# Лекция 11. Предикаты на конечном множестве. Формулы, $S$-формулы и замкнутые классы предикатов. Задача обобщенной выполнимости $S$-*ВЫП*. Сложность некоторых задач $S$-*ВЫП*.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

# Предикат

Пусть $k \geqslant 2$ — целое число, $E_k = \{0, 1, \ldots, k-1\}$.

Отображение $g : E_k^n \to E_2$ называется $n$-местным **предикатом** на множестве $E_k$, $n \geqslant 0$.

Множество всех $n$-местных предикатов на $E_k$ обозначим $R_k^{(n)}$.

Пусть $R_k = \bigcup\limits_{n \geqslant 0} R_k^{(n)}$ — множество всех предикатов на $E_k$.

# Ложный и истинный предикаты

Предикат, равный 0 на любом наборе, называется **тождественно ложным** и обозначается 0.

Предикат, равный 1 на любом наборе, называется **тождественно истинным** и обозначается 1.

# Операции над предикатами

Если $g, h \in R_k$, то $\bar{g}$, $g \& h$, $g \vee h$ обозначают **отрицание**, **конъюнкцию** и **дизъюнкцию** соответствующих предикатов (при этом знак & будем заменять на $\cdot$ или вообще пропускать).

# Множества единиц и нулей предиката

Если $g \in R_k^{(n)}$ и $a \in E_2$, то

$$N_a(g) = \{\alpha \in E_k^n \mid g(\alpha) = a\}$$

множество всех наборов из $E_k^n$, на которых предикат $g$ принимет значение $a$.

# Формула для предикатов

Пусть $S \subseteq R_k$, причем в $S$ каждый предикат имеет свое, отличное от других предикатов обозначение. Для предикатов по индукции определим понятие **формулы** над множеством $S$.

*Базис индукции.*

*1.* Если $g$ — обозначение $n$-местного предиката из $S$ и $x_{i_1}, \ldots, x_{i_n}$ — (не обязательно различные) переменные, то выражение $g(x_{i_1}, \ldots, x_{i_n})$ — формула.

*2.* Если $x_i, x_j$ — (не обязательно различные) переменные, то выражение $x_i = x_j$ — формула.

*Индуктивный переход.*

*1.* Если $G_1$ и $G_2$ — формулы, то выражение $G_1 \cdot G_2$ — формула.

*2.* Если $G_1$ — формула и $x_i$ — переменная, то выражение $\exists x_i(G_1)$ — формула.

# Предикат, определяемый формулой

Каждая формула $G$ над множеством $S$, где $S \subseteq R_k$, задает некоторый предикат $g_G \in R_k$.

*Базис индукции.*

*1.* Если $g$ — обозначение $n$-местного предиката из $S$, то формула $g(x_{i_1}, \ldots, x_{i_n})$ определяет предикат $g(x_{i_1}, \ldots, x_{i_n}) \in R_k$.

*2.* Если $x_i, x_j$ — переменные, то формула $x_i = x_j$ определяет предикат $d(x_i, x_j) \in R_k$ с

$$N_1(d) = \{(a, a) \in E_k^2 \mid a \in E_k\}.$$

# Предикат, определяемый формулой

Каждая формула $G$ над множеством $S$, где $S \subseteq R_k$, задает некоторый предикат $g_G \in R_k$.

*Индуктивный переход.*

*1.* Если $G_1, G_2$ — формулы, определяющие соответственно предикаты $g_1, g_2 \in R_k$, то формула $G = G_1 \cdot G_2$ определяет предикат $g = g_1 \cdot g_2 \in R_k$.

*2.* Если $G_1$ — формула, определяющая предикат $g_1(x_1, \ldots, x_n) \in R_k$, то формула $G = \exists x_i (G_1)$ определяет предикат

$$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \bigvee_{a \in E_k} g_1(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \in R_k.$$

# Предикат, определяемый формулой

**Пример**. Пусть $k = 2$ и

$$S = \{x_1^{\sigma_1} \vee x_2^{\sigma_2} \vee x_3^{\sigma_3} \mid \sigma_1, \sigma_2, \sigma_3 \in E_2\} \subseteq R_2.$$

Тогда формула

$$G(x_1, x_2, x_3, x_4) = \exists y (x_1 \vee x_2 \vee y)(\bar{y} \vee x_3 \vee x_4)$$

над множеством $S$ определяет предикат

$$\begin{aligned} g(x_1, x_2, x_3, x_4) &= (x_1 \vee x_2 \vee 0)(\bar{0} \vee x_3 \vee x_4) \vee \\ &\vee (x_1 \vee x_2 \vee 1)(\bar{1} \vee x_3 \vee x_4) = \\ &= x_1 \vee x_2 \vee x_3 \vee x_4 \in R_2. \end{aligned}$$

# Соглашение для формул и предикатов

Как правило, мы не будем различать формулы и определяемые ими предикаты (если это не приводит к путанице).

В частности, если $G(x_1, \dots, x_n)$ — формула, определяющая предикат $g_G(x_1, \dots, x_n) \in R_k$, то вместо $g_G(\alpha)$, где $\alpha \in E_k^n$, будем писать $G(\alpha)$.

# Замыкание множества предикатов

Пусть $S \subseteq R_k$.

**Замыканием** $\langle S \rangle \subseteq R_k$ множества $S$ называется множество всех предикатов $g \in R_k$, которые можно выразить формулами над $S \cup \{0\}$, где $0$ — тождественно ложный предикат.

# Замыкание множества предикатов

Другими словами, **замыканием** множества $S \subseteq R_k$ является множество $\langle S \rangle \subseteq R_k$, состоящее из предикатов, которые можно получить из $S \cup \{0, =_k\}$ при помощи

1) переименования переменных с возможным отождествлением (в том числе, удаления несущественных переменных),
2) добавления несущественных переменных,
3) конъюнкции
4) и квантора существования.

# Замкнутый класс предикатов

Множество $S \subseteq R_k$ называется **замкнутым классом предикатов**, если

$$\langle S \rangle = S.$$

Отметим, что любой замкнутый класс предикатов содержит тождественно ложный предикат 0, а также все *диагонали*, т. е. предикаты вида

$$d_\varepsilon(x_1, \dots, x_n) = \prod_{i \sim_\varepsilon j} (x_i = x_j),$$

где $\varepsilon$ — отношение эквивалентности на $\{1, 2, \dots, n\}$.

# $S$-формула

Пусть $S \subseteq R_k$. Формулу над множеством $S$ назовем $S$-**формулой**, если она построена только при помощи

1) *п. 1 базиса индукции* и
2) *п. 1 индуктивного перехода*

индуктивного определения формулы.

# $S$-формулы

**Пример**. Пусть $S = \{\neq_k\} \subseteq R_k$, где $\neq_k$ — предикат **неравенства** на множестве $E_k$.

Тогда $S$-формулами являются, например, следующие выражения:

$$\begin{aligned} K_1 &= (x_1 \neq_k x_2)(x_1 \neq_k x_3)(x_2 \neq_k x_3), \\ K_2 &= (x_1 \neq_k x_2)(x_1 \neq_k x_4)(x_2 \neq_k x_3)(x_3 \neq_k x_4). \end{aligned}$$

# Выполнимая $S$-формула

Если $S \subseteq R_k$, то $S$-формула $K(x_1, \dots, x_n)$ называется **выполнимой**, если найдется такой набор $\alpha \in E_k^n$, что $K(\alpha) = 1$.

Иначе $S$-формула $K(x_1, \dots, x_n)$ называется **невыполнимой**.

Невыполнимая $S$-формула $K(x_1, \dots, x_n)$ определяет тождественно ложный предикат.

# $S$-формулы

**Пример**. Пусть $S = \{\neq_k\} \subseteq R_k$, где $\neq_k$ — предикат **неравенства** на множестве $E_k$.

Тогда $S$-формула $K_1$,

$$K_1 = (x_1 \neq_k x_2)(x_1 \neq_k x_3)(x_2 \neq_k x_3),$$

является невыполнимой при $k = 2$ и является выполнимой при $k = 3$;

а $S$-формула $K_2$,

$$K_2 = (x_1 \neq_k x_2)(x_1 \neq_k x_4)(x_2 \neq_k x_3)(x_3 \neq_k x_4),$$

является выполнимой при $k = 2$ и при $k = 3$.

# Задача $S$-*ВЫП*

Пусть $S \subseteq R_k$. Определим задачу распознавания $S$-*ВЫП*, которая называется задачей **обобщенной выполнимости**, или **выполнимости ограничений**.

Задача $S$-*ВЫП*.

*Вход*: $S$-формула $K(x_1, \dots, x_n)$.

*Вопрос*: является ли $S$-формула $K$ выполнимой, т. е. найдется ли такой набор $\alpha \in E_k^n$, что $K(\alpha) = 1$?

# Полиномиальная сводимость

Пусть $\mathcal{Z}_1$ и $\mathcal{Z}_2$ — задачи распознавания.

Задача $\mathcal{Z}_1$ **полиномиально сводится** (**$P$-сводится**) к задаче $\mathcal{Z}_2$, если найдется такой полиномиальный алгоритм $\mathcal{A}$, который произвольный пример $z_1$ задачи $\mathcal{Z}_1$ преобразует в некоторый пример $z_2 = z_2(z_1)$ задачи $\mathcal{Z}_2$, при этом $z_2 \in L_{\mathcal{Z}_2}$ тогда и только тогда, когда $z_1 \in L_{\mathcal{Z}_1}$.

Отметим, что задача $\mathcal{Z}_1$ полиномиально сводится к задаче $\mathcal{Z}_2$, если при помощи полиномиального алгоритма для $\mathcal{Z}_2$ можно построить полиномиальный алгоритм для $\mathcal{Z}_1$.

# Полиномиальная сводимость задач

Пусть $\mathcal{Z}_1, \mathcal{Z}_2 \in NP$, $\mathcal{Z}_1$ $P$-сводится к $\mathcal{Z}_2$ и $\mathcal{Z}_2$ $P$-сводится к $\mathcal{Z}_1$.

Тогда

1) $\mathcal{Z}_1 \in P \Leftrightarrow \mathcal{Z}_2 \in P$;

2) $\mathcal{Z}_1$ — $NP$-полна $\Leftrightarrow \mathcal{Z}_2$ — $NP$-полна.

# Сложность задачи $\{\neq_k\}$-*ВЫП*

**Теорема 1**. *Задача* $\{\neq_k\}$-*ВЫП, где* $\neq_k$ — *предикат неравенства на множестве* $E_k$, *является полиномиальной при* $k = 2$ *и является* $NP$-*полной при* $k \geqslant 3$.

# Сложность задачи $\{\neq_k\}$-*ВЫП*

**Доказательство.** Покажем, что задачи обобщенной выполнимости $\{\neq_k\}$-*ВЫП* и $k$-раскраски графов $k$-*ВР* полиномиально сводятся друг к другу.

# Сложность задачи $\{\neq_k\}$-ВЫП

Покажем, что $k$-ВР $P$-сводится к $\{\neq_k\}$-ВЫП.

Если граф $G = (V, E)$ является примером задачи $k$-ВР, то $S$-формула

$$K_G = \prod_{(v_i, v_j) \in E} (v_i \neq_k v_j)$$

является примером задачи $\{\neq_k\}$-ВЫП.

При этом если $\rho : V \to E_k$ — раскраска графа $G$ в $k$-цветов, то

$$\alpha = (\rho(v_1), \dots, \rho(v_{|V|})) \in E_k^{|V|} -$$

набор, обращающий $S$-формулу $K_G$ в единицу.

Кроме того, построить $S$-формулу $K_G$ по графу $G$ можно полиномиальным алгоритмом.

# Сложность задачи $\{\neq_k\}$-*ВЫП*

Покажем, что $\{\neq_k\}$-*ВЫП* $P$-сводится к $k$-*ВР*.

Наоборот, если $S$-формула

$$K(x_1, \ldots, x_n) = \prod_{j=1}^{m} (x_{j_1} \neq_k x_{j_2})$$

является примером задачи $\{\neq_k\}$-*ВЫП*, то граф $G_K = (V_K, E_K)$, где

$$\begin{array}{rcl} V_K & = & \{x_1, \ldots, x_n\}, \\ E_K & = & \{(x_{j_1}, x_{j_2}) \mid j = 1, \ldots, m\}, \end{array}$$

является примером задачи $k$-*ВР*.

При этом если $\alpha \in E_k^n$ — набор, обращающий $S$-формулу $K$ в единицу, то $\rho : V_K \to E_k$, где $\rho(x_i) = \alpha_i$ для всех $i = 1, \ldots, n$, — раскраска графа $G_K$ в $k$-цветов.

Кроме того, построить граф $G_K$ по $S$-формуле $K$ можно полиномиальным алгоритмом.

# Сложность задачи $\{\neq_k\}$-*ВЫП*

Итак, задачи $\{\neq_k\}$-*ВЫП* и $k$-*ВР* $P$-сводятся друг к другу.

Поэтому

1) $\{\neq_k\}$-*ВЫП* $\in P \Leftrightarrow k$-*ВР* $\in P$;

2) $\{\neq_k\}$-*ВЫП* — $NP$-полна $\Leftrightarrow$ $k$-*ВР* — $NP$-полна.

Задача $k$-*ВР* является полиномиальной при $k = 2$ и является $NP$-полной при $k \geqslant 3$.

Значит, задача $\{\neq_k\}$-*ВЫП* является полиномиальной при $k = 2$ и является $NP$-полной при $k \geqslant 3$.

$\square$

# Сложность задач $S$-*ВЫП*

**Теорема 2**. *Пусть* $S, T \subseteq R_k$, $S, T$ *— конечны,* $0 \in S$ *и* $T \subseteq \langle S \rangle$. *Тогда задача* $T$-*ВЫП* $P$-*сводится к задаче* $S$-*ВЫП*.

# Сложность задач $S$-*ВЫП*

**Доказательство**. Покажем, что задача $T$-*ВЫП* $P$-сводится к задаче $S$-*ВЫП*.

Из $T \subseteq \langle S \rangle$ следует, что любой предикат $h \in T$ можно выразить некоторой формулой $H$ над множеством $S$.

# Сложность задач $S$-ВЫП

Можно считать, что предикат $h(x_1, \ldots, x_n) \in T$ задается формулой следующего вида:

$$H = \exists y_1 \ldots \exists y_p G(x_1, \ldots, x_n, y_1, \ldots, y_p)$$

где $G$ — формула без кванторов существования.

Все кванторы существования можно вынести в начало, т. к. всегда можно построить формулу, в которой разные кванторы существования связывают разные переменные.

# Сложность задач $S$-ВЫП

Пусть $T$-формула

$$K_1(x_1, \ldots, x_n) = \prod_{j=1}^{m} h_j(x_{j,1}, \ldots, x_{j,n_j}),$$

является примером задачи $T$-ВЫП.

Каждый предикат $h_j \in T$ задается формулой $H_j$ над множеством $S$, где

$$H_j = \exists y_{j,1} \ldots \exists y_{j,p_j} G_j(x_{j,1}, \ldots, x_{j,n_j}, y_{j,1}, \ldots, y_{j,p_j})$$

и $G_j$ — формула без кванторов существования.

Можно считать, что при $j_1 \neq j_2$ множества переменных $\{y_{j_1,1}, \ldots, y_{j_1,p_{j_1}}\}$ и $\{y_{j_2,1}, \ldots, y_{j_2,p_{j_2}}\}$ не пересекаются.

# Сложность задач $S$-ВЫП

Итак, каждый предикат $h_j \in T$ задается формулой $G_j$, где

$$G_j = \exists y_{j,1} \ldots \exists y_{j,p_j} G_j(x_{j,1}, \ldots, x_{j,n_j}, y_{j,1}, \ldots, y_{j,p_j}).$$

Рассмотрим формулу над $S$

$$G = H_1 \cdot \ldots \cdot H_m = \exists y_1 \ldots \exists y_p \prod_{j=1}^{m} G_j(x_{j,1}, \ldots, x_{j,n_j}, y_{j,1}, \ldots, y_{j,p_j}),$$

где

$$\{y_1, \ldots, y_p\} = \bigcup_{j=1}^{m} \{y_{j,1}, \ldots, y_{j,p_j}\}.$$

Все кванторы существования можно вынести в начало, т. к.

$\{y_{j_1,1}, \ldots, y_{j_1,p_{j_1}}\}$ и $\{y_{j_2,1}, \ldots, y_{j_2,p_{j_2}}\}$ не пересекаются при $j_1 \neq j_2$.

Заметим, что формулы $G$ и $K_1$ задают один и тот же предикат.

# Сложность задач $S$-ВЫП

Итак, получили формулу над $S$

$$G = \exists y_1 \dots \exists y_p \prod_{j=1}^{m} G_j(x_{j,1}, \dots, x_{j,n_j}, y_{j,1}, \dots, y_{j,p_j}).$$

Рассмотрим $(S \cup \{=_k\})$-формулу

$$K = \prod_{j=1}^{m} G_j(x_{j,1}, \dots, x_{j,n_j}, y_{j,1}, \dots, y_{j,p_j}).$$

Т. е. уберем все кванторы существования в формуле $G$.

Заметим, что формула $G$ выполнима тогда и только тогда, когда формула $K$ выполнима.

# Сложность задач $S$-ВЫП

$(S \cup \{=_k\})$-формула $K$ имеет следующий вид:

$$K = \left(\prod_{i=1}^{l} g_i(u_{i,1}, \dots, u_{i,q_i})\right) \cdot (v_1 = w_1) \cdot \ldots \cdot (v_r = w_r),$$

где $g_i \in S$, $u_{i,1}, \dots, u_{i,q_i}, v_t, w_t \in \{x_1, \dots, x_n, y_1, \dots, y_p\}$, $i = 1, \dots, l$, $t = 1, \dots, r$.

Теперь для всех $t = 1, \dots, r$ последовательно выполним преобразования: уберем множитель $v_t = w_t$ и заменим в оставшейся формуле везде переменную $w_t$ на переменную $v_t$.

Полученную в итоге $S$-формулу обозначим $K_2$.

# Сложность задач $S$-*ВЫП*

Итак, по $T$-формуле $K_1$ построили $S$-формулу $K_2$.

Это построение можно выполнить полиномиальным алгоритмом.

Более того, $T$-формула $K_1$ — выполнима тогда и только тогда, когда $S$-формула $K_2$ выполнима.

Значит, задача $T$-*ВЫП* $P$-сводится к задаче $S$-*ВЫП*.

$\square$

# Сложность $S$-$ВЫП$ с бесконечным множеством $S$

Пусть $S \subseteq R_k$ и $S$ — бесконечное множество.

Задачу $S$-$ВЫП$ назовем **полиномиальной**, если для любого $T$, $T \subseteq S$ и $T$ — конечное множество, верно $T$-$ВЫП \in P$.

Задачу $S$-$ВЫП$ назовем $NP$-**полной**, если существует $T$, $T \subseteq S$ и $T$ — конечное множество, что $T$-$ВЫП$ — $NP$-полна.

# Сложность задач $S$-*ВЫП*

Пусть $S \subseteq R_k$ и $S$ — конечное множество.

Из теоремы 2 следует, что оценить сложность задачи $S$-*ВЫП* можно через сложность задачи $\langle S \rangle$-*ВЫП*.

Т. е. можно рассматривать сразу замкнутый класс предикатов.

А замкнутые классы предикатов можно определять при помощи k-значных функций.

Конец лекции