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.ru

Факультет ВМК МГУ имени М.В. Ломоносова

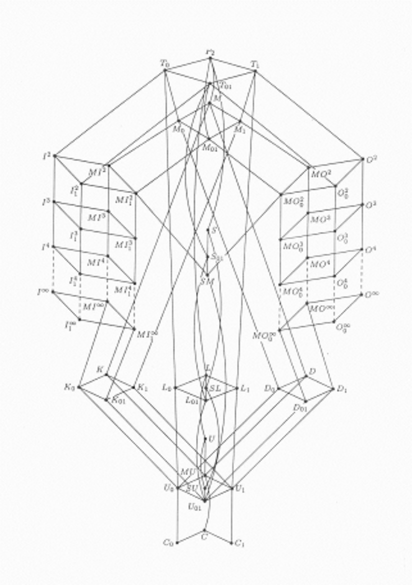
Лекции на сайте http://mk.cs.msu.ru

Замкнутый класс

Множество A, $A \subseteq P_k$, называется **замкнутым классом**, если $[A] = A$.

Э. Пост доказал, что в P_2 существует **счетное число** замкнутых классов и построил их **решетку** по включению.

Решетка замкнутых классов в P_2



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.

Любой базис всего класса P_2 содержит не более 4-х функций (т.е. является **конечным**).

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 $\{f_0, f_1, f_2, \ldots\} \subseteq P_k$:

$$f_0 = 0,$$

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

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

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

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

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.

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

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. $\square$

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 $A = [\{f_2, f_3, \ldots\}]$.

Теорема Мучника

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.
Предположим противное: 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 $n_1 > n_0$, поэтому 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.

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

Теорема Мучника

Значит, B — неизбыточная система.

Поэтому 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 $\{f_2, f_3, \ldots\} \subseteq P_k$ из доказательства теоремы Мучника. Для каждой бесконечной возрастающей последовательности натуральных чисел

$$\nu = n_1, n_2, \ldots,$$

где $n_1 \geq 2$, построим замкнутый класс

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

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 $k \geq 3$. $\square$

Предикат

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

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

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

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

если

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

для всех $i = 1, \ldots, n$.

Сохранение функцией предиката

Функция $f(x_1, \dots, x_n) \in P_k$ **сохраняет** предикат $\rho \in R_k^{(m)}$, если для произвольных m наборов $\alpha_1, \dots, \alpha_m \in E_k^n$ из

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

следует

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

Инвариантные предикаты и полиморфизмы

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

Множество всех предикатов, инвариантных относительно функции $f \in P_k$, обозначается через $\mathrm{Inv}(f)$, 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 через $\mathrm{Pol}(\rho)$, 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 $\rho \in R_k^{(m)}$. Заметим, что $x \in \mathrm{Pol}(\rho)$.
Пусть $f_0(y_1, \ldots, y_t) \in \mathrm{Pol}(\rho)$, и $f_i(x_1, \ldots, x_n) \in \mathrm{Pol}(\rho)$, где $i = 1, \ldots, t$.
Рассмотрим функцию
$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_t(x_1, \ldots, x_n))$.
Тогда если $\alpha_1, \ldots, \alpha_m \in E_k^n$ и $\rho(\alpha_1, \ldots, \alpha_m) = 1$, то

$$\begin{array}{rcl} f(\alpha_1) & = & f_0(f_1(\alpha_1), \ldots, f_t(\alpha_1)) = f_0(\gamma_1), \\ \ldots & & , \\ f(\alpha_m) & = & f_0(f_1(\alpha_m), \ldots, f_t(\alpha_m)) = f_0(\gamma_m), \end{array}$$

и $\rho(f(\alpha_1), \ldots, f(\alpha_m)) = 1$, т.к. $\rho(\gamma_1, \ldots, \gamma_m) = 1$.
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, по теореме 4 $T_k(E)$ — 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, по теореме 4 $U_k(D)$ — замкнутый класс.

Замкнутый класс предикатов

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

$$\rho(x_1, \dots, x_m) =$$
$$\exists y_1 \dots \exists y_l \left(\rho_1(z_{1,1}, \dots, z_{1,m_1}) \& \dots \& \rho_t(z_{t,1}, \dots, z_{t,m_t})\right),$$

где $\rho_1, \dots, \rho_t \in S \cup \{=, 0\}$, $z_{j,i} \in \{x_1, \dots, x_m, y_1, \dots, y_l\}$.

Описание замкнутых классов

Теорема 5.
1. *Если множество* A, $A \subseteq P_k$, *содержит тождественную функцию, то*

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

2. *Если* $S \subseteq R_k$, *то*

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

Соответствие Галуа

Теорема 6.
1. *Если A и B, где $A, B \subseteq P_k$, — замкнутые классы, содержащие тождественную функцию, и $A \subseteq B$, то*

$$\mathrm{Inv}(B) \subseteq \mathrm{Inv}(A).$$

2. *Если S и T, где $S, T \subseteq R_k$, — замкнутые классы предикатов и $S \subseteq T$, то*

$$\mathrm{Pol}(T) \subseteq \mathrm{Pol}(S).$$

Соответствие Галуа

Соответствие Галуа означает, что решетки замкнутых классов в P_k, содержащих тождественную функцию, и замкнутых классов предикатов в R_k являются **антиизоморфными**.

Из результатов Э. Поста следует, что в R_2 существует **счетное число** замкнутых классов предикатов.

Из теоремы 3 следует, что в R_k при $k \geq 3$ существует **континум** замкнутых классов предикатов.

Задача обобщенной выполнимости

Пусть $S \subseteq R_k$. Задача **обобщенной выполнимости** над S состоит в том, чтобы по системе условий из S, связывающих какие-то переменные, выяснить, можно ли подобрать такие значения этих переменных, чтобы все условия выполнялись.

Задача обобщенной выполнимости

1. Задача **выполнимости 3-КНФ**:
$S = \{x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee x_3^{\sigma_3} \mid \sigma_1, \sigma_2, \sigma_3 \in E_2\} \subseteq R_2$.

Пример задачи **выполнимости 3-КНФ**.

$$K_1(x_1, x_2, x_3, x_4) = (x_1 \vee \bar{x}_2 \vee x_3)(\bar{x}_1 \vee x_2 \vee \bar{x}_4)(\bar{x}_2 \vee \bar{x}_3 \vee x_4).$$

Несложно проверить, что $K_1(1, 1, 0, 0) = 1$, т.е. КНФ K_1 — выполнима.

Задача обобщенной выполнимости

2. Задача **выполнимости 2-КНФ**:
$S = \{x_1^{\sigma_1} \vee x_2^{\sigma_2} \mid \sigma_1, \sigma_2 \in E_2\} \subseteq R_2$.

Пример задачи **выполнимости 2-КНФ**.

$$K_2(x_1, x_2) = (\bar{x}_1 \vee \bar{x}_2)(\bar{x}_1 \vee x_2)(x_1 \vee \bar{x}_2)(x_1 \vee x_2).$$

Можно проверить, что $K_2 = 0$, т.е. КНФ K_2 не является выполнимой.

Задача обобщенной выполнимости

3. Пусть $S = \{x_1 \neq x_2\} \subseteq R_k$, $k \geq 2$.

Пример

$$K_3(x_1, x_2, x_3) = (x_1 \neq x_2)(x_2 \neq x_3)(x_3 \neq x_1).$$

Можно проверить, что $K_3 = 0$ при $k = 2$ и $K_3(0, 1, 2) = 1$ при $k \geq 3$.

Т.е. K_3 не является выполнимой при $k = 2$ и K_3 — выполнима при $k \geq 3$.

Задача обобщенной выполнимости

Можно ли для каждого $S \subseteq R_k$ найти **общий алгоритм**, который по каждой системе K условий из S, связывающих какие-то переменные, выясняет, найдутся ли такие значения этих переменных, чтобы все условия выполнялись?

Такой алгоритм существует: надо перебрать все возможные k^n наборов значений переменных $x_1, \ldots, x_n$ из системы K и проверить, выполняются ли все условия из K на каком-то из этих наборов.

Однако трудоемкость такого алгоритма велика.

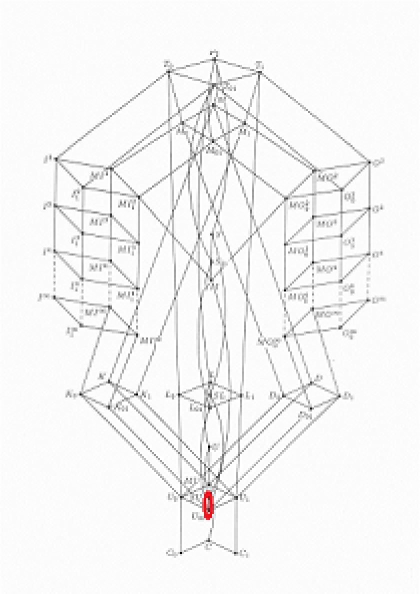
Задача обобщенной выполнимости

А можно ли построить **быстрый (полиномиальный)** алгоритм?

Оказывается, что при каждом S, $S \subseteq R_k$, существование быстрого алгоритма для задачи обобщенной выполнимости над S или **труднорешаемость** этой задачи зависят только от **наличия определенных функций** в множестве $\mathrm{Pol}(S)$.

Это теорема о **дихотомии** вычислительной сложности задачи обобщенной выполнимости.

Дихотомия в P_2



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.

3. Горшков С.П., Тарасов А.В. Сложность решения систем булевых уравнений. М.: Курс, 2017.

Конец лекции