов в P_k при $k \geqslant 3$ И. Розенберг.

Литература к лекции

1. Марченков С.С. Основы теории булевых функций. М.: Физматлит, 2014. Гл. IV, с. 66–82.

2. Яблонский С.В., Гаврилов Г.П., Набебин А.А. Предполные классы в многозначных логиках. М.: МЭИ, 1997. С. 24–26.

3. Lau D. Function Algebras on Finite Sets. Springer, 2006. P. 125–126, 130–131.