Лекция 12. Функции на конечном множестве. Формулы и замкнутые классы функций. Сохранение функцией предиката. Двузначный случай. Сложность некоторых задач *S-ВЫП*. Теорема разделимости.

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

факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте http://mk.cs.msu.ru

Функция

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

Отображение $f : E_k^n \to E_k$ называется n-местной k-**значной функцией** (функцией на множестве E_k), $n \geqslant 1$.

Множество всех n-местных k-значных функций обозначим $P_k^{(n)}$.

Пусть $P_k = \bigcup\limits_{n \geqslant 1} P_k^{(n)}$ — множество всех k-значных функций.

Множество значений функции

Если $f \in P_k^{(n)}$, то положим

$$E(f) = \{a \in E_k \mid \exists \alpha \in E_k^n : f(\alpha) = a\}.$$

Т. е. $E(f)$ — множество значений функции f.

Формула для функций

Пусть $A \subseteq P_k$, причем в A каждая функция имеет свое, отличное от других функций обозначение. Для функций по индукции определим понятие **формулы** над множеством A.

Базис индукции.

Если f — обозначение n-местной функции из A и $x_{i_1}, \ldots, x_{i_n}$ — (не обязательно различные) переменные, то выражение $f(x_{i_1}, \ldots, x_{i_n})$ — формула.

Индуктивный переход.

Если f — обозначение m-местной функции из A и $F_1, \ldots, F_m$ — формулы или (не обязательно различные) переменные, то выражение $f(F_1, \ldots, F_m)$ — формула.

Функция, определяемая формулой

Каждая формула F над множеством A, где $A \subseteq P_k$, задает некоторую функцию $f_F \in P_k$.

Базис индукции.

Если $F = f(x_{i_1}, \ldots, x_{i_n})$, то формула F определяет функцию $f(x_{i_1}, \ldots, x_{i_n}) \in P_k$.

Индуктивный переход.

Если $F = f(F_1, \ldots, F_m)$, где формула F_i определяет функцию $f_i(x_{i,1}, \ldots, x_{i,n_i}) \in P_k$ (если $F_i = x_{i,1}$, то $f_i(x_{i,1}) = x_{i,1}$), причем

$$\bigcup_{i=1}^{m} \{x_{i,1}, \ldots, x_{i,n_i}\} = \{x_1, \ldots, x_n\},$$

то формула F определяет функцию

$$f(x_1, \ldots, x_n) = f(f_1(x_{1,1}, \ldots, x_{1,n_1}), \ldots, f_m(x_{m,1}, \ldots, x_{m,n_m})) \in P_k.$$

Соглашение для формул и функций

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

В частности, если $F(x_1, \ldots, x_n)$ — формула, определяющая функцию $f_F(x_1, \ldots, x_n) \in P_k$, то вместо $f_F(\alpha)$, где $\alpha \in E_k^n$, будем писать $F(\alpha)$.

Замыкание множества функций

Пусть $A \subseteq P_k$.

Замыканием $[A] \subseteq P_k$ множества A называется множество всех функций из P_k, которые можно выразить формулами над множеством $A \cup \{e(x_1, x_2)\}$, где $e(x_1, x_2) = x_1$ — функция, тождественно равная x_1.

Замыкание множества функций

Другими словами, **замыканием** множества $A \subseteq P_k$ является множество $[A] \subseteq P_k$, состоящее из функций, которые можно получить из $A \cup \{e(x_1, x_2)\}$ при помощи

1) переименования переменных с возможным отождествлением (в том числе, удаления несущественных переменных),

2) добавления несущественных переменных,

3) композиции.

Замкнутый класс функций

Множество $A \subseteq P_k$ называется **замкнутым классом функций**, если

$$[A] = A.$$

Отметим, что любой замкнутый класс функций содержит все *селекторы*, т. е. тождественные функции любых переменных

$$e_i^n(x_1, \ldots, x_n) = x_i,$$

где $1 \leqslant i \leqslant n$, $n \geqslant 1$.

Применение функции к наборам

Пусть $f \in P_k^{(m)}$ и $\alpha_1, \ldots, \alpha_m \in E_2^n$. Считаем, что

$$f(\alpha_1, \ldots, \alpha_m) = \beta \in E_2^n,$$

где

$$\beta_i = f(\alpha_{1,i}, \ldots, \alpha_{m,i})$$

для всех $i = 1, \ldots, n$.

Применение функции к наборам

Пример. Пусть $f(x_1, x_2) = x_1 \vee x_2 \in P_2$. Применим функцию f к наборам $\alpha_1 = (0, 1, 1, 0) \in E_2^4$ и $\alpha_2 = (0, 0, 1, 1) \in E_2^4$.

Получаем:

α_j	$\alpha_{j,1}$	$\alpha_{j,2}$	$\alpha_{j,3}$	$\alpha_{j,4}$
α_1	0	1	1	0
α_2	0	0	1	1
$f(\alpha_1, \alpha_2)$	$f(0,0) = 0$	$f(1,0) = 1$	$f(1,1) = 1$	$f(0,1) = 1$

Поэтому $f(\alpha_1, \alpha_2) = (0, 1, 1, 1) \in E_2^4$.

Сохранение функцией предиката

Функция $f \in P_k^{(m)}$ **сохраняет** предикат $g \in R_k^{(n)}$, если для любых наборов $\alpha_1, \ldots, \alpha_m \in E_2^n$ из

$$\alpha_1, \ldots, \alpha_m \in N_1(g)$$

следует

$$f(\alpha_1, \ldots, \alpha_m) \in N_1(g).$$

Сохранение функцией предиката

Если функция $f \in P_k$ сохраняет предикат $g \in R_k$, то

функция f называется полиморфизмом предиката g,

а предикат g называется инвариантным относительно функции f.

Множество полиморфизмов предиката

Если $g \in R_k$, то множество всех полиморфизмов предиката g обозначается $\mathrm{Pol}(g)$.

Если $S \subseteq R_k$, то

$$\mathrm{Pol}(S) = \bigcap_{g \in S} \mathrm{Pol}(g).$$

Если

$$S \subseteq T \subseteq R_k,$$

то

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

Для любого $S \subseteq R_k$ множество $\mathrm{Pol}(S)$ является замкнутым классом функций.

Множество инвариантных предикатов функции

Если $f \in P_k$, то множество всех предикатов, инвариантных относительно функции f, обозначается $\mathrm{Inv}(f)$.

Если $A \subseteq P_k$, то

$$\mathrm{Inv}(A) = \bigcap_{f \in A} \mathrm{Inv}(f).$$

Если

$$A \subseteq B \subseteq P_k,$$

то

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

Для любого $A \subseteq P_k$ множество $\mathrm{Inv}(A)$ является замкнутым классом предикатов.

Соответствие Галуа

Для любого множества предикатов $S \subseteq R_k$ верно

$$\langle S \rangle = \mathrm{Inv}(\mathrm{Pol}(S)).$$

Для любого множества функций $A \subseteq P_k$ верно

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

Решетки по включению замкнутых классов функций из P_k и замкнутых классов предикатов из R_k антиизоморфны.

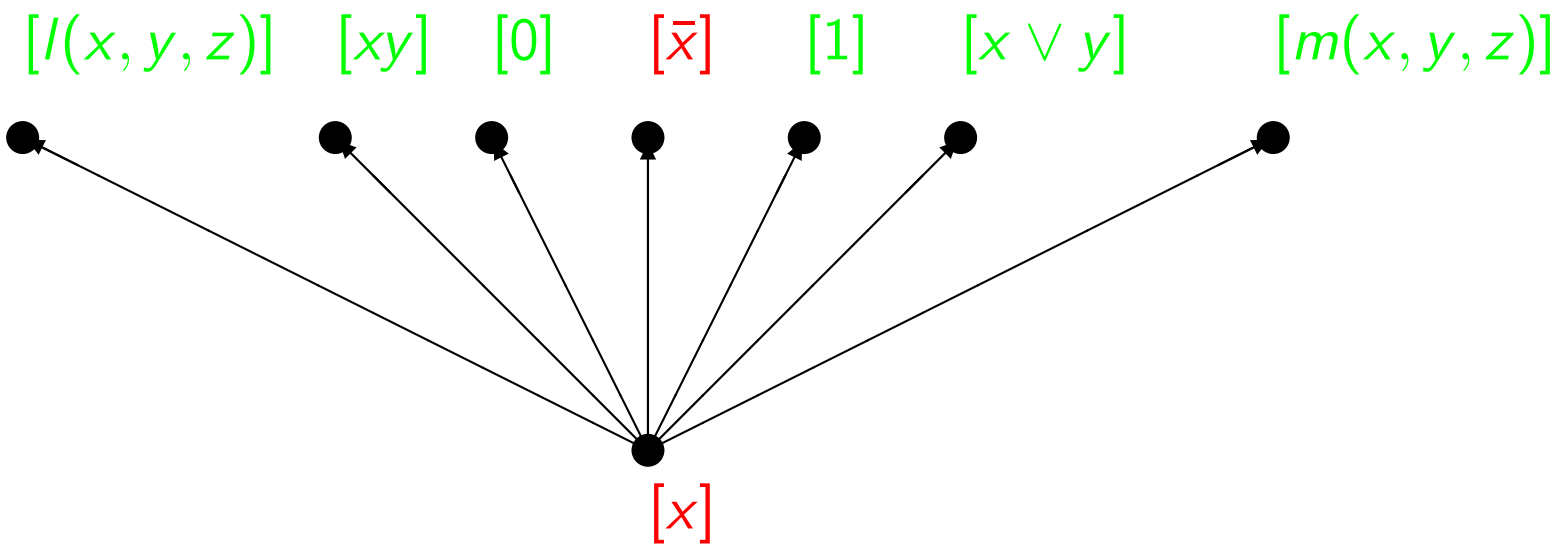
Двузначный случай

Пусть $k = 2$. Тогда

$f \in P_2$	$\mathrm{Inv}(f) \subseteq R_2$
0	$T_0' \cup \{0\}$
1	$T_1 \cup \{0\}$
$x \cdot y$	WN
$x \vee y$	WP
$m(x, y, z)$	B
$x \oplus y \oplus z$	MA

Решетка Поста замкнутых классов в P_2

Рассмотрим минимальные замкнутые классы (клоны) решетки по включению в P_2:



Для упрощения записи считаем, что $[\{f\}] = [f]$, где $f \in P_2$.

Теорема разделимости Шефера

Пусть $S \subseteq R_2$ и S — конечно. Из теоремы Шефера получаем, что S-*ВЫП* $\in P$, если $f \in \mathrm{Pol}(S)$, где

$$f \in \{0, 1, x \cdot y, x \vee y, m(x, y, z), x \oplus y \oplus z\};$$

в остальных случаях S-*ВЫП* — NP-полна, т. е. когда $\mathrm{Pol}(S)$ содержит только функции одной переменной, принимающие два значения.

Теорема разделимости Шефера

Перепишем теорему Шефера в следующем виде.

Теорема Шефера. *Пусть $S \subseteq R_2$ и S — конечно. Если множество $\mathrm{Pol}(S)$ содержит только функции одной переменной, принимающие два значения, то задача S-ВЫП — NP-полна; в остальных случая задача S-ВЫП является полиномиальной.*

Полиномиальная эквивалентность задач

Задачи распознавания $\mathcal{Z}_1$ и $\mathcal{Z}_2$ называются **полиномиально эквивалентными**, если они полиномиально сводятся друг к другу.

Пусть задачи $\mathcal{Z}_1$ и $\mathcal{Z}_2$ принадлежат классу NP и являются полиномиально эквивалентными.

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.

Одноместный полиморфизм

Теорема 1. *Пусть* $k \geqslant 2$, $S \subseteq R_k$, S — *конечно;* $f(x) \in \mathrm{Pol}(S)$, $E(f) = E_{k'} \subseteq E_k$, *где* $k' \leqslant k$, *и*

$$f(S) = \{g(f(x_1), \ldots, f(x_n)) \in R_l \mid g(x_1, \ldots, x_n) \in S\} \subseteq R_{k'}.$$

Тогда задачи S-ВЫП *и* $f(S)$-ВЫП *являются полиномиально эквивалентными*.

Одноместный полиморфизм

Доказательство. Если S-формула

$$K_1(x_1, \ldots, x_n) = \prod_{j=1}^{m} g_j(x_{j_1}, \ldots, x_{j_{n_j}}),$$

где $g_j \in S$, $1 \leqslant j_1, \ldots, j_{n_j} \leqslant n$, $j = 1, \ldots, m$, является примером задачи S-*ВЫП*, то $f(S)$-формула

$$K_2(x_1, \ldots, x_n) = K_1(f(x_1), \ldots, f(x_n)) = \prod_{j=1}^{m} g_j(f(x_{j_1}), \ldots, f(x_{j_{n_j}}))$$

является примером задачи $f(S)$-*ВЫП*.

При этом если на наборе $\alpha \in E_k^n$ формула K_1 равна единице, то на наборе $\beta = (f(\alpha_1), \ldots, f(\alpha_n)) \in E_{k'}^n$ формула K_2 равна единице.

Одноместный полиморфизм

Отметим, что построить $f(S)$-формулу K_2 по S-формуле K_1 можно полиномиальным алгоритмом.

Одноместный полиморфизм

И наоборот, если $f(S)$-формула

$$K_2(x_1, \ldots, x_n) = \prod_{j=1}^{m} g_j(f(x_{j_1}), \ldots, f(x_{j_{n_j}})),$$

где $g_j \in S$, $1 \leqslant j_1, \ldots, j_{n_j} \leqslant n$, $j = 1, \ldots, m$, является примером задачи $f(S)$-*ВЫП*, то S-формула

$$K_1(x_1, \ldots, x_n) = \prod_{j=1}^{m} g_j(x_{j_1}, \ldots, x_{j_{n_j}})$$

является примером задачи S-*ВЫП*.

При этом если на наборе $\beta \in E_{k'}^n$ формула K_2 равна единице, то найдутся такие $a_i \in E_k$, где $f(a_i) = \beta_i$, $i = 1, \ldots, n$, что на наборе $\alpha = (a_1, \ldots, a_n) \in E_k^n$ формула K_1 равна единице.

Одноместный полиморфизм

Отметим, что построить S-формулу K_1 по $f(S)$-формуле K_2 можно полиномиальным алгоритмом.

Одноместный полиморфизм

Следовательно, задачи S-*ВЫП* и $f(S)$-*ВЫП* являются полиномиально эквивалентными.

□

Полиморфизм, принимающий не все значения

Пусть $k \geqslant 2$, $S \subseteq R_k$ и S — конечно.

Из теоремы 1 следует, что если найдется полиморфизм $f(x) \in \mathrm{Pol}(S)$, принимающий не все значения, т. е. $E(f) = E_{k'} \subseteq E_k$, где $k' < k$, то при исследовании сложности вместо задачи S-ВЫП можно рассматривать задачу $f(S)$-ВЫП, в которой предикаты определены на меньшем множестве $E_{k'}$.

Полиморфизм, принимающий не все значения

Пример. Пусть $k = 3$, $S = \{g(x_1, x_2, x_3)\} \subseteq R_3$, где

$$N_1(g) = \{(0,0,1),(1,1,0),(1,1,2),(2,2,1)\}.$$

Проверим, что функция $f(x) \in P_3$,

x	$f(x)$
0	2
1	1
2	2

является полиморфизмом множества S. Итак:

$$\begin{aligned}
(f(0), f(0), f(1)) &= (2,2,1) \in N_1(g),\\
(f(1), f(1), f(0)) &= (1,1,2) \in N_1(g),\\
(f(1), f(1), f(2)) &= (1,1,2) \in N_1(g),\\
(f(2), f(2), f(1)) &= (2,2,1) \in N_1(g).
\end{aligned}$$

Поэтому $f(x) \in \mathrm{Pol}(S)$.

Полиморфизм, принимающий не все значения

Значит, при исследовании сложности задачи S-*ВЫП* можно рассмотреть задачу $f(S)$-*ВЫП*.

Получаем: $k' = 2$, $E_{k'} = \{1, 2\}$, $f(S) = \{g'(x_1, x_2, x_3)\} \subseteq R_2$, где $g'(x_1, x_2, x_3) = g(f(x_1), f(x_2), f(x_3))$,

$$N_1(g') = \{(1, 1, 2), (2, 2, 1)\} \subseteq E_2^3.$$

Заметим, что $g' \in MA$, и по теореме Шефера $f(S)$-*ВЫП* $\in P$.

По теореме 1 получаем, что S-*ВЫП* $\in P$.

Приведенная задача обобщенной выполнимости

Пусть $k \geqslant 2$, $S \subseteq R_k$ и S — конечно.

Задачу *S-ВЫП* назовем **приведенной**, если все одноместные полиморфизмы множества S принимают все k значений, т. е. для любого $f(x) \in \mathrm{Pol}(S)$ верно $E(f) = E_k$ (или $f(x)$ является **перестановкой** на множестве E_k).

Все полиморфизмы — перестановки

Теорема 2. *Пусть* $k \geqslant 2$, $S \subseteq R_k$ *и* S *— конечно. Если* $\mathrm{Pol}(S)$ *содержит только перестановки на множестве* E_k, *то задача* S*-ВЫП является NP-полной*.

Все полиморфизмы — перестановки

Доказательство. Рассмотрим два случая.

1. Пусть $k = 2$. Тогда

$$\mathrm{Pol}(S) \subseteq \{x, \bar{x}\}.$$

Для предиката $g(x_1, x_2, x_3) = (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)(x_1 \vee x_2 \vee x_3)$ верно:

$$g(x_1, x_2, x_3) \in \mathrm{Inv}(\{x, \bar{x}\}).$$

Значит, $g(x_1, x_2, x_3) \in \langle S \rangle$. Из того, что $\{g\}$-*ВЫП* — *NP*-полна, получаем, что S-*ВЫП* — *NP*-полна.

Все полиморфизмы — перестановки

2. Пусть $k \geqslant 3$. Если $\mathrm{Pol}(S)$ содержит только перестановки на E_k, то

$$\neq_k \in \mathrm{Inv}(\mathrm{Pol}(S)).$$

Значит, $\neq_k \in \langle S \rangle$. Из того, что $\{\neq_k\}$-*ВЫП* — *NP*-полна при $k \geqslant 3$, получаем, что *S*-*ВЫП* — *NP*-полна.

□

Одноместные одноэлементные предикаты

Рассмотрим **одноместные одноэлементные предикаты** $g_a(x) \in R_k$, где $g_a(a) = 1$, $g_a(x) = 0$ при $x \neq a$.

Положим:

$$S_0 = \{g_a(x) \in R_k \mid a \in E_k\}.$$

Одноместные одноэлементные предикаты

Теорема 3. *Пусть* $k \geqslant 2$, $S_0 = \{g_a(x) \in R_k \mid a \in E_k\}$, $S \subseteq R_k$, S *— конечно и* S*-ВЫП —* приведенная *задача. Тогда задачи* S*-ВЫП и* $(S \cup S_0)$*-ВЫП являются полиномиально эквивалентными*.

Одноместные одноэлементные предикаты

Доказательство. Рассмотрим предикат $g_S \in R_k^{(k)}$,

$$N_1(g_S) = \{(f(0), f(1), \ldots, f(k-1)) \in E_k^k \mid f \in \mathrm{Pol}(S) \cap P_k^{(1)}\}.$$

Покажем, что $g_S \in \langle S \rangle$, т. е. что $g_S \in \mathrm{Inv}(\mathrm{Pol}(S))$.

Одноместные одноэлементные предикаты

Пусть $h(z_1, \ldots, z_m) \in \mathrm{Pol}(S)$. Если $\alpha_1, \ldots, \alpha_m \in N_1(g_S)$, то

$$\alpha_j = (f_j(0), f_j(1), \ldots, f_j(k-1)) \in E_k^k$$

для некоторой функции $f_j(x) \in \mathrm{Pol}(S)$, $j = 1, \ldots, m$. Пусть

$$\beta = h(\alpha_1, \ldots, \alpha_m) \in E_k^k.$$

Тогда при $i = 1, \ldots, k$ получаем:

$$\beta_i = h(f_1(i-1), \ldots, f_m(i-1)) = f(i-1),$$

где $f(z) = h(f_1(z), \ldots, f_m(z))$. Но $f \in \mathrm{Pol}(S)$, а значит,

$$\beta = (f(0), f(1), \ldots, f(k-1)) \in N_1(g_S).$$

Одноместные одноэлементные предикаты

Итак, $g_S \in \langle S \rangle$.

Далее, если S-формула $K_1(x_1, \ldots, x_n)$ является примером задачи S-*ВЫП*, то она же является примером задачи $(S \cup S_0)$-*ВЫП*.

Одноместные одноэлементные предикаты

Пусть теперь $(S \cup S_0)$-формула $K_2(x_1, \ldots, x_n)$ — пример задачи $(S \cup S_0)$-*ВЫП*, в которой не встречаются одновременно $g_a(x)$ и $g_b(x)$ при $a \neq b$.

В формуле K_2 для каждого $a \in E_k$ выполним следующие преобразования.

Каждый множитель вида $g_a(x_i)$ удалим и в оставшемся выражении заменим везде переменную x_i на новую переменную y_a.

Затем в формулу добавим множитель $g_S(y_0, y_1, \ldots, y_{k-1})$. В итоге получим S-формулу $K_1(x_1, \ldots, x_n, y_0, y_1, \ldots, y_{k-1})$, являющуюся примером задачи S-*ВЫП*.

Отметим, что построить S-формулу K_1 по $(S \cup S_0)$-формуле K_2 можно полиномиальным алгоритмом.

Одноместные одноэлементные предикаты

Если на наборе $\alpha \in E_k^n$ формула K_2 равна единице, то на наборе $\beta = (\alpha, 0, 1, \ldots, k-1) \in E_k^{n+k}$ формула K_1 равна единице, т. к. $f(x) = x \in \mathrm{Pol}(S)$.

Одноместные одноэлементные предикаты

Пусть теперь наборе $\beta = (\alpha, \gamma) \in E_k^{n+k}$, где $\alpha \in E_k^n$, $\gamma \in E_k^k$, формула K_1 равна единице. Тогда

$$\gamma = (f(0), f(1), \ldots, f(k-1)) \in E_k^k$$

для некоторой функции $f(x) \in \mathrm{Pol}(S)$. Но в множестве $\mathrm{Pol}(S) \cap P_k^{(1)}$ содержатся только перестановки на E_k. Поэтому найдется $f^{-1}(x) \in \mathrm{Pol}(S)$ — обратная к $f(x)$ перестановка.

На наборе

$$f^{-1}(\beta) = (f^{-1}(\alpha), 0, 1, \ldots, k-1) \in E_k^{n+k},$$

где $f^{-1}(\alpha) = (f^{-1}(\alpha_1), \ldots, f^{-1}(\alpha_n)) \in E_k^n$, формула K_1 также равна единице, т. к. $f^{-1}(x) \in \mathrm{Pol}(S)$.

Значит, на наборе $f^{-1}(\alpha) \in E_k^n$ формула K_2 равна единице.

Одноместные одноэлементные предикаты

Итак, $(S \cup S_0)$-формула K_2 — выполнима тогда и только тогда, когда S-формула K_1 — выполнима.

Следовательно, задачи S-*ВЫП* и $(S \cup S_0)$-*ВЫП* являются полиномиально эквивалентными.

□

Теорема разделимости

Приведем теорему разделимости в общем случае.

Слабая функция почти единогласия

Функция $f \in P_k^{(m)}$, $m \geqslant 2$, называется **слабой функцией почти единогласия**, если

1) $f(x, \ldots, x) = x$,

2) $f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \ldots = f(x, \ldots, x, y)$.

Теорема разделимости

Как итог ряда работ П. Джевонса, А. А. Булатова, А. Крохина, М. Мароти, Р. Маккензи, Д. Н. Жука и др. получена следующая теорема разделимости.

Теорема 4 (разделимости). *Пусть* $k \geqslant 2$, $S_0 = \{g_a(x) \in R_k \mid a \in E_k\}$, $S \subseteq R_k$, S *— конечно и* $S_0 \subseteq S$. *Если в множестве* $\mathrm{Pol}(S)$ *найдется слабая функция почти единогласия, то задача* S*-ВЫП является полиномиальной; иначе задача* S*-ВЫП является NP-полной.*

Конец лекции