Лекция 4. Особенности многозначных логик. Замкнутый класс, базис замкнутого класса. Теоремы Янова и Мучника о существовании в многозначных логиках замкнутых классов без базиса и замкнутых классов со счетным базисом. Классы функций, сохраняющих предикат, их замкнутость. Соответствие Галуа.

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

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.su

Базис замкнутого класса

Пусть A, $A \subseteq P_k$, — замкнутый класс, и $B \subseteq A$.
Множество B называется **базисом** класса A, если
1) $[B] = A$, т.е. система B **полна** в A;
2) для каждой функции $f \in B$ верно $[B \setminus \{f\}] \neq A$, т.е. система B **неизбыточна** в A.

В P_2 каждый базис всего класса P_2 содержит не более 4-х функций.
Э. Пост доказал, что в P_2 каждый замкнутый класс имеет **конечный** базис.

Теорема Янова

Теорема 1 (Ю.И. Янова). *В P_k при $k \geq 3$ существует замкнутый класс, не имеющий базиса.*

Доказательство. Пусть $k \geq 3$. Рассмотрим множество функций $\{f_0, f_1, f_2, \dots\} \subseteq P_k$:

$$f_0 = 0,$$

$$f_i(x_1, \dots, x_i) = \begin{cases} 1, & x_1 = \dots = x_i = 2, \\ 0, & \text{иначе.} \end{cases}$$

Пусть $A = [\{f_0, f_1, f_2, \dots\}]$.
Заметим, что

$$f_i(\dots, f_j, \dots) = 0.$$

Поэтому в классе A содержатся только функции, конгруэнтные функциям $f_0, f_1, f_2, \dots$.

Теорема Янова

Докажем от противного, что замкнутый класс A не имеет базиса.
Пусть $B \subseteq A$ – базис класса A, и f_{n_0} — функция с наименьшим индексом в базисе B.
Возможны два случая.

Теорема Янова

Доказательство.
1. В базисе B есть еще хотя бы одна функция f_{n_1}, где $n_1 > n_0$. Но тогда противоречие с п. 2 определения базиса, т.к.

$$f_{n_0}(x_1, \dots, x_{n_0}) = f_{n_1}(x_1, \dots, x_{n_0}, x_{n_0}, \dots, x_{n_0}).$$

Теорема Янова

Доказательство.
2. В базисе B есть только функция f_{n_0}. Но тогда противоречие с п. 1 определения базиса, а именно, никакая функция f_n при $n > n_0$ не может быть получена, т.к.

$$f_{n_0}(\ldots, f_{n_0}, \ldots) = 0.$$

Значит, класс A не имеет базиса. □

Теорема Мучника

Теорема 2 (А.А. Мучника). *В P_k при $k \geq 3$ существует замкнутый класс, имеющий счетный базис.*

Доказательство. Пусть $k \geq 3$. Рассмотрим множество функций $\{f_2, f_3, \ldots\} \subseteq P_k$:

$$f_i(x_1, \ldots, x_i) = \begin{cases} 1, & x_1 = \ldots = x_{j-1} = x_{j+1} = \ldots = 2, x_j = 1, \\ & j = 1, \ldots, i, \\ 0, & \text{иначе.} \end{cases}$$

Пусть $A = [\{f_2, f_3, \ldots\}]$.

Докажем, что $B = \{f_2, f_3, \ldots\}$ — базис замкнутого класса A.

Докажем от противного, что для каждого $n_0 = 2, 3, \ldots$ функция f_{n_0} не задается формулой над множеством $B \setminus \{f_{n_0}\}$.

Теорема Мучника

Доказательство.
Пусть
$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(F_1, \ldots, F_{n_1}).$$
Возможны три случая.

Теорема Мучника

Доказательство.
Пусть
$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(F_1, \ldots, F_{n_1}).$$

1. Среди формул $F_1, \ldots, F_{n_1}$ не менее двух, которые не являются переменными:

$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(\ldots, f_i, \ldots, f_j, \ldots).$$

Но тогда противоречие на наборе $(1, 2, \ldots, 2) \in E_k^{n_0}$, т.к.

$$1 = f_{n_0}(1, 2, \ldots, 2) = f_{n_1}(\ldots, \{0, 1\}, \ldots, \{0, 1\}, \ldots) = 0.$$

Теорема Мучника

Доказательство.
Пусть
$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(F_1, \ldots, F_{n_1}).$$

2. Среди формул $F_1, \ldots, F_{n_1}$ только одна, которая не является переменной. Т.к. $n_1 \geq 2$, хотя бы одна формула равна переменной, например, x_1:

$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(\ldots, x_1, \ldots, f_i, \ldots).$$

Но тогда противоречие на наборе $(1, 2, \ldots, 2) \in E_k^{n_0}$, т.к.

$$1 = f_{n_0}(1, 2, \ldots, 2) = f_{n_1}(\ldots, 1, \ldots, \{0, 1\}, \ldots) = 0.$$

Теорема Мучника

Доказательство.
Пусть

$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(F_1, \ldots, F_{n_1}).$$

3. Все формулы $F_1, \ldots, F_{n_1}$ являются переменными. Тогда $n_1 > n_0$, и хотя бы одна переменная встречается по меньшей мере дважды, например, x_1:

$$f_{n_0}(x_1, \ldots, x_{n_0}) = f_{n_1}(\ldots, x_1, \ldots, x_1, \ldots).$$

Но тогда противоречие на наборе $(1, 2, \ldots, 2) \in E_k^{n_0}$, т.к.

$$1 = f_{n_0}(1, 2, \ldots, 2) = f_{n_1}(\ldots, 1, \ldots, 1, \ldots) = 0.$$

Значит, B — неизбыточная система. Отсюда B — базис замкнутого класса A.

$\square$

Мощность множества замкнутых классов в P_k при $k \geq 3$

Теорема 3. *В P_k при $k \geq 3$ существует континум замкнутых классов.*

Доказательство. Пусть $k \geq 3$. Рассмотрим множество функций $\{f_2, f_3, \dots\} \subseteq P_k$ из доказательства теоремы Мучника. Для каждой бесконечной возрастающей последовательности натуральных чисел

$$\nu = n_1, n_2, \dots,$$

где $n_1 \geq 2$, построим замкнутый класс

$$A_\nu = [\{f_{n_1}, f_{n_2}, \dots\}].$$

Тогда, если последовательности ν_1 и ν_2 различны, то $A_{\nu_1} \neq A_{\nu_2}$.

Значит, построены континум различных замкнутых классов в P_k при $k \geq 3$. $\square$

Э. Пост доказал, что в P_2 существует только **счетное** число замкнутых классов.

Предикат

Отображение $\rho : E_k^h \to \{0,1\}$ называется h-местным **предикатом** на множестве E_k.

Пусть R_k^h обозначает множество всех h-местных предикатов на E_k, и $R_k = \bigcup\limits_{h \geq 0} R_k^h$.

Если $\alpha_j = (a_1^{(j)}, \ldots, a_n^{(j)}) \in E_k^n$, $j = 1, \ldots, h$, то положим

$$\rho(\alpha_1, \ldots, \alpha_h) = 1,$$

если

$$\rho(a_i^{(1)}, \ldots, a_i^{(h)}) = 1$$

для всех $i = 1, \ldots, n$.

Сохранение функцией предиката

Функция $f(x_1, \dots, x_n) \in P_k$ **сохраняет** предикат $\rho \in R_k^h$, если для произвольных h наборов $\alpha_j = (a_1^{(j)}, \dots, a_n^{(j)}) \in E_k^n$, $j = 1, \dots, h$, из

$$\rho(\alpha_1, \dots, \alpha_h) = 1$$

следует

$$\rho(f(\alpha_1), \dots, f(\alpha_h)) = 1.$$

Инварианты и полиморфизмы

Если функция $f \in P_k$ сохраняет предикат $\rho \in R_k$, то предикат ρ называется **инвариантом** функции f, а функция f называется **полиморфизмом** предиката ρ.

Множество всех инвариантов функции $f \in P_k$ обозначается как $\mathrm{Inv}(f)$, и если $A \subseteq P_k$, то $\mathrm{Inv}(A) = \bigcap\limits_{f \in A} \mathrm{Inv}(f)$.

Множество всех полиморфизмов предиката $\rho \in R_k$ обозначается как $\mathrm{Pol}(\rho)$, и если $S \subseteq R_k$, то $\mathrm{Pol}(S) = \bigcap\limits_{\rho \in S} \mathrm{Pol}(\rho)$.

Замкнутость множества полиморфизмов

Теорема 4. *Если* $\rho \in R_k$, *то* $\mathrm{Pol}(\rho)$ *— замкнутый класс.*
Доказательство. Пусть $\rho \in R_k^h$. Заметим, что $x \in \mathrm{Pol}(\rho)$.
Пусть $f_0(y_1, \dots, y_m) \in \mathrm{Pol}(\rho)$, и $f_i(x_1, \dots, x_n) \in \mathrm{Pol}(\rho)$, 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 $\alpha_1, \dots, \alpha_h \in E_k^n$ и $\rho(\alpha_1, \dots, \alpha_h) = 1$, то

$$\begin{array}{rcl} f(\alpha_1) & = & f_0(f_1(\alpha_1), \dots, f_m(\alpha_1)) = f_0(\gamma_1), \\ & \dots & , \\ f(\alpha_h) & = & f_0(f_1(\alpha_h), \dots, f_m(\alpha_h)) = f_0(\gamma_h), \end{array}$$

и $\rho(f(\alpha_1), \dots, f(\alpha_h)) = 1$, т.к. $\rho(\gamma_1, \dots, \gamma_h) = 1$.
Т.е. $f \in \mathrm{Pol}(\rho)$. $\square$

Функции, сохраняющие множество

Если $E \subseteq E_k$, то $T_k(E) = \mathrm{Pol}(\rho_E)$, где ρ_E — такой одноместный предикат, что $\rho_E(a) = 1$ при $a \in E$.

Значит, $T_k(E)$ — замкнутый класс.

Функции, сохраняющие разбиение

Если D — разбиение множества E_k, то $U_k(D) = \mathrm{Pol}(\rho_D)$, где ρ_D — такой двуместный предикат, что $\rho_D(a, b) = 1$ при $a \sim_D b$.

Значит, $U_k(D)$ — замкнутый класс.

Замкнутый класс предикатов

Определим предикат **равенства** $=(x, y) \in R_k$:

$$=(x, y) = 1 \Leftrightarrow x = y$$

и **тождественно ложный** предикат $0 \in R_k$.

Если $S \subseteq R_k$, то **замыканием** $[S]$ множества S назовем все те предикаты $\rho \in R_k$, которые можно выразить формулами вида

$$\rho(x_1, \ldots, x_h) =$$
$$\exists y_1 \ldots \exists y_l \rho_1(z_{1,1}, \ldots, z_{1,h_1}) \& \ldots \& \rho_m(z_{m,1}, \ldots, z_{m,h_m}),$$

где $\rho_1, \ldots, \rho_m \in S \subseteq \{=, 0\}$, $z_{j,i} \in \{x_1, \ldots, x_h, y_1, \ldots, y_l\}$.

Описание замкнутых классов

Теорема 5. *Если* $\{x\} \subseteq A \subseteq P_k$ *и* $S \subseteq R_k$, *то*

$$[A] = \mathrm{Pol}(\mathrm{Inv}(A)),$$

$$[S] = \mathrm{Inv}(\mathrm{Pol}(S)).$$

Литература к лекции

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001. Ч. I, гл. 2, с. 65–69.

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

Конец лекции