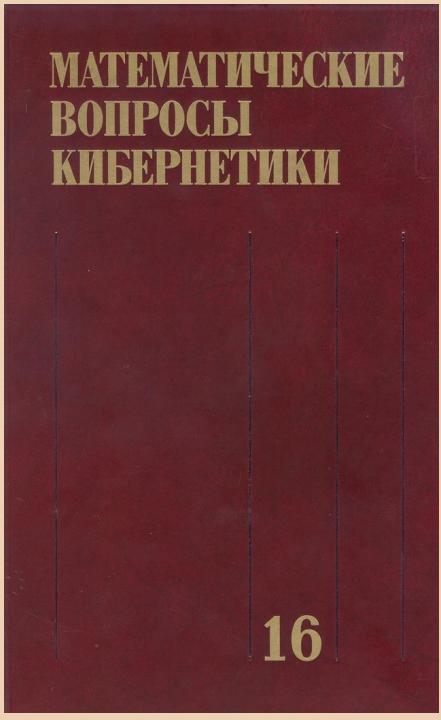
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 16



С. А. Волков

Экспоненциальное расширение класса функций, элементарных по Сколему, и ограниченные суперпозиции простых арифметических функций

Рекомендуемая форма библиографической ссылки: Волков С. А. Экспоненциальное расширение класса функций, элементарных по Сколему, и ограниченные суперпозиции простых арифметических функций // Математические вопросы кибернетики. Вып. 16. — М.: ФИЗМАТЛИТ, 2007. — С. 163–190. URL: http://library.keldysh.ru/mvk.asp?id=2007-163

ЭКСПОНЕНЦИАЛЬНОЕ РАСШИРЕНИЕ КЛАССА ФУНКЦИЙ, ЭЛЕМЕНТАРНЫХ ПО СКОЛЕМУ, И ОГРАНИЧЕННЫЕ СУПЕРПОЗИЦИИ ПРОСТЫХ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ *)

С. А. ВОЛКОВ

(МОСКВА)

§ 1. Введение

Впервые вопрос о существовании конечных базисов по суперпозиции в некоторых классах рекурсивных функций был поставлен известным польским логиком А. Гжегорчиком [1]. Положительный ответ на этот вопрос для класса K функций, элементарных по Кальмару (см. [4]), получил Д. Реддинг [9]. Позже Ч. Парсонс [8] выписал в явном виде систему из 19 элементарных функций, полную в классе K. Через некоторое время С. С. Марченков [2, 3] показал, что класс функций, элементарных по Кальмару, может быть порожден суперпозициями функций очень простого вида, а именно, что полными в классе K являются следующие системы функций:

$$\{x+1, \quad x^y, \quad \left[x/y\right], \quad \varphi(x,\, y)\},$$
$$\{x \div 1, \quad \left[x/y\right], \quad 2^{x+y}, \quad \sigma(x)\},$$
$$\{x+1, \quad \left[x/y\right], \quad x^y, \quad \tau(x)\},$$

где $\varphi(x,\, y)$ равно номеру наименьшего нулевого разряда в представлении y в позиционной системе счисления с основанием x при $x \geqslant 2$, и нулю при $x \leqslant 1$, $\sigma(x)$ равно количеству единиц в двоичном представлении числа x, $\tau(x)$ равно показателю числа 2 в разложении x на простые множители при $x > 0$, и $\tau(0) = 0$, $x \div y = \max(x - y, 0)$, $\left[x/y\right]$ равно целой части от деления x на y при $y > 0$, и нулю при $y = 0$.

С. Маззанти [7] усилил результат С. С. Марченкова, приведя несколько полных в классе K систем, состоящих из простейших функций арифметики. Одной из таких систем является система

$$\{x+y, \quad x \div y, \quad [x/y], \quad 2^x\}.$$

Отметим, что все приведенные полные системы состоят из функций медленного роста (ограниченных полиномами) и из функций экспоненциального роста. Сила полученных результатов во многом достигается за счет

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 06–01–00438).

использования функций экспоненциального роста. Поэтому возник вопрос: что будет, если в формулах ограничить использование функций экспоненциального роста.

В этой работе описаны классы функций, получаемые суперпозициями простых общеизвестных функций (арифметических и используемых в стандартных языках программирования) со следующим ограничением на формулы: формула должна иметь не более двух «этажей». Доказывается, что полученные классы совпадают с введенным в этой работе классом XS, который является экспоненциальным расширением класса S функций, элементарных по Сколему (см. [4]). Все функции класса XS ограничены функциями экспоненциального роста (функциями вида $2^{p(\bar{x})}$, где p — полином). С точки зрения сложности вычисления одного бита значения функции класс XS подобен классу S, но отличается от него по ограничениям на скорость роста функций (в классе XS функции ограничены функциями экспоненциального роста, а в S — полиномами).

§ 2. Основные определения и формулировка результата

Пусть $N = \{0, 1, 2, \ldots\}$ — множество натуральных чисел. Рассматриваются всюду определенные функции (произвольного числа аргументов) на множестве N. Под операцией суперпозиции будем подразумевать подстановку функций в функции, перестановку и отождествление переменных, введение фиктивных переменных.

Будем говорить, что функция $f(x, z_1, \ldots, z_n)$ получается из функции $g(y, z_1, \ldots, z_n)$ с помощью операции *ограниченного суммирования* по переменной y, если при любых натуральных $x, z_1, \ldots, z_n$ выполнено

$$f(x, z_1, \ldots, z_n) = \begin{cases} \sum\limits_{y<x} g(y, z_1, \ldots, z_n), & \text{если } x > 0, \\ 0, & \text{если } x = 0. \end{cases}$$

Положим

$$\mathrm{sg}(x) = \begin{cases} 1, & \text{если } x > 0, \\ 0 & \text{в противном случае,} \end{cases}$$

$$\mathrm{rm}(x, y) = \begin{cases} \text{остатку от деления } x \text{ на } y, & \text{если } y > 0, \\ 0 & \text{в противном случае,} \end{cases}$$

$$[\log_2 x] = \begin{cases} \text{целой части двоичного логарифма } x, & \text{если } x > 0, \\ 0 & \text{в противном случае,} \end{cases}$$

$x\langle y\rangle$ равно y-му двоичному разряду числа x

$$\text{(таким образом, } x = \sum_{y=0}^{\infty} x\langle y\rangle 2^y\text{)},$$

$$\mathrm{len}(x) = [\log_2 x] + 1.$$

Заметим, что $\mathrm{len}(x)$ равно длине двоичной записи x, если $x > 0$, и нулю в противном случае. Определим функцию $x \wedge y$ — поразрядную конъюнкцию двоичных представлений чисел x и y. Пусть $a_n a_{n-1} \ldots a_0$ и $b_n b_{n-1} \ldots b_0$ — двоичные представления чисел x и y (если длины двоичных представлений различны, то старшие разряды двоичного представления меньшего числа равны нулю). Тогда двоичное представление числа $x \wedge y$ есть

$$(a_n \cdot b_n)(a_{n-1} \cdot b_{n-1}) \ldots (a_0 \cdot b_0).$$

Класс S функций, элементарных по Сколему (см. [4]) — это минимальный класс функций, содержащий функции

$$0, \quad x+1, \quad x \div y$$

и замкнутый относительно суперпозиции и ограниченного суммирования.

Определим XS как класс всех функций $f(x_1, \ldots, x_n)$, для которых выполнены следующие два условия.

1. Существует полином $p(x_1, \ldots, x_n)$ с натуральными коэффициентами такой, что для любых $x_1, \ldots, x_n$ справедливо неравенство

$$f(x_1, \ldots, x_n) < 2^{p(x_1, \ldots, x_n)}.$$

2. $f(x_1, \ldots, x_n)\langle y \rangle \in \mathrm{S}$.

Очевидно, что $\mathrm{S} \subseteq \mathrm{XS}$.

Пусть Q — некоторый класс функций натурального аргумента. Будем обозначать через $[Q]$ замыкание по суперпозиции класса Q.

Определим классы $[Q]_{2^x}$ и $[Q]_{x^y}$ индуктивно.

1. Все функции класса Q принадлежат $[Q]_{2^x}$ и $[Q]_{x^y}$.

2. Если $f \in [Q]_{2^x}$ $(f \in [Q]_{x^y})$ и g получается из f перестановкой или отождествлением переменных, а также введением фиктивных переменных, то $g \in [Q]_{2^x}$ $(g \in [Q]_{x^y})$

3. Если $f(y_1, \ldots, y_m) \in Q$ и $g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n) \in [Q]_{2^x}$ $([Q]_{x^y})$, то

$$f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)) \in [Q]_{2^x} \quad ([Q]_{x^y}).$$

4. Если $f \in [Q]$, $g \in [Q]_{x^y}$, то $2^f \in [Q]_{2^x}$ и $g^f \in [Q]_{x^y}$.

Положим

$$T = \{x+1, \quad xy, \quad x \div y, \quad x \wedge y, \quad [x/y]\}.$$

Основная теорема.

$$\mathrm{XS} = [T]_{2^x} = [T]_{x^y}.$$

§ 3. Вспомогательные определения

Характеристической функцией предиката $\rho(x_1, \ldots, x_n)$ будем называть функцию $\chi_\rho(x_1, \ldots, x_n)$ такую, что при любых $x_1, \ldots, x_n$

$$\chi_\rho(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если } \rho(x_1, \ldots, x_n) \text{ истинно,} \\ 0 & \text{в противном случае.} \end{cases}$$

Определение. Предикат $\rho(x_1, \ldots, x_n)$ назовем *правильным*, если существует функция $f(y) \in [T]_{2^x}$ такая, что при любом $y \geqslant 1$

$$f(y) = \sum_{0 \leqslant x_1 < y} \ldots \sum_{0 \leqslant x_n < y} (\chi_\rho(x_1, \ldots, x_n) 2^{x_1 + x_2 y + \ldots + x_n y^{n-1}}).$$

В этом случае функция f называется *производящей функцией предиката* ρ.

Далее производящую функцию любого предиката ρ будем обозначать f_ρ.

О п р е д е л е н и е. Функция $f(x_1, \ldots, x_n)$ называется *T-полиномиальной* по множеству переменных $\{x_{i_1}, \ldots, x_{i_k}\}$, если для любых функций $g_1(\widetilde{y}), \ldots, g_n(\widetilde{y})$ из выполнения для всех i, $1 \leqslant i \leqslant n$, соотношений

$$g_i \in [T]_{2^x}\ , \text{ если } i \in \{i_1, \ldots, i_k\},$$
$$g_i \in [T]\ , \text{ если } i \notin \{i_1, \ldots, i_k\},$$

следует, что

$$f(g_1(\widetilde{y}), \ldots, g_n(\widetilde{y})) \in [T]_{2^x}\ .$$

Под *явными преобразованиями* будем подразумевать операции перестановки и отождествления переменных, введения фиктивных переменных и подстановки констант (из множества N) вместо переменных.

Будем говорить, что предикат $\varphi(x_1, \ldots, x_n, y)$ получается из предиката $\psi(x_1, \ldots, x_n)$ с помощью *операции подсчета* по переменной x_i и полиному $p(x_1, \ldots, x_n)$, если при любых $x_1, \ldots, x_n, y$ из N значение $\varphi(x_1, \ldots, x_n, y)$ истинно тогда и только тогда, когда y есть количество таких x, что $x < p(x_1, \ldots, x_n)$ и $\psi(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n)$ истинно.

Пусть $\mathrm{BA}^{\#}$ есть минимальный класс предикатов, содержащий предикаты $x + y = z$ и $xy = z$, замкнутый относительно явных преобразований, логических операций и операции подсчета.

Класс BA (см. [4]) определим как минимальный класс предикатов, содержащий предикаты $x + y = z$, $xy = z$ и замкнутый относительно явных преобразований, логических операций и ограниченных квантификаций вида $(\exists x)_{x<y}$ и $(\forall x)_{x<y}$.

Пусть S_* есть множество всех предикатов, характеристические функции которых лежат в S.

Графиком функции $f(x_1, \ldots, x_n)$ назовем предикат $y = f(x_1, \ldots, x_n)$.

Пусть $\mathrm{BA}_f^{\#}$ есть множество всех функций, ограниченных сверху полиномами, графики которых лежат в $\mathrm{BA}^{\#}$.

Будем говорить, что функция $f(x, z_1, \ldots, z_n)$ получается из функции $g(y, z_1, \ldots, z_n)$ с помощью операции *суженного ограниченного суммирования*, если при любых натуральных $x, z_1, \ldots, z_n$

$$f(x, z_1, \ldots, z_n) = \begin{cases} \sum\limits_{y<x} \mathrm{sg}(g(y, z_1, \ldots, z_n)), & \text{если } x > 0, \\ 0, & \text{если } x = 0. \end{cases}$$

Если A — некоторый алфавит, то будем обозначать A^+ множество всех конечных непустых слов в алфавите A. Если X — некоторое слово в алфавите A, то будем обозначать $|X|$ длину этого слова.

Назовем FOM-*термом* над переменными $x_1, \ldots, x_m$ выражение вида $x_1, \ldots, x_m, 1, |X|$.

О п р е д е л е н и е. *Элементарными FOM-формулами* над переменными $x_1, \ldots, x_m$ называются выражения вида $(t_1 \leqslant t_2)$, $\mathrm{BIT}(t_1, t_2)$ или $\mathrm{X}\langle t_1 \rangle$, где t_1, t_2 — FOM-термы над переменными $x_1, \ldots, x_m$.

Определим индуктивно понятие FOM-формулы над переменными $x_1, \ldots, x_m$.

1. Все элементарные FOM-формулы над $x_1, \ldots, x_m$ являются FOM-формулами над $x_1, \ldots, x_m$.

2. Если Φ_1, Φ_2 — FOM-формулы, $x_i \in \{x_1, \ldots, x_m\}$, то $(\Phi_1 \& \Phi_2)$, $(\Phi_1 \vee \Phi_2)$, $(\neg\Phi_1)$, $\exists x_i(\Phi_1)$, $(\forall x_i)(\Phi_1)$, $(Mx_i)(\Phi_1)$ являются FOM-формулами над $x_1, \ldots, x_m$.

Каждому FOM-терму t над переменными $x_1, \ldots, x_m$ следующим образом сопоставим функцию $h_t(X, x_1, \ldots, x_m)$, определенную на множестве всех наборов $(X, x_1, \ldots, x_m)$ таких, что $X \in \{0, 1\}^+$ и $x_1, \ldots, x_m \in N$.

1. Если t есть 1, то

$$h_t(X, x_1, \ldots, x_m) = 1.$$

2. Если t есть $|X|$, то

$$h_t(X, x_1, \ldots, x_m) = |X|.$$

3. Если t есть x_i, то

$$h_t(X, x_1, \ldots, x_m) = x_i.$$

Каждой элементарной FOM-формуле Φ над переменными $x_1, \ldots, x_m$ следующим образом сопоставим предикат $\rho_\Phi(X, x_1, \ldots, x_m)$, область определения которого совпадает с областью определения функций FOM-термов над $x_1, \ldots, x_m$.

1. Если Φ имеет вид $(t_1 \leqslant t_2)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv (h_{t_1}(X, x_1, \ldots, x_m) \leqslant h_{t_2}(X, x_1, \ldots, x_m)).$$

2. Если Φ имеет вид $\mathrm{BIT}(t_1, t_2)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv (h_{t_1}(X, x_1, \ldots, x_m)\langle h_{t_2}(X, x_1, \ldots, x_m)\rangle = 1).$$

3. Если Φ имеет вид $\mathrm{X}\langle t_1\rangle$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv (h_{t_1}(X, x_1, \ldots, x_m) = 1).$$

Каждой FOM-формуле Φ над переменными $x_1, \ldots, x_m$ следующим образом сопоставим предикат $\rho_\Phi(X, x_1, \ldots, x_m)$, область определения которого совпадает с областью определения функций FOM-термов над $x_1, \ldots, x_m$.

1. Если формула является элементарной FOM-формулой, то соответствующий ей предикат совпадает с предикатом, определенным для данной элементарной формулы.

2. Если Φ имеет вид $(\Phi_1 \& \Phi_2)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv \rho_{\Phi_1}(X, x_1, \ldots, x_m) \& \rho_{\Phi_2}(X, x_1, \ldots, x_m).$$

3. Если Φ имеет вид $(\Phi_1 \vee \Phi_2)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv \rho_{\Phi_1}(X, x_1, \ldots, x_m) \vee \rho_{\Phi_2}(X, x_1, \ldots, x_m).$$

4. Если Φ имеет вид $(\neg\Phi_1)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv \neg\rho_{\Phi_1}(X, x_1, \ldots, x_m).$$

5. Если Φ имеет вид $(\exists x_i)(\Phi_1)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv (\exists x)_{(1 \leqslant x \leqslant |X|)}\rho_{\Phi_1}(X, x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m).$$

6. Если Φ имеет вид $(\forall x_i)(\Phi_1)$, то

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv (\forall x)_{(1 \leqslant x < |X|)}\rho_{\Phi_1}(X, x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m).$$

7. Если Φ имеет вид $(Mx_i)(\Phi_1)$, то $\rho_\Phi(X, x_1, \ldots, x_m)$ истинно тогда и только тогда, когда количество x таких, что $1 \leqslant x \leqslant |X|$ и $\rho_{\Phi_1}(X, x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m)$ истинно, больше, чем $|X|/2$.

Класс FOM (см. [6]) определим как множество всех всюду определенных на множестве $\{0,1\}^+$ предикатов $\varphi(X)$, для которых существует FOM-формула, которой соответствует предикат $\rho(X, x_1, \ldots, x_m)$ такой, что при любых $X, x_1, \ldots, x_m$ из его области определения

$$\varphi(X) \equiv \rho(X, x_1, \ldots, x_m).$$

Если $x_1, \ldots, x_m$ — целые неотрицательные числа, то будем обозначать $\mathrm{CODE}(x_1, \ldots, x_m)$ слово

$$01s_101s_201\ldots01s_m01,$$

где

$$s_i = \begin{cases} \text{пустому слову,} & \text{если } x_i = 0, \\ \text{слову, получающемуся из двоичной записи } x_i \text{ заменой каждой} \\ \quad \text{единицы на 11, а каждого нуля на 00,} & \text{если } x_i \neq 0. \end{cases}$$

Класс FOM^N определим как множество всех всюду определенных на множестве натуральных чисел предикатов $\varphi(x_1, \ldots, x_n)$, для которых существует предикат $\psi(X)$ из FOM такой, что при любых $x_1, \ldots, x_n$ выполнено

$$\varphi(x_1, \ldots, x_n) \equiv \psi(\mathrm{CODE}(x_1, \ldots, x_n)).$$

Класс FFOM определим как множество всех всюду определенных на множестве натуральных чисел функций $f(x_1, \ldots, x_n)$ таких, что выполняются следующие два условия.

1. Существует полином $p(y_1, \ldots, y_n)$ такой, что при любых $x_1, \ldots, x_n$

$$f(x_1, \ldots, x_n) \leqslant 2^{p([\log_2(x_1)], \ldots, [\log_2(x_n)])}.$$

2. Предикат ρ, определяемый соотношением

$$\rho(x_1, \ldots, x_n, y) \equiv (f(x_1, \ldots, x_n)\langle y\rangle = 1),$$

лежит в FOM^N.

Положим

$$(\mu x_i)_{x_i < y}(f(x_1, \ldots, x_n) = z) = \begin{cases} \text{наименьшему из таких значений } x_i, \\ \quad \text{что } x_i < y \text{ и } f(x_1, \ldots, x_n) = z, \\ \quad \text{если такое } x_i \text{ существует,} \\ \\ 0 \quad \text{в противном случае.} \end{cases}$$

Операцию μ будем называть операцией *ограниченной минимизации*.

§ 4. Включение $[T]_{x^y} \subseteq \mathbf{XS}$

Утверждение 1. *Функция $x\langle y\rangle$ лежит в* S. *Кроме того, предикат $(x\langle y\rangle = 1)$ лежит в* S_*.

Доказательство. Действительно, ясно, что

$$(x\langle y\rangle = 1) \equiv (\exists z)_{z \leqslant x}(\exists t)_{t < z}(\exists u)_{u \leqslant x}((x = 2uz + z + t)\&(z = 2^y)).$$

Из [4] известно, что $(x = 2uz + z + t)$ и $(z = 2^y)$ лежат в BA. Из этого следует, что $(x\langle y\rangle = 1) \in \mathrm{BA} \subseteq \mathrm{S}_*$. Из этого и из того, что $x\langle y\rangle$ принимает значения 0 и 1, следует доказываемое утверждение.

Утверждение 2 [4]. *Класс* S *замкнут относительно ограниченной минимизации.*

Утверждение 3. *Если* $f(\tilde{x}) \in \mathrm{XS}$, *то* $\mathrm{len}(f(\tilde{x})) \in \mathrm{S}$.

Доказательство. Пусть $p(\tilde{x})$ — полином, ограничивающий сверху (строго) длину двоичной записи $f(\tilde{x})$ (существование такого полинома следует из определения XS). Тогда ясно, что

$$\mathrm{len}(f(\tilde{x})) = (\mu z)_{z<p(\tilde{x})}(f(\tilde{x}) < 2^z).$$

Из [4] известно, что

$$(x < 2^y) \in \mathrm{S}_*.$$

Из этого и из утверждения 2 следует доказываемое утверждение.

Утверждение 4. *Пусть* $g_1(\tilde{z}), \ldots, g_k(\tilde{z}) \in \mathrm{XS}$, t — FOM-*терм над переменными* $x_1, \ldots, x_m$, *ему соответствует функция* $h_t(X, x_1, \ldots, x_m)$. *Тогда*

$$h_t(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) \in \mathrm{S}.$$

Доказательство. Всюду определенность $h_t(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m)$ следует из того, что в область значений CODE не входит пустое слово. Докажем принадлежность классу S. Возможны следующие случаи.

1. t есть 1. Тогда ясно, что

$$h_t(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) = 1.$$

Принадлежность S очевидна.

2. t есть $|X|$. Тогда

$$h_t(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) = 2 \cdot (\mathrm{len}(g_1(\tilde{z})) + \ldots + \mathrm{len}(g_k(\tilde{z})) + k + 1)$$

(см. определение CODE и h_t). Принадлежность классу S следует из утверждения 3.

3. t имеет вид x_i. Тогда

$$h_t(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) = x_i.$$

Принадлежность классу S очевидна.

Утверждение доказано.

Утверждение 5. *Пусть* $g_1(\tilde{z}), \ldots, g_k(\tilde{z}) \in \mathrm{XS}$, Φ — *элементарная* FOM-*формула над переменными* $x_1, \ldots, x_m$, *ей соответствует предикат* $\rho_\Phi(X, x_1, \ldots, x_m)$. *Тогда*

$$\rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) \in \mathrm{S}_*.$$

Доказательство. Всюду определенность предиката $\rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m)$ следует из того, что в область значений CODE не входит пустое слово. Докажем принадлежность классу S_*. Возможны случаи.

1. Φ имеет вид $(t_1 = t_2)$. Тогда

$$\rho_\Phi \equiv (h_{t_1} = h_{t_2}).$$

Принадлежность классу S_* следует из утверждения 4 и из того, что $(x = y) \in BA \subseteq S_*$ (см. [4]).

2. Ф имеет вид $(t_1 \leqslant t_2)$. Аналогично.

3. Ф имеет вид $BIT(t_1, t_2)$. Из утверждения 1 следует, что $(x\langle y\rangle = 1)$ принадлежит S_*. Из определения ρ_Φ следует представление

$$\rho_\Phi(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m) \equiv$$
$$\equiv (h_{t_1}(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m)\langle h_{t_2}(CODE(g_1(\widetilde{z}), \ldots$$
$$\ldots, g_k(\widetilde{z})), x_1, \ldots, x_m)\rangle = 1).$$

Отсюда, из утверждения 4 и из того, что $(x\langle y\rangle = 1)$ принадлежит S_*, следует, что

$$\rho_\Phi(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m) \in S_*.$$

4. Ф имеет вид $X\langle t_1\rangle$. Для краткости выражения $h_{t_1}(CODE(g_1(\widetilde{z}), \ldots$ $\ldots, g_k(\widetilde{z})), x_1, \ldots, x_m)$ и $\rho_\Phi(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m)$ будем обозначать просто h_{t_1} и ρ_Φ, а выражения $2 \cdot \mathrm{len}(g_i(\widetilde{z}))$ будем обозначать l_i $(1 \leqslant i \leqslant k)$. Тогда из определений CODE и ρ_Φ следует, что

$$\rho_\Phi \equiv \begin{cases} (g_i(\widetilde{z}) \left\langle \left[\dfrac{h_{t_1} \div (2i + l_1 + \ldots + l_{i-1} + 1)}{2} \right] \right\rangle = 1), & \text{если} \\ \qquad 2i + l_1 + \ldots + l_{i-1} + 1 \leqslant h_{t_1} < 2i + l_1 + \ldots + l_{i-1} + l_i + 1, \\ \qquad 1 \leqslant i \leqslant k, \\ \text{истина}, & \text{если } h_{t_1} = 2i + l_1 + \ldots + l_i + 2,\ 0 \leqslant i \leqslant k, \\ \text{ложь} & \text{в остальных случаях.} \end{cases}$$

По предположению индукции, $h_{t_1} \in S$. Отсюда, из включений $g_i \in XS$, из определения XS и из простейших свойств класса S (см. [4]) следует, что при любом i $(1 \leqslant i \leqslant k)$

$$g_i(\widetilde{z}) \left\langle \left[\frac{h_{t_1} \div (2i + l_1 + \ldots + l_{i-1} + 1)}{2} \right] \right\rangle \in S.$$

Кроме того, по утверждению 3, $l_i \in S$ $(1 \leqslant i \leqslant k)$. Из этого и из замкнутости S относительно разбора случаев по предикатам из S_* (см. [4]) следует, что $\rho_\Phi \in S$.

Утверждение доказано.

У т в е р ж д е н и е 6. *Пусть* $g_1(\widetilde{z}), \ldots, g_k(\widetilde{z}) \in XS$, Φ — FOM-*формула над переменными* $x_1, \ldots, x_m$, *ей соответствует предикат* $\rho_\Phi(X, x_1, \ldots, x_m)$. *Тогда*

$$\rho_\Phi(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m) \in S_*.$$

Д о к а з а т е л ь с т в о. Всюду определенность предиката $\rho_\Phi(CODE(g_1(\widetilde{z}), \ldots, g_k(\widetilde{z})), x_1, \ldots, x_m)$ следует из того, что в область значений CODE не входит пустое слово. Пусть l — сокращенное обозначение для

$$2 \cdot (\mathrm{len}(g_1(\widetilde{z})) + \ldots + \mathrm{len}(g_k(\widetilde{z})) + k + 1).$$

Из утверждения 3 следует, что $l \in S$. Принадлежность классу S_* докажем индукцией по построению формулы.

1. Φ — элементарная FOM-формула. Тогда данное утверждение следует из утверждения 5.

2. Φ имеет вид $(\Phi_1 \& \Phi_2)$, $(\Phi_1 \vee \Phi_2)$ или $(\neg\Phi_1)$. Утверждение следует из замкнутости S_* относительно логических операций (см. [4]).

3. Φ имеет вид $(\exists x_i)\Phi_1$. Тогда

$$\rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) \equiv$$

$$\equiv (\exists x)_{(1 \leqslant x \leqslant l)} \rho_{\Phi_1}(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m).$$

Принадлежность классу S_* следует из того, что $l \in S$, и из замкнутости S_* относительно ограниченной квантификации (см. [4]).

4. Φ имеет вид $(\forall x_i)(\Phi_1)$. Тогда данное утверждение есть следствие из пп. 2 и 3.

5. Φ имеет вид $(Mx_i)(\Phi_1)$. Пусть

$$r(\tilde{z}, x_1, \ldots, x_m) = \sum_{1 \leqslant x \leqslant l} \chi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m),$$

где χ — характеристическая функция предиката ρ_{Φ_1}. Ясно, что $r(\tilde{z}, x_1, \ldots, x_m)$ есть количество x таких, что $1 \leqslant x \leqslant l$ и

$$\rho_{\Phi_1}(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_m)$$

истинно. Из определения S, предположения индукции и того, что $l \in S$, следует, что $r \in S$. Из определения ρ_Φ следует, что

$$\rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) \equiv$$
$$\equiv (r(\tilde{z}, x_1, \ldots, x_m) > l \div r(\tilde{z}, x_1, \ldots, x_m)).$$

Поэтому из $(x \div y) \in S$ и $(x > y) \in S_*$ следует, что $\rho_\Phi \in S_*$.

Утверждение доказано.

У т в е р ж д е н и е 7. *Пусть* $g_1(\tilde{z}), \ldots, g_k(\tilde{z}) \in XS$, $\rho(y_1, \ldots, y_n) \in \mathrm{FOM}^N$. *Тогда предикат*

$$\varphi(\tilde{z}) = \rho(g_1(\tilde{z}), \ldots, g_k(\tilde{z}))$$

лежит в S_*.

Д о к а з а т е л ь с т в о. Из определения FOM^N следует, что существует такой предикат $\psi(X)$ из FOM, что

$$\rho(y_1, \ldots, y_n) \equiv \psi(\mathrm{CODE}(y_1, \ldots, y_n)).$$

Из определения FOM следует, что существует FOM-формула Φ, которой соответствует предикат $\rho_\Phi(X, x_1, \ldots, x_m)$ такой, что

$$\rho_\Phi(X, x_1, \ldots, x_m) \equiv \psi(X).$$

Таким образом,

$$\rho(g_1(\tilde{z}), \ldots, g_k(\tilde{z})) \equiv \rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m).$$

Из утверждения 6 следует, что

$$\rho_\Phi(\mathrm{CODE}(g_1(\tilde{z}), \ldots, g_k(\tilde{z})), x_1, \ldots, x_m) \in S_*.$$

Утверждение доказано.

Утверждение 8. *Пусть* $g_1(\tilde{z}), \ldots, g_k(\tilde{z}) \in \mathrm{XS}$, $f(y_1, \ldots, y_n) \in \mathrm{FFOM}$. *Тогда*

$$h(\tilde{z}) = f(g_1(\tilde{z}), \ldots, g_k(\tilde{z}))$$

принадлежит XS.

Доказательство. Ограниченность $h(\tilde{z})$ функцией вида $2^{p(\tilde{z})}$, где p — некоторый полином, следует из ограничений в определениях XS и FFOM. Докажем, что $(h(\tilde{z})\langle t\rangle = 1) \in \mathrm{S}_*$. Действительно, ясно, что

$$(h(\tilde{z})\langle t\rangle = 1) \equiv \xi(g_1(\tilde{z}), \ldots, g_k(\tilde{z}), t),$$

где

$$\xi(y_1, \ldots, y_m, t) \equiv (f(y_1, \ldots, y_m)\langle t\rangle = 1).$$

Из определения FFOM следует, что $\xi \in \mathrm{FOM}^N$. Отсюда и из утверждения 7 следует, что

$$\xi(g_1(\tilde{z}), \ldots, g_k(\tilde{z}), t) \in \mathrm{S}_*.$$

А это эквивалентно тому, что

$$h(\tilde{z})\langle t\rangle \in \mathrm{S}$$

(потому что $h(\tilde{z})\langle t\rangle$ принимает только значения 0 и 1). Из этого и из определения XS следует, что $h \in \mathrm{XS}$. Утверждение доказано.

Утверждение 9. *Функции*

$$x + 1, \quad x \div y, \quad xy, \quad x \wedge y, \quad \lfloor x/y \rfloor, \quad x^{\mathrm{len}(y)}$$

лежат в классе FFOM.

Для функции $x \wedge y$ это очевидно следует из эквивалентных определений класса FOM (например, через схемы из функциональных элементов, см. [6]). Для остальных функций доказательство имеется в [5].

Утверждение 10. *Если* $f(\tilde{x}) \in \mathrm{S}$, *то* $2^{f(\tilde{x})} \div 1 \in \mathrm{XS}$.

Доказательство. Справедливость ограничения на скорость роста очевидна. Из простейших свойств двоичных записей чисел следует, что выполнено

$$((2^{f(\tilde{x})} \div 1)\langle y\rangle = 1) \equiv (y < f(\tilde{x})).$$

Ясно, что предикат $(x < y)$ лежит в S_* (см. [4]). Поэтому

$$(y < f(\tilde{x})) \in \mathrm{S}_*.$$

Из этого и следует доказываемое утверждение.

Теорема 1. *Имеет место включение* $[T]_{x^y} \subseteq \mathrm{XS}$.

Доказательство. Докажем это утверждение индукцией по построению функций в классе $[T]_{x^y}$. Пусть $h \in [T]_{x^y}$. Тогда возможны случаи.

1. $h \in T$. Тогда очевидно (см. например [4]), что $h \in \mathrm{S}$. Из $\mathrm{S} \subseteq \mathrm{XS}$ следует, что $h \in \mathrm{XS}$.

2. h получается из f перестановкой, отождествлением переменных или введением фиктивных переменных, $f \in \mathrm{XS}$. В этом случае включение $h \in \mathrm{XS}$, следует из того, что класс S замкнут относительно суперпозиции (в частности, перестановки, отождествления переменных, введения фиктивных переменных).

3. $h(\tilde{x}) = f(g_1(\tilde{x}), \ldots, g_m(\tilde{x}))$, где $f \in T$, $g_1, \ldots, g_m \in \mathrm{XS}$. В этом случае из утверждений 9 и 8 следует, что $h \in \mathrm{XS}$.

4. $h = f^g$, где $f \in \mathrm{XS}$, $g \in [T]$. Тогда можно записать

$$h = f^{\mathrm{len}(2^g \div 1)}.$$

Ясно, что $g \in \mathrm{S}$ (см. [4]), поэтому $2^g \div 1 \in \mathrm{XS}$ (утверждение 10). Отсюда, из соотношения $x^{\mathrm{len}(y)} \in \mathrm{FFOM}$ (утверждение 9) и из утверждения 8 следует, что $h \in \mathrm{XS}$. Теорема доказана.

§ 5. Классы $\mathbf{BA}^{\#}$, $\mathbf{BA}_f^{\#}$ и T-полиномиальность

Утверждение 11. *Класс* $\mathrm{BA}^{\#}$ *замкнут относительно ограниченных квантификаций вида* $(\exists x)_{x<p(\tilde{y})}$ *и* $(\forall x)_{x<p(\tilde{y})}$, *где* p — *полином с натуральными коэффициентами.*

Доказательство. Пусть

$$\varphi(\tilde{y}) \equiv (\exists x)_{x<p(\tilde{y})}\psi(x,\tilde{y}),$$

$\psi \in \mathrm{BA}^{\#}$. Пусть $\rho(x,\tilde{y},z)$ получается из $\psi(x,\tilde{y})$ с помощью операции подсчета по переменной x и полиному $p(\tilde{y})$. Тогда $\rho(x,\tilde{y},z)$ истинно в том и только в том случае, когда z есть количество таких t, $t<p(\tilde{y})$, что $\psi(t,\tilde{y})$ истинно. Из этого следует, что $\rho(0,\tilde{y},0)$ истинно тогда и только тогда, когда не существует такого t, $t<p(\tilde{y})$, что $\psi(t,\tilde{y})$ истинно. Отсюда следует, что при любом $\tilde{y}$ выполнено

$$\varphi(\tilde{y}) \equiv \neg\rho(0,\tilde{y},0).$$

Поскольку $\mathrm{BA}^{\#}$ замкнут относительно операции подсчета, операций подстановки констант и логических операций, получаем, что $\varphi \in \mathrm{BA}^{\#}$. Замкнутость класса $\mathrm{BA}^{\#}$ относительно $(\forall x)_{x<p(\tilde{y})}$ следует из замкнутости $\mathrm{BA}^{\#}$ относительно $(\exists x)_{x<p(\tilde{y})}$ и логических операций. Утверждение доказано.

Утверждение 12. *Имеет место включение* $\mathrm{BA} \subseteq \mathrm{BA}^{\#}$.

Доказательство. Действительно, для этого достаточно доказать, что $\mathrm{BA}^{\#}$ замкнут относительно квантификаций вида $(\exists x)_{x<y}$ и $(\forall x)_{x<y}$, а это следует из утверждения 11. Утверждение доказано.

Утверждение 13. *Класс* $\mathrm{BA}_f^{\#}$ *замкнут относительно суперпозиции.*

Доказательство. Замкнутость относительно перестановки, отождествления переменных и введения фиктивных переменных следует из того, что $\mathrm{BA}^{\#}$ замкнут относительно явных преобразований.

Докажем замкнутость относительно подстановки функций в функцию. Пусть

$$h(\tilde{x}) = f(g_1(\tilde{x}),\ldots,g_m(\tilde{x})),$$

$f, g_1, \ldots, g_m \in \mathrm{BA}_f^{\#}$. Установим, что $h \in \mathrm{BA}_f^{\#}$. Полиномиальная ограниченность функции h следует из полиномиальной ограниченности $f, g_1, \ldots, g_m$. Пусть $p(\tilde{x})$ — полином, ограничивающий сверху (строго) функции $g_1(\tilde{x}), \ldots, g_m(\tilde{x})$. Тогда

$$(z = h(\tilde{x})) \equiv (\exists y_1)_{y_1<p(\tilde{x})}\ldots(\exists y_m)_{y_m<p(\tilde{x})}((y_1 = g_1(\tilde{x}))\&\ldots\&(y_m = g_m(\tilde{x}))\& \\ \&(z = f(y_1,\ldots,y_m))).$$

Отсюда, из замкнутости $\mathrm{BA}^{\#}$ относительно логических операций и явных преобразований и из утверждения 11 следует, что $(z = h(\tilde{x})) \in \mathrm{BA}^{\#}$. Утверждение доказано.

Утверждение 14. *Класс* $\mathrm{BA}_f^{\#}$ *замкнут относительно операции суженного ограниченного суммирования.*

Доказательство. Пусть

$$f(x,z_1,\ldots,z_n) = \sum_{y<x} \mathrm{sg}(g(y,z_1,\ldots,z_n)),$$

$g \in \mathrm{BA}^{\#}_f$. Докажем, что $f \in \mathrm{BA}^{\#}_f$. Пусть

$$\rho(x, z_1, \ldots, z_n) \equiv \neg(0 = g(x, z_1, \ldots, z_n)).$$

Ясно, что ρ получается из графика g с помощью логических операций и подстановки констант, поэтому $\rho \in \mathrm{BA}^{\#}$. Пусть $\varphi(x, z_1, \ldots, z_n, u)$ получается из $\rho(x, z_1, \ldots, z_n)$ с помощью операции подсчета по переменной x и полиному x. Тогда $\varphi(x, z_1, \ldots, z_n, u)$ истинно тогда и только тогда, когда u есть количество $y < x$ таких, что $\rho(y, z_1, \ldots, z_n)$ истинно (т. е. $\mathrm{sg}(g(y, z_1, \ldots, z_n)) = 1$). Таким образом, при любых $x, z_1, \ldots, z_n, u$ выполнено

$$(u = f(x, z_1, \ldots, z_n)) \equiv \varphi(x, z_1, \ldots, z_n, u).$$

Из $\rho \in \mathrm{BA}^{\#}$ и из замкнутости $\mathrm{BA}^{\#}$ относительно явных преобразований и операции подсчета следует, что $\varphi \in \mathrm{BA}^{\#}$, т. е. график функции f лежит в $\mathrm{BA}^{\#}$. Полиномиальная ограниченность f, очевидно, следует из полиномиальной ограниченности g. Утверждение доказано.

У т в е р ж д е н и е 15. *Функции* 0, $x+1$, $x \div y$, xy *лежат в* $\mathrm{BA}^{\#}_f$.

Д о к а з а т е л ь с т в о. Известно [4], что предикаты

$$x = 0, \quad y = x + 1, \quad z = x \div y, \quad z = xy$$

лежат в BA. Из этого и из утверждения 12 следует доказываемое утверждение.

У т в е р ж д е н и е 16. *Выполнено* $\mathrm{S}_* \subseteq \mathrm{BA}^{\#}$.

Д о к а з а т е л ь с т в о. Из [4] известно, что S совпадает с наименьшим классом функций, содержащим функции 0, $x + 1$, $x \div y$, xy и замкнутым относительно суперпозиции и суженного ограниченного суммирования. Отсюда и из утверждений 15, 13, 14 следует, что

$$\mathrm{S} \subseteq \mathrm{BA}^{\#}_f.$$

Из [4] известно, что S_* есть множество всех графиков функций из S. Таким образом,

$$\mathrm{S}_* \subseteq \mathrm{BA}^{\#}.$$

Утверждение доказано.

Нетрудно убедиться в том, что справедливы следующие пять утверждений.

У т в е р ж д е н и е 17. *Если функция f T-полиномиальна по некоторому множеству переменных, то* $f \in [T]_{2^x}$.

У т в е р ж д е н и е 18. *Если функция f T-полиномиальна по множеству переменных X и $Y \subseteq X$, то f T-полиномиальна по множеству переменных Y.*

У т в е р ж д е н и е 19. *Если функция $f(x_1, \ldots, x_n)$ T-полиномиальна по множеству переменных $\{x_{i_1}, \ldots, x_{i_k}\}$, функция $g(y_1, \ldots, y_m)$ T-полиномиальна по множеству переменных $\{y_{j_1}, \ldots, y_{j_p}\}$, то*

$$f(x_1, \ldots, x_{i_1-1}, g(y_1, \ldots, y_m), x_{i_1+1}, \ldots, x_n)$$

T-полиномиальна по множеству переменных $\{x_{i_2}, \ldots, x_{i_k}, y_{j_1}, \ldots, y_{j_p}\}$.

У т в е р ж д е н и е 20. *Пусть функция $f(x_1, \ldots, x_n)$ T-полиномиальна по множеству переменных $\{x_{i_1}, \ldots, x_{i_k}\}$, $1 \leqslant i \leqslant n$, $i \notin \{i_1, \ldots, i_k\}$ и $g(y_1, \ldots, y_m) \in [T]$. Тогда*

$$f(x_1, \ldots, x_{i-1}, g(y_1, \ldots, y_m), x_{i+1}, \ldots, x_n)$$

T-полиномиальна по множеству $\{x_{i_1}, \ldots, x_{i_k}\}$.

Утверждение 21. *Пусть функция* $g(y_1, \ldots, y_m)$ *T-полиномиальна по множеству переменных* $\{y_{j_1}, \ldots, y_{j_n}\}$,

$$f(x_1, \ldots, x_k) = g(x_{i_1}, \ldots, x_{i_m}),$$

Тогда $f(x_1, \ldots, x_k)$ *T-полиномиальна по множеству всех переменных* x_i, *для которых множество всех* y_j *таких, что* $i_j = i$, *входит в* $\{y_{j_1}, \ldots, y_{j_n}\}$.

Утверждение 22. *Пусть* $f(x_1, \ldots, x_n)$ *T-полиномиальна по множеству переменных* X, $g(x_1, \ldots, x_n)$ *отличается от* f *в конечном числе точек. Тогда* $g(x_1, \ldots, x_n)$ *T-полиномиальна по* X.

Доказательство. Ясно, что достаточно доказать это утверждение для одной точки. Пусть

$$f(a_1, \ldots, a_n) = b, \quad g(a_1, \ldots, a_n) = c,$$

в остальных точках f и g совпадают. Тогда, если $b < c$, то

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + \\ + (c - b) \cdot (1 \div ((x_1 \div a_1) + (a_1 \div x_1))) \cdot \ldots \cdot (1 \div ((x_n \div a_n) + (a_n \div x_n))).$$

Аналогичная формула справедлива при $b > c$. Из этих формул и из утверждений 19—21 следует, что $g(x_1, \ldots, x_n)$ T-полиномиальна по X.

§ 6. Включение $\mathbf{XS} \subseteq [T]_{2^x}$

Утверждение 23. *Функция* $\mathrm{rm}(x, y)$ *T-полиномиальна по множеству переменных* $\{x, y\}$.

Доказательство. Имеем $\mathrm{rm}(x, y) = x \div [x/y] \cdot y$. Значит, $\mathrm{rm}(x, y) \in [T]$. Отсюда следует T-полиномиальность функции rm.

Пусть

$$\langle x_0, \ldots, x_{n-1};\ l \rangle = \sum_{i=0}^{n-1} x_i 2^{il}.$$

Заметим, что при выполнении условий $x_0, x_1, \ldots, x_{n-1} < 2^l$ для любого i $(0 \leqslant i < n)$ двоичные разряды числа $\langle x_0, x_1, \ldots, x_{n-1};\ l \rangle$ от (il)-го до $(il + l - 1)$-го образуют двоичную запись числа x_i.

Пусть

$$\mathrm{rep}(x, n, l) = x \cdot \left[\frac{2^{nl} \div 1}{2^l \div 1} \right].$$

Утверждение 24. *Если* $n, l \geqslant 1$, *то*

$$\mathrm{rep}(x, n, l) = \langle \underbrace{x, x, \ldots, x}_{n \text{ раз}};\ l \rangle.$$

Кроме того, $\mathrm{rep}(x, n, l)$ *T-полиномиальна по* $\{x\}$.

Доказательство. Пользуясь формулой суммы членов геометрической прогрессии, получаем

$$\mathrm{rep}(x, n, l) = x \cdot \sum_{i=0}^{n-1} 2^{li} = \sum_{i=0}^{n-1} x 2^{li} = \langle \underbrace{x, x, \ldots, x}_{n \text{ раз}};\ l \rangle.$$

T-полиномиальность по $\{x\}$ следует из вида формулы (x не входит в показатели степеней). Утверждение доказано.

Пусть

$$\mathrm{incrx}(x, n, l_1, l_2) = \mathrm{rep}(x, n, l_2 \div l_1) \wedge \mathrm{rep}(2^{l_1} \div 1, n, l_2).$$

Утверждение 25. *Если* $n, l_1 \geqslant 1$, $l_2 \geqslant (n+1)l_1$, $x = \langle x_0, \ldots, x_{n-1};\ l_1\rangle$, $0 \leqslant x_0, \ldots, x_{n-1} < 2^{l_1}$, *то*

$$\mathrm{incrx}(x, n, l_1, l_2) = \langle x_0, \ldots, x_{n-1};\ l_2\rangle.$$

Кроме того, $\mathrm{incrx}(x, n, l_1, l_2)$ *T-полиномиальна по* $\{x\}$.

Доказательство. Имеем

$$x = \sum_{i=0}^{n-1} x_i 2^{il_1} \leqslant \sum_{i=0}^{n-1} (2^{l_1} - 1)2^{il_1} < 2^{nl_1}.$$

Из $l_2 \geqslant (n+1)l_1$ следует, что

$$l_2 - l_1 \geqslant nl_1.$$

Поэтому двоичные разряды числа $\mathrm{rep}(x, n, l_2 \div l_1)$ от $i(l_2 - l_1)$-го до $(i(l_2 - l_1) + l_2 - l_1 - 1)$-го образуют двоичную запись числа x $(0 \leqslant i \leqslant n-1)$. Кроме того, двоичные разряды числа x от (il_1)-го до $(il_1 + l_1 - 1)$-го образуют двоичную запись числа x_i $(0 \leqslant i \leqslant n-1)$. Отсюда следует, что двоичные разряды числа $\mathrm{rep}(x, n, l_2 \div l_1)$ от (il_2)-го до $(il_2 + l_1 - 1)$-го образуют двоичную запись числа x_i $(0 \leqslant i \leqslant n-1)$.

Заметим, что двоичная запись числа $\mathrm{rep}(2^{l_1} \div 1, n, l_2)$ представляет собой n блоков из единиц, причем i-й блок $(0 \leqslant i \leqslant n-1)$ занимает разряды от (il_2)-го до $(il_2 + l_1 - 1)$-го. Таким образом, получаем, что

$$\mathrm{rep}(x, n, l_2 \div l_1) \wedge \mathrm{rep}(2^{l_1} \div 1, n, l_2) = \langle x_0, \ldots x_{n-1};\ l_2\rangle.$$

T-полиномиальность $\mathrm{incrx}(x, n, l_1, l_2)$ по $\{x\}$ следует из вида формулы, из T-полиномиальности $\mathrm{rep}(x, n, l)$ по $\{x\}$ и из утверждений 19, 21. Утверждение доказано.

Определим семейства функций p_n, a_n $(n \geqslant 1)$ следующим образом:

$$\mathrm{p}_n(q, m_1, \ldots, m_n) = q^{2^n} + q \cdot (m_1 + \ldots + m_n + 1),$$

$$\mathrm{a}_n(q, k_1, \ldots, k_n, m_1, \ldots, m_n) = q \cdot \mathrm{p}_n(q, m_1, \ldots, m_n) \cdot (k_1 + \ldots + k_n + 1).$$

В дальнейшем для краткости выражения $\mathrm{p}_n(q, m_1, \ldots, m_n)$ и $\mathrm{a}_n(q, k_1, \ldots$ $\ldots, k_n, m_1, \ldots, m_n)$ будем заменять на p и a соответственно. Определим семейство функций swap_n $(n \geqslant 1)$ следующим образом:

$$\mathrm{swap}_n(x, q, k_1, \ldots, k_n, m_1, \ldots, m_n) = \mathrm{rm}\left(\left[\frac{\mathrm{incrx}(x, q^n, 1, \mathrm{p}) \cdot \prod\limits_{r=1}^{n} \left[\frac{2^{\mathrm{a}+k_r\mathrm{p}} \div 2^{\mathrm{a}+k_r\mathrm{p}\div q(k_r\mathrm{p}\div m_r)}}{2^{k_r\mathrm{p}} \div 2^{m_r}}\right]}{2^{n\cdot\mathrm{a}}}\right], 2^{\mathrm{p}}\right).$$

Утверждение 26. *Пусть* $n, q \geqslant 1$, $f(i_1, \ldots, i_n)$ — *некоторая функция, принимающая значения* 0 *и* 1. *Кроме того, пусть числа*

$k_1, \ldots, k_n \geqslant 1$ таковы, что для любых различных векторов $(i'_1, \ldots, i'_n)$ и $(i''_1, \ldots, i''_n)$ $(0 \leqslant i'_1, \ldots, i'_n, i''_1, \ldots, i''_n < q)$ выполненяется неравенство

$$k_1 i'_1 + \ldots + k_n i'_n \neq k_1 i''_1 + \ldots + k_n i''_n.$$

Тогда, если

$$x = \sum_{0 \leqslant i_1, \ldots, i_n < q} f(i_1, \ldots, i_n) 2^{k_1 i_1 + \ldots + k_n i_n}, \tag{1}$$

то при любых $m_1, \ldots, m_n$ имеет место

$$\mathrm{swap}_n(x, q, k_1, \ldots, k_n, m_1, \ldots, m_n) = \sum_{0 \leqslant i_1, \ldots, i_n < q} f(i_1, \ldots, i_n) 2^{m_1 i_1 + \ldots + m_n i_n}.$$

Кроме того, $\mathrm{swap}_n(x, q, k_1, \ldots, k_n, m_1, \ldots, m_n)$ *T-полиномиальна по* $\{x\}$.

Доказательство. Из определения p и из того, что $k_r, q \geqslant 1$, следует, что при любом r $(1 \leqslant r \leqslant n)$ выполнено $k_r \mathrm{p} \geqslant m_r$. Кроме того, из определения a следует, что при любом r $(1 \leqslant r \leqslant n)$ выполнено $\mathrm{a} \geqslant q k_r \mathrm{p}$. Из этих двух неравенств следует, что

$$\left[\frac{2^{\mathrm{a}+k_r \mathrm{p}} \div 2^{\mathrm{a}+k_r \mathrm{p} \div q(k_r \mathrm{p} \div m_r)}}{2^{k_r \mathrm{p}} \div 2^{m_r}}\right] = \left[\frac{2^{\mathrm{a}+k_r \mathrm{p}} - 2^{\mathrm{a}+k_r \mathrm{p} - q(k_r \mathrm{p} - m_r)}}{2^{k_r \mathrm{p}} - 2^{m_r}}\right]$$

Воспользовавшись формулой суммы членов геометрической прогрессии, получаем

$$\left[\frac{2^{\mathrm{a}+k_r \mathrm{p}} \div 2^{\mathrm{a}+k_r \mathrm{p} \div q(k_r \mathrm{p} \div m_r)}}{2^{k_r \mathrm{p}} \div 2^{m_r}}\right] = \sum_{j=0}^{q-1} 2^{\mathrm{a}+j(m_r - k_r \mathrm{p})}.$$

Таким образом, имеем

$$\prod_{r=1}^{n} \left[\frac{2^{\mathrm{a}+k_r \mathrm{p}} \div 2^{\mathrm{a}+k_r \mathrm{p} \div q(k_r \mathrm{p} \div m_r)}}{2^{k_r \mathrm{p}} \div 2^{m_r}}\right] = \prod_{r=1}^{n} \sum_{j=0}^{q-1} 2^{\mathrm{a}+j(m_r - k_r \mathrm{p})} =$$

$$= \sum_{0 \leqslant j_1, \ldots, j_n < q} 2^{n\mathrm{a} + j_1(m_1 - k_1 \mathrm{p}) + \ldots + j_n(m_n - k_n \mathrm{p})}.$$

Из определения p и из $q \geqslant 1$, следует, что $\mathrm{p} \geqslant q^n + 1$. Отсюда, из того, что f принимает только значения из $\{0, 1\}$, и из (1) и утверждения 25 следует, что

$$\mathrm{incrx}(x, q^n, 1, \mathrm{p}) = \sum_{0 \leqslant i_1, \ldots, i_n < q} f(i_1, \ldots, i_n) 2^{\mathrm{p} \cdot (k_1 i_1 + \ldots + k_n i_n)}.$$

Таким образом,

$$\mathrm{incrx}(x, q^n, 1, \mathrm{p}) \cdot \prod_{r=1}^{n} \left[\frac{2^{\mathrm{a}+k_r \mathrm{p}} \div 2^{\mathrm{a}+k_r \mathrm{p} \div q(k_r \mathrm{p} \div m_r)}}{2^{k_r \mathrm{p}} \div 2^{m_r}}\right] =$$

$$= \Big(\sum_{0 \leqslant i_1, \ldots, i_n < q} f(i_1, \ldots, i_n) 2^{\mathrm{p} \cdot (k_1 i_1 + \ldots + k_n i_n)}\Big) \times$$

$$\times \Big(\sum_{0 \leqslant j_1, \ldots, j_n < q} 2^{n\mathrm{a} + j_1(m_1 - k_1 \mathrm{p}) + \ldots + j_n(m_n - k_n \mathrm{p})}\Big) =$$

$$= \sum_{\substack{0 \leqslant i_1, \ldots, i_n < q \\ 0 \leqslant j_1, \ldots, j_n < q}} f(i_1, \ldots, i_n) 2^{n\mathrm{a} + j_1 m_1 + \ldots + j_n m_n + \mathrm{p} \cdot (k_1(i_1 - j_1) + \ldots + k_n(i_n - j_n))}.$$

Разобьем все слагаемые этой суммы на три группы.

1. Слагаемые, для которых $k_1(i_1-j_1)+\ldots+k_n(i_n-j_n)\leqslant -1$. Сумму этих слагаемых обозначим через A. Ясно, что для таких слагаемых справедливы неравенства

$$na+j_1m_1+\ldots+j_nm_n+\mathrm{p}\cdot(k_1(i_1-j_1)+\ldots+k_n(i_n-j_n))\leqslant$$
$$\leqslant na+q\cdot(m_1+\ldots+m_n)-\mathrm{p}\leqslant na-q^{2n}.$$

Последнее неравенство следует из определения p. Из этих неравенств следует, что каждое слагаемое данного типа не превосходит $2^{na-q^{2n}}$. Отсюда и из того, что общее количество слагаемых равно q^{2n}, можно сделать вывод, что

$$A<2^{na}.$$

2. Слагаемые, для которых $k_1(i_1-j_1)+\ldots+k_n(i_n-j_n)\geqslant 1$. Пусть сумма этих слагаемых равна B. Ясно, что для таких слагаемых

$$na+j_1m_1+\ldots+j_nm_n+\mathrm{p}\cdot(k_1(i_1-j_1)+\ldots+k_n(i_n-j_n))\geqslant na+\mathrm{p}.$$

Поэтому каждое такое слагаемое делится на $2^{na+\mathrm{p}}$. Таким образом, имеем

$$B=2^{na+\mathrm{p}}B_0,$$

где B_0 — натуральное число.

3. Слагаемые, для которых $k_1(i_1-j_1)+\ldots+k_n(i_n-j_n)=0$, т. е.

$$k_1i_1+\ldots+k_ni_n=k_1j_1+\ldots+k_nj_n.$$

Пусть сумма этих слагаемых равна C. По условию, в этом случае $i_r=j_r$ для любого $r=1,2,\ldots,n$. Поскольку для каждого вектора $(j_1,\ldots,j_n)$ существует единственный вектор $(i_1,\ldots,i_n)$, для которого это условие выполняется, справедливо

$$C=\sum_{0\leqslant j_1,\ldots,j_n<q} f(j_1,\ldots,j_n)2^{na+j_1m_1+\ldots+j_nm_n}=2^{na}\cdot C_0,$$

где

$$C_0=\sum_{0\leqslant j_1,\ldots,j_n<q} f(j_1,\ldots,j_n)2^{j_1m_1+\ldots+j_nm_n}.$$

Количество слагаемых суммы равно q^n, каждое слагаемое не превосходит $2^{q\cdot(m_1+\ldots+m_n)}$. Отсюда и из определения p следует, что

$$C_0\leqslant q^n\cdot 2^{q\cdot(m_1+\ldots+m_n)}<2^{q^{2n}}\cdot 2^{q\cdot(m_1+\ldots+m_n)}\leqslant 2^{\mathrm{p}}.$$

Таким образом, имеем

$$\mathrm{swap}_n(x,q,k_1,\ldots,k_n,m_1,\ldots,m_n)=\mathrm{rm}\left(\left[\frac{A+2^{na+\mathrm{p}}B_0+2^{na}C_0}{2^{na}}\right],2^{\mathrm{p}}\right)=C_0.$$

Последнее равенство следует из того, что $A<2^{na}$ и $C_0<2^{\mathrm{p}}$. T-полиномиальность $\mathrm{swap}_n(x,q,k_1,\ldots,k_n,m_1,\ldots,m_n)$ по $\{x\}$ следует из вида формулы и из утверждений 19, 21, 25, 23.

Пусть

$$\mathrm{incr}(x,q,l)=\mathrm{swap}_1(x,q,1,l),$$
$$\mathrm{decr}(x,q,l)=\mathrm{swap}_1(x,q,l,1).$$

У т в е р ж д е н и е 27. *Пусть* $q, l \geqslant 1$, $0 \leqslant x_0, \ldots, x_{q-1} \leqslant 1$,

$$x = \langle x_0, \ldots, x_{q-1};\ 1\rangle.$$

Тогда

$$\mathrm{incr}(x, q, l) = \langle x_0, \ldots, x_{q-1};\ l\rangle.$$

Кроме того, $\mathrm{incr}(x, q, l)$ *T-полиномиальна по переменной* x.

Д о к а з а т е л ь с т в о. Пусть $k_1 = 1$, $m_1 = l$, $n = 1$, $f(i) = x_i$, если $i < q$, $f(i) = 0$ в противном случае. Тогда для чисел q, n, k_1, m_1, x и функции f выполнены все условия утверждения 26. Поэтому

$$\mathrm{swap}_1(x, q, 1, l) = \sum_{i=0}^{q-1} 2^{lx_i} = \langle x_0, \ldots, x_{n-1};\ l\rangle.$$

T-полиномиальность по $\{x\}$ следует из утверждений 27 и 19. Утверждение доказано.

У т в е р ж д е н и е 28. *Пусть* $q, l \geqslant 1$, $0 \leqslant x_0, \ldots, x_{q-1} \leqslant 1$,

$$x = \langle x_0, \ldots, x_{q-1};\ l\rangle.$$

Тогда

$$\mathrm{decr}(x, q, l) = \langle x_0, \ldots, x_{q-1};\ 1\rangle.$$

Кроме того, $\mathrm{decr}(x, q, l)$ *T-полиномиальна по множеству переменных* $\{x\}$.

Доказательство полностью аналогично доказательству утверждения 27.

Пусть

$$\mathrm{not}(x, n) = (2^n \div 1) \div x,$$
$$\mathrm{or}(x, y, n) = \mathrm{not}(\mathrm{not}(x, n) \wedge \mathrm{not}(y, n), n),$$
$$\mathrm{xor}(x, y, n) = \mathrm{or}(x, y, n) \wedge \mathrm{not}(x \wedge y, n).$$

У т в е р ж д е н и е 29. *Пусть* $n \geqslant 1$,

$$x = \langle x_0, \ldots, x_{n-1};\ 1\rangle,\ \ y = \langle y_0, \ldots, y_{n-1};\ 1\rangle,$$

$$0 \leqslant x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} \leqslant 1.$$

Тогда

$$\mathrm{not}(x, n) = \langle 1 - x_0, \ldots, 1 - x_{n-1};\ 1\rangle,$$
$$\mathrm{or}(x, y, n) = \langle x_0 + y_0 - x_0 y_0, \ldots, x_{n-1} + y_{n-1} - x_{n-1} y_{n-1};\ 1\rangle,$$
$$\mathrm{xor}(x, y, n) = \langle \mathrm{rm}(x_0 + y_0, 2), \ldots, \mathrm{rm}(x_{n-1} + y_{n-1}, 2);\ n\rangle.$$

Кроме того, $\mathrm{not}(x, n)$ *T-полиномиальна по* $\{x\}$, $\mathrm{or}(x, y, n)$ *и* $\mathrm{xor}(x, y, n)$ *T-полиномиальны по* $\{x, y\}$.

Д о к а з а т е л ь с т в о. Имеем

$$\mathrm{not}(x, n) = \sum_{i=0}^{n-1} 2^i \div \sum_{i=0}^{n-1} x_i 2^i = \sum_{i=0}^{n-1} (1 - x_i) 2^i = \langle 1 - x_0, \ldots, 1 - x_{n-1};\ 1\rangle.$$

Утверждения для or и xor следуют из этого и из соответствующих тождеств алгебры логики:

$$\alpha \vee \beta = \neg(\neg\alpha \wedge \neg\beta),$$
$$\alpha \oplus \beta = (\alpha \vee \beta) \wedge \neg(\alpha \wedge \beta).$$

T-полиномиальность следует из определения и утверждений 19—21. Утверждение доказано.

Утверждение 30. *Множество всех правильных предикатов замкнуто относительно операций логики высказываний.*

Доказательство. Пусть $\rho(x_1, \ldots, x_n)$, $\varphi(x_1, \ldots, x_n)$ — правильные предикаты, f_ρ, f_φ — их производящие функции,

$$\psi_1(x_1, \ldots, x_n) \equiv \neg\rho(x_1, \ldots, x_n),$$

$$\psi_2(x_1, \ldots, x_n) \equiv \rho(x_1, \ldots, x_n)\&\varphi(x_1, \ldots, x_n),$$

f_{ψ_1}, f_{ψ_2} — производящие функции предикатов ψ_1, ψ_2 соответственно. Из утверждения 29 и определения производящей функции следует, что при любом $x \geqslant 1$ выполнено

$$f_{\psi_1}(x) = \mathrm{not}(f_\rho(x), x^n), \qquad f_{\psi_2}(x) = f_\rho(x) \wedge f_\varphi(x).$$

Из этого и из утверждений 29, 19, 22 следует, что

$$f_{\psi_1}, f_{\psi_2} \in [T]_{2^x}.$$

Утверждение доказано.

Пусть

$$\mathrm{cmp}(x, y, n, l) = \\ = \mathrm{decr}\left(\left[\frac{((\mathrm{rep}(2^{2l \div 1}, n, 2l) + \mathrm{incr}(x, nl, 2)) \div \mathrm{incr}(y, nl, 2)) \wedge \mathrm{rep}(2^{2l \div 1}, n, 2l)}{2^{2l \div 1}}\right], n, 2l\right).$$

Утверждение 31. *Пусть* $n, l \geqslant 1$,

$$x = \langle x_0, \ldots, x_{n-1};\ l\rangle,\ \ y = \langle y_0, \ldots, y_{n-1};\ l\rangle,$$

$$0 \leqslant x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} < 2^l.$$

Тогда

$$\mathrm{cmp}(x, y, n, l) = \langle \sigma_0, \ldots, \sigma_{n-1};\ 1\rangle,$$

где

$$\sigma_i = \begin{cases} 1, & \text{если } x_i \geqslant y_i, \\ 0 & \text{в противном случае.} \end{cases}$$

Кроме того, $\mathrm{cmp}(x, y, n, l)$ T*-полиномиальна по* $\{x, y\}$.

Доказательство. Пусть $x_{i,j}$ означает j-й двоичный разряд числа x_i, $y_{i,j}$ — j-й разряд y_i. Тогда при любом i $(0 \leqslant i \leqslant n-1)$ выполнено

$$x_i = \langle x_{i,0}, \ldots, x_{i,l-1};\ 1\rangle, \quad y_i = \langle y_{i,0}, \ldots, y_{i,l-1};\ 1\rangle.$$

Кроме того,

$$x = \langle x_{0,0}, \ldots, x_{0,l-1}, x_{1,0}, \ldots, x_{1,l-1}, \ldots, x_{n,0}, \ldots, x_{n,l-1};\ 1\rangle,$$
$$y = \langle y_{0,0}, \ldots, y_{0,l-1}, y_{1,0}, \ldots, y_{1,l-1}, \ldots, y_{n,0}, \ldots, y_{n,l-1};\ 1\rangle.$$

Из утверждения 27 и простейших свойств двоичных записей чисел следует, что

$$\mathrm{incr}(x, nl, 2) = \langle x'_0, \ldots, x'_{n-1};\ 2l\rangle, \quad \mathrm{incr}(y, nl, 2) = \langle y'_0, \ldots, y'_{n-1};\ 2l\rangle,$$

где при всех i $(0 \leqslant i \leqslant n-1)$

$$x'_i = \langle x_{i,0}, \ldots, x_{i,l-1};\ 2\rangle, \quad y'_i = \langle y_{i,0}, \ldots, y_{i,l-1};\ 2\rangle.$$

Отсюда и из утверждения 24 следует, что

$$(\mathrm{rep}(2^{2l \div 1}, n, 2l) + \mathrm{incr}(x, nl, 2)) \div \mathrm{incr}(y, nl, 2) = \\ = \langle 2^{2l-1} + x'_0 - y'_0, \ldots, 2^{2l-1} + x'_{n-1} - y'_{n-1};\ 2l\rangle.$$

Отметим, что при любом i $(0 \leqslant i < n)$ справедливо

$$0 \leqslant 2^{2l-1} + x'_i - y'_i < 2^{2l}.$$

Из этого, из утверждения 24 и простейших свойств двоичных записей чисел следует, что

$$((\mathrm{rep}(2^{2l \div 1}, n, 2l) + \mathrm{incr}(x, nl, 2)) \div \mathrm{incr}(y, nl, 2)) \wedge \mathrm{rep}(2^{2l \div 1}, n, 2l) = \\ = \langle (2^{2l-1} + x'_0 \div y'_0) \wedge 2^{2l-1}, \ldots, (2^{2l-1} + x'_{n-1} \div y'_{n-1}) \wedge 2^{2l-1};\ 2l\rangle.$$

Очевидно, что при любом i $(0 \leqslant i < n)$

$$(2^{2l-1} + x'_i - y'_i) \wedge 2^{2l-1} = \begin{cases} 2^{2l-1}, & \text{если } x'_i \geqslant y'_i, \\ 0 & \text{в противном случае.} \end{cases}$$

Кроме того, при любом i $(0 \leqslant i < n)$ справедливо

$$(x_i \geqslant y_i) \Leftrightarrow (x'_i \geqslant y'_i).$$

Таким образом,

$$((\mathrm{rep}(2^{2l \div 1}, n, 2l) + \mathrm{incr}(x, nl, 2)) \div \mathrm{incr}(y, nl, 2)) \wedge \mathrm{rep}(2^{2l \div 1}, n, 2l) = \\ = \langle \sigma_0 2^{2l-1}, \ldots, \sigma_{n-1} 2^{2l-1};\ 2l\rangle.$$

Из этого и из утверждения 28 следует, что

$$\mathrm{cmp}(x, y, n, l) = \langle \sigma_0, \ldots, \sigma_{n-1};\ 1\rangle.$$

T-полиномиальность следует из 27, 28, 24, 19, 21.

Пусть

$$\mathrm{cmpeq}(x, y, n, l) = \mathrm{cmp}(x, y, n, l) \wedge \mathrm{cmp}(y, x, n, l).$$

У т в е р ж д е н и е 32. *Пусть* $n, l \geqslant 1$,

$$x = \langle x_0, \ldots, x_{n-1};\ l\rangle, \quad y = \langle y_0, \ldots, y_{n-1};\ l\rangle,$$

$$0 \leqslant x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1} < 2^l.$$

Тогда

$$\mathrm{cmpeq}(x, y, n, l) = \langle \sigma_0, \ldots, \sigma_{n-1};\ 1\rangle,$$

где

$$\sigma_i = \begin{cases} 1, & \textit{если } x_i = y_i, \\ 0 & \textit{в противном случае.} \end{cases}$$

Кроме того, $\mathrm{cmpeq}(x, y, n, l)$ *T-полиномиальна по* $\{x, y\}$.

Доказательство. Из утверждения 31 следует, что

$$\mathrm{cmp}(x,y,n,l)=\langle\sigma'_0,\ldots,\sigma'_{n-1};\ 1\rangle,\quad \mathrm{cmp}(y,x,n,l)=\langle\sigma''_0,\ldots,\sigma''_{n-1};\ 1\rangle,$$

где

$$\sigma'_i=\begin{cases}1, & \text{если } x_i\geqslant y_i,\\ 0 & \text{в противном случае,}\end{cases}\qquad \sigma''_i=\begin{cases}1, & \text{если } x_i\leqslant y_i,\\ 0 & \text{в противном случае.}\end{cases}$$

Отсюда следует первая часть доказываемого утверждения. Вторая часть следует из утверждения 31.

Утверждение 33. *При любом $n\geqslant 0$ функция $g_n(y,z)$, определяемая соотношением*

$$g_n(y,z)=\sum_{x<y}2^{xz}x^n,$$

принадлежит $[T]_{2^x}$.

Это утверждение следует из известных формул суммирования.

Следствие. *Если $r(z_1,\ldots,z_n)$ — полином с натуральными коэффициентами, то*

$$\sum_{0\leqslant z_1,\ldots,z_n<x} r(z_1,\ldots,z_n)2^{y(z_1+z_2x+\ldots+z_nx^{n-1})}\in[T]_{2^x}.$$

Доказательство. Действительно, ясно, что достаточно рассмотреть случай, когда r — одночлен,

$$r(z_1,\ldots,z_n)=C\cdot z_1^{m_1}\ldots z_n^{m_n}.$$

Тогда

$$\sum_{0\leqslant z_1,\ldots,z_n<x} r(z_1,\ldots,z_n)2^{y(z_1+z_2x+\ldots+z_nx^{n-1})}=$$
$$=\sum_{0\leqslant z_1,\ldots,z_n<x} C\cdot z_1^{m_1}\ldots z_n^{m_n}2^{y(z_1+z_2x+\ldots+z_nx^{n-1})}=$$
$$=C\cdot\Big(\sum_{0\leqslant z<x} z^{m_1}2^{zy}\Big)\cdot\Big(\sum_{0\leqslant z<x} z^{m_2}2^{zyx}\Big)\cdot\ldots\cdot\Big(\sum_{0\leqslant z<x} z^{m_n}2^{zyx^{n-1}}\Big).$$

Поэтому из утверждения 33 следует доказываемое утверждение.

Утверждение 34. *Пусть $p(x_1,\ldots,x_n)$ и $q(x_1,\ldots,x_n)$ — полиномы с натуральными коэффициентами. Тогда предикат*

$$\varphi(x_1,\ldots,x_n)\equiv(p(x_1,\ldots,x_n)\geqslant q(x_1,\ldots,x_n))$$

является правильным.

Доказательство. Для любой функции $r(z_1,\ldots,z_n)$ будем обозначать

$$g_r(x,y)=\sum_{0\leqslant z_1,\ldots,z_n<x} r(z_1,\ldots,z_n)2^{y(z_1+z_2x+\ldots+z_nx^{n-1})}.$$

По следствию из утверждения 33, $g_p(x,y)\in[T]_{2^x}$ и $g_q(x,y)\in[T]_{2^x}$.

Пусть

$$f(x) = \mathrm{cmp}(g_p(x, p+q+1), g_q(x, p+q+1), x^n, p+q+1),$$

где p, q — сокращенные обозначения для $p(\underbrace{x, \ldots, x}_{n \text{ раз}})$ и $q(\underbrace{x, \ldots, x}_{n \text{ раз}})$ соответственно. Докажем, что при любом $x \geqslant 1$ верно

$$f(x) = f_\varphi(x),$$

где f_φ — производящая функция предиката φ. Действительно, пусть $x \geqslant 1$. Заметим, что

$$g_p(x, p+q+1) = \\ = \langle p(0, \ldots, 0), p(1, 0, \ldots, 0), \ldots, p(x-1, \ldots, x-1);\ p+q+1\rangle,$$

$$g_q(x, p+q+1) = \\ = \langle q(0, \ldots, 0), q(1, 0, \ldots, 0), \ldots, q(x-1, \ldots, x-1);\ p+q+1\rangle$$

(вектора упорядочены в обратном лексикографическом порядке). Ясно, что при любых $z_1, \ldots, z_n$ таких, что $0 \leqslant z_1, \ldots, z_n < x$, справедливо

$$p(z_1, \ldots, z_n), q(z_1, \ldots, z_n) < 2^{p+q+1}.$$

Из этого и из утверждения 31 можно заключить, что

$$f(x) = \langle \sigma(0, \ldots, 0), \sigma(1, 0, \ldots, 0), \ldots, \sigma(x-1, \ldots, x-1);\ 1\rangle,$$

где

$$\sigma(z_1, \ldots, z_n) = \begin{cases} 1, & \text{если } p(z_1, \ldots, z_n) \geqslant q(z_1, \ldots, z_n), \\ 0 & \text{в противном случае.} \end{cases}$$

Таким образом, при $x \geqslant 1$ $f(x) = f_\varphi(x)$. Из утверждений 31, 19, 22 следует, что $f_\varphi(x) \in [T]_{2^x}$. Таким образом, φ — правильный предикат. Утверждение доказано.

Следствие. *Для полиномов p и q предикаты $p = q$, $p \neq q$, $p > q$ являются правильными.*

Действительно, это вытекает из утверждения 30 и соотношений

$$(p = q) \equiv (p \geqslant q)\&(q \geqslant p), \quad (p \neq q) \equiv \neg(p = q), \quad (p > q) \equiv (p \geqslant q)\&\neg(q \geqslant p).$$

Утверждение 35. *Множество всех правильных предикатов замкнуто относительно явных преобразований.*

Доказательство. Очевидно, что для доказательства утверждения достаточно установить замкнутость множества правильных предикатов относительно перестановки переменных, подстановки константы вместо последней переменной, отождествления последних двух переменных, введения последней фиктивной переменной.

1. *Перестановка переменных.* Пусть

$$\varphi(x_1, \ldots, x_n) = \psi(x_{i_1}, \ldots, x_{i_n}),$$

где $(i_1, \ldots, i_n)$ — некоторая перестановка чисел $1, 2, \ldots, n$, $f_\varphi(y), f_\psi(y)$ — производящие функции предикатов φ и ψ соответственно, предикат ψ — правильный. Тогда

$$f_\psi(y) = \sum_{0 \leqslant x_1, \ldots, x_n < y} \chi_\psi(x_1, \ldots, x_n) 2^{x_1 + x_2 y + \ldots + x_n y^{n-1}} = \\ = \sum_{0 \leqslant x_1, \ldots, x_n < y} \chi_\psi(x_1, \ldots, x_n) 2^{k_1 x_1 + \ldots + k_n x_n},$$

$$f_\varphi(y) = \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\psi(x_{i_1},\ldots,z_{i_n})2^{x_1+x_2y+\ldots+x_ny^{n-1}} =$$

$$= \sum_{0\leqslant z_1,\ldots,z_n<y} \chi_\psi(z_1,\ldots,z_n)2^{m_1z_1+\ldots+m_nz_n},$$

где

$$k_i = y^{i-1},\ m_i = y^{j_i-1},\ 1\leqslant i\leqslant n,$$

$(j_1,\ldots,j_n)$ — обратная перестановка к $(i_1,\ldots,i_n)$, χ_φ, χ_ψ — характеристические функции предикатов φ и ψ соответственно. Нетрудно заметить, что для чисел $y, k_1,\ldots,k_n, m_1,\ldots,m_n$ выполняются условия утверждения 26. Из этого следует, что

$$f_\varphi(y) = \mathrm{swap}_n(f_\psi(y), y, k_1,\ldots,k_n,m_1,\ldots,m_n) =$$
$$= \mathrm{swap}_n(f_\psi(y), y, 1, y,\ldots,y^{n-1},y^{j_1-1},\ldots,y^{j_n-1}).$$

Отсюда, из утверждений 19, 21, 26 и из $f_\psi\in[T]_{2^x}$ следует, что $f_\varphi\in[T]$. Таким образом, предикат φ — правильный.

2. *Подстановка константы вместо последней переменной.* Пусть

$$\varphi(x_1,\ldots,x_n) = \psi(x_1,\ldots,x_n,a),$$

где ψ — правильный предикат, $a\in N$ — некоторая константа. Положим

$$\rho(x_1,\ldots,x_{n+1}) \equiv \psi(x_1,\ldots,x_{n+1})\&(x_{n+1}=a).$$

Из утверждения 30, следствия из утверждения 34 и из того, что ψ — правильный, следует, что ρ тоже правильный. Пусть χ_φ, χ_ψ, χ_ρ — характеристические функции предикатов φ, ψ, ρ соответственно, f_φ, f_ψ, f_ρ — их производящие функции. Тогда при $y>a$ имеем

$$f_\rho(y) = \sum_{0\leqslant x_1,\ldots,x_{n+1}<y} \chi_\rho(x_1,\ldots,x_{n+1})2^{x_1+x_2y+\ldots,x_{n+1}y^n} =$$
$$= \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\psi(x_1,\ldots,x_n,a)2^{x_1+x_2y+\ldots,x_ny^{n-1}+ay^n} =$$
$$= 2^{ay^n}\cdot \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\varphi(x_1,\ldots,x_n)2^{x_1+x_2y+\ldots,x_ny^{n-1}} = 2^{ay^n}\cdot f_\varphi(y).$$

Таким образом, при любом $y>a$ выполнено

$$f_\varphi(y) = \left[\frac{f_\rho(y)}{2^{ay^n}}\right].$$

Отсюда, из $f_\rho\in[T]_{2^x}$ и из утверждений 19, 22 следует, что $f_\varphi\in[T]_{2^x}$. Таким образом, предикат φ — правильный.

3. *Отождествление последних двух переменных.* Пусть

$$\varphi(x_1,\ldots,x_n) = \psi(x_1,\ldots,x_n,x_n),$$

где ψ — правильный предикат. Положим

$$\rho(x_1,\ldots,x_{n+1}) \equiv \psi(x_1,\ldots,x_{n+1})\&(x_n=x_{n+1}).$$

Из утверждения 30, следствия из утверждения 34 и из того, что ψ — правильный, следует, что ρ тоже правильный. Пусть χ_φ, χ_ρ — характеристические функции предикатов φ, ρ соответственно, f_φ, f_ρ — их производящие функции. Тогда имеем

$$f_\rho(y) = \sum_{0\leqslant x_1,\ldots,x_{n+1}<y} \chi_\rho(x_1,\ldots,x_{n+1}) 2^{x_1+x_2y+\ldots,x_{n+1}y^n} =$$
$$= \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\varphi(x_1,\ldots,x_n) 2^{x_1+x_2y+\ldots+x_{n-1}y^{n-2}+x_n(y^{n-1}+y^n)} =$$
$$= \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\varphi(x_1,\ldots,x_n) 2^{k_1x_1+\ldots+k_nx_n},$$

где

$$k_i = y^{i-1},\ 1\leqslant i\leqslant n-1, \quad k_n = y^{n-1}+y^n.$$

С другой стороны,

$$f_\varphi(y) = \sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\varphi(x_1,\ldots,x_n) 2^{m_1x_1+\ldots+m_nx_n},$$

где

$$m_i = y^{i-1},\ 1\leqslant i\leqslant n.$$

Легко проверить, что для чисел $y, k_1,\ldots,k_n, m_1,\ldots,m_n$ выполняются условия утверждения 26. Таким образом, получаем

$$f_\varphi(y) = \mathrm{swap}_n(f_\rho(y), y, k_1,\ldots,k_n, m_1,\ldots,m_n) =$$
$$= \mathrm{swap}_n(f_\rho(y), y, 1, y, \ldots, y^{n-2}, y^{n-1}+y^n, 1, y, \ldots, y^{n-1}).$$

Из этого и из утверждений 26, 19, 21 следует, что $f_\varphi \in [T]_{2^x}$. Таким образом, предикат φ — правильный.

4. *Введение фиктивной последней переменной.* Пусть

$$\varphi(x_1,\ldots,x_n,x_{n+1}) = \psi(x_1,\ldots,x_n),$$

ψ — правильный предикат, χ_φ, χ_ψ — характеристические функции предикатов φ, ψ соответственно, f_φ, f_ψ — их производящие функции. При $y\geqslant 1$ имеем

$$f_\varphi(y) = \sum_{0\leqslant x_1,\ldots,x_{n+1}<y} \chi_\psi(x_1,\ldots,x_n) 2^{x_1+x_2y+\ldots+x_{n+1}y^n} =$$
$$= \Big(\sum_{0\leqslant x_1,\ldots,x_n<y} \chi_\psi(x_1,\ldots,x_n) 2^{x_1+x_2y+\ldots+x_ny^{n-1}}\Big)\cdot\Big(\sum_{0\leqslant x<y} 2^{xy^n}\Big) =$$
$$= f_\psi(y)\cdot\left[\frac{2^{y^{n+1}}\div 1}{2^{y^n}\div 1}\right].$$

Из этого и из утверждений 19 и 22 следует, что $f_\varphi \in [T]_{2^x}$, т. е. φ — правильный предикат.

Утверждение доказано.

Пусть

$$\mathrm{sum}(x,n,l,k) = \left[\frac{(x\cdot\left[\frac{2^{kl}\div 1}{2^l\div 1}\right])\wedge \mathrm{rep}(\mathrm{rep}(1,l,1),n,kl)}{2^{(k\div 1)l}}\right].$$

Утверждение 36. *Пусть* $n, l, k \geqslant 1$, $k < 2^l$,

$$x = \langle x_{0,0}, x_{0,1}, \ldots, x_{0,k-1}, \ldots, x_{n-1,0}, x_{n-1,1}, \ldots, x_{n-1,k-1};\ l\rangle,$$

где при всех i, j $(0 \leqslant i < n,\ 0 \leqslant j < k)$ *выполнено* $0 \leqslant x_{i,j} \leqslant 1$. *Тогда*

$$\mathrm{sum}(x, n, l, k) = \langle s_0, \ldots, s_{n-1};\ lk\rangle,$$

где

$$s_i = \sum_{j=0}^{k-1} x_{i,j}, \quad 0 \leqslant i < n.$$

Кроме того, $\mathrm{sum}(x, n, l, k)$ T*-полиномиальна по* $\{x\}$.

Доказательство. Представим x в следующем виде:

$$x = \langle y_0, \ldots, y_{kn-1};\ l\rangle,$$

причем

$$0 \leqslant y_i \leqslant 1, \quad 0 \leqslant i < kn.$$

Тогда

$$x \cdot \left[\frac{2^{kl} \div 1}{2^l \div 1}\right] = \Big(\sum_{0 \leqslant i < kn} y_i 2^{il}\Big) \cdot \Big(\sum_{0 \leqslant j < k} 2^{jl}\Big) = \sum_{\substack{0 \leqslant i < kn \\ 0 \leqslant j < k}} y_i 2^{(i+j)l} =$$

$$= \sum_{p=0}^{k(n+1)-2} \sum_{\substack{0 \leqslant i < kn \\ 0 \leqslant p-i < k}} y_i 2^{pl} = \langle z_0, \ldots, z_{k(n+1)-2};\ l\rangle,$$

где

$$z_p = \sum_{\substack{0 \leqslant i < kn \\ 0 \leqslant p-i < k}} y_i \qquad (0 \leqslant p \leqslant k(n+1) - 2).$$

Отметим, что двоичная запись числа $\mathrm{rep}(\mathrm{rep}(1, l, 1), n, kl)$ состоит из n блоков из единиц, причем r-й блок занимает разряды от $l(rk + k - 1)$-го до $(l(rk + k) - 1)$-го $(0 \leqslant r < n)$. Отсюда, из того, что при любом p $(0 \leqslant p \leqslant k(n+1) - 2)$ выполнено $z_p \leqslant k < 2^l$, и из того, что при любом i $(0 \leqslant i < n)$ справедливо $s_i = z_{ik+k-1}$, следует, что

$$\Big(x \cdot \left[\frac{2^{kl} \div 1}{2^l \div 1}\right]\Big) \wedge \mathrm{rep}(\mathrm{rep}(1, l, 1), n, kl) =$$

$$= \langle \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, z_{k-1}, \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, z_{2k-1}, \ldots, \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, z_{nk-1};\ l\rangle =$$

$$= \langle \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, s_0, \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, s_1, \ldots, \underbrace{0, \ldots, 0}_{k-1 \text{ раз}}, s_{n-1};\ l\rangle =$$

$$= 2^{(k-1)l} \cdot \langle s_0, \ldots, s_{n-1};\ kl\rangle.$$

Из этого следует, что

$$\mathrm{sum}(x, n, l, k) = \langle s_0, \ldots, s_{n-1};\ kl\rangle.$$

T-полиномиальность по $\{x\}$ следует из утверждений 24, 19, 21. Утверждение доказано.

Утверждение 37. *Множество всех правильных предикатов замкнуто относительно операции подсчета.*

Доказательство. В силу утверждения 35 достаточно доказать замкнутость относительно подсчета по первой переменной. Пусть $\varphi(x_1, \ldots, x_n, y)$ получается из $\psi(x_1, \ldots, x_n)$ с помощью операции подсчета по переменной x_1 и полиному $p(x_1, \ldots, x_n)$, ψ — правильный предикат. Введем предикат ρ следующим образом:

$$\rho(x, x_1, \ldots, x_n, y) \equiv \psi(x, x_2, \ldots, x_n)\&(x < p(x_1, \ldots, x_n)).$$

Из правильности ψ, утверждений 30, 35 и следствия из утверждения 34 следует, что ρ — правильный предикат. Пусть

$$q(z) = p(\underbrace{z, \ldots, z}_{n \text{ раз}}) + z + 1.$$

Положим

$$f'_\rho(z) = \mathrm{incr}(f_\rho(q(z)), q(z)^{n+2}, q(z)).$$

Пусть $z \geqslant 1$. Из утверждений 27, 19 следует, что $f'_\rho \in [T]_{2^x}$. Кроме того,

$$f_\rho(q(z)) = \langle \chi_\rho(0, \ldots, 0), \chi_\rho(1, 0, \ldots, 0), \ldots, \chi_\rho(q(z) - 1, \ldots, q(z) - 1);\ 1\rangle.$$

Поэтому из утверждения 27 следует, что

$$f'_\rho(z) = \langle \chi_\rho(0, \ldots, 0), \chi_\rho(1, 0, \ldots, 0), \ldots, \chi_\rho(q(z) - 1, \ldots, q(z) - 1);\ q(z)\rangle.$$

Положим

$$u(z) = \mathrm{sum}(f'_\rho(z), q(z)^{n+1}, q(z), q(z)).$$

Из утверждения 36 следует, что

$$u(z) = \langle g(0, \ldots, 0, z), g(1, 0, \ldots, 0, z), \ldots, g(q(z) - 1, \ldots, q(z) - 1, z);\ q(z)^2\rangle, \tag{2}$$

где $g(x_1, \ldots, x_n, y, z)$ есть количество $x < q(z)$ таких, что $\rho(x, x_1, \ldots, x_n, y)$ истинно. Кроме того, из утвердений 36 и 19 следует, что $u \in [T]_{2^x}$. Пусть

$$v(z) = \langle h(0, \ldots, 0), h(1, 0, \ldots, 0), \ldots, h(q(z) - 1, \ldots, q(z) - 1);\ q(z)^2\rangle, \tag{3}$$

где $h(x_1, \ldots, x_n, y) = y$ при любых натуральных $x_1, \ldots, x_n, y$. Ясно, что

$$v(z) = \Big(\sum_{y=0}^{q(z)-1} y 2^{y q(z)^{n-2}}\Big) \cdot \Big(\sum_{i=0}^{q(z)^n - 1} 2^{q(z)^2 i}\Big).$$

Из утверждения 33 следует, что $v(z) \in [T]_{2^x}$. Из (2), (3) и утверждения 32 следует, что

$$\mathrm{cmpeq}(u(z), v(z), q(z)^{n+1}, q(z)^2) = \\ = \langle \sigma(0, \ldots, 0, z), \sigma(1, \ldots, 0, z), \ldots, \sigma(q(z) - 1, \ldots, q(z) - 1, z);\ 1\rangle, \tag{4}$$

где

$$\sigma(x_1, \ldots, x_n, y, z) = \begin{cases} 1, & \text{если } y \text{ есть количество } x < q(z) \text{ таких,} \\ & \text{что } \rho(x, x_1, \ldots, x_n, y) \text{ истинно,} \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть

$$w(z)=\sum_{0\leqslant i_1,\ldots,i_{n+1}<z}2^{i_1+i_2q(z)+\ldots+i_{n+1}q(z)^n}=\prod_{j=1}^{n+1}\left(\sum_{i=0}^{z-1}2^{iq(z)^{j-1}}\right).$$

Из утверждения 33 следует, что $w\in[T]$. Из того, что $q(z)>z$, следует, что

$$w(z)=\langle\xi(0,\ldots,0,z),\xi(1,\ldots,0,z),\ldots,\xi(q(z)-1,\ldots,q(z)-1,z);\ 1\rangle,$$

где при всех натуральных $x_1,\ldots,x_n,y,z$ выполнено

$$\xi(x_1,\ldots,x_n,y,z)=\begin{cases}1, & \text{если истинно } (x_1<z)\&\ldots\&(x_n<z)\&(y<z),\\ 0 & \text{в противном случае.}\end{cases}$$

Из этого и из (4) следует, что

$$\begin{aligned}&\mathrm{cmpeq}(u(z),v(z),q(z)^{n+1},q(z)^2)\wedge w(z)=\\ &\quad=\langle\sigma'(0,\ldots,0,z),\sigma'(1,\ldots,0,z),\ldots,\sigma'(q(z)-1,\ldots,q(z)-1,z);\ 1\rangle,\end{aligned}$$

где

$$\sigma'(x_1,\ldots,x_n,y,z)=\begin{cases}1, & \text{если выполнено } (x_1<z)\&\ldots\&(x_n<z)\&(y<z)\\ & \text{и } y \text{ есть количество } x<q(z) \text{ таких,}\\ & \text{что } \rho(x,x_1,\ldots,x_n,y) \text{ истинно,}\\ 0 & \text{в противном случае.}\end{cases}$$

Из этого следует, что

$$\begin{aligned}&\mathrm{cmpeq}(u(z),v(z),q(z)^{n+1},q(z)^2)\wedge w(z)=\\ &\qquad=\sum_{0\leqslant x_1,\ldots,x_n,y<z}\sigma(x_1,\ldots,x_n,y,z)2^{x_1+x_2q(z)+\ldots+x_nq(z)^{n-1}+yq(z)^n}.\end{aligned}$$

Отсюда, из того, что $q(z)>z$, и из утверждения 26 следует, что

$$\begin{aligned}&\mathrm{swap}_{n+1}(\mathrm{cmpeq}(u(z),v(z),q(z)^{n+1},q(z)^2)\wedge\\ &\qquad\wedge w(z),z,1,q(z),\ldots,q(z)^n,1,z,\ldots,z^n)=\\ &\quad=\sum_{0\leqslant x_1,\ldots,x_n,y<z}\sigma(x_1,\ldots,x_n,y,z)2^{x_1+x_2z+\ldots+x_nz^{n-1}+yz^n}=\\ &\quad=\langle\sigma(0,\ldots,0,z),\sigma(1,\ldots,0,z),\ldots,\sigma(z-1,\ldots,z-1,z);\ 1\rangle.\qquad(5)\end{aligned}$$

Ясно, что при любых $x_1,\ldots,x_n<z$ справедливо $p(x_1,\ldots,x_n)<q(z)$. Из этого и из определения σ и ρ следует, что при любых $x_1,\ldots,x_n,y,z$ таких, что $x_1,\ldots,x_n<z$, выполнено

$$\sigma(x_1,\ldots,x_n,y,z)=\begin{cases}1, & \text{если } y \text{ есть количество } x<p(x_1,\ldots,x_n) \text{ таких,}\\ & \text{что } \psi(x,x_2,\ldots,x_n) \text{ истинно,}\\ 0 & \text{в противном случае.}\end{cases}$$

Из этого и из (5) следует, что при любом $z\geqslant 1$ выполнено

$$\begin{aligned}f_\varphi(z)=\mathrm{swap}_{n+1}(&\mathrm{cmpeq}(u(z),v(z),q(z)^{n+1},q(z)^2)\wedge\\ &\wedge w(z),z,1,q(z),\ldots,q(z)^n,1,z,\ldots,z^n).\end{aligned}$$

Поэтому из включений $u(z), v(z), w(z) \in [T]$ и из утверждений 26, 32, 22, 19, 21 следует, что $f_\varphi \in [T]$. Утверждение доказано.

Утверждение 38. *Любой предикат из* $\mathrm{BA}^{\#}$ *является правильным.*

Доказательство. Действительно, по следствию из утверждения 34 предикаты $x+y=z$ и $xy=z$ являются правильными. Отсюда и из утверждений 35, 30 и 37 следует, что любой предикат из $\mathrm{BA}^{\#}$ является правильным. Утверждение доказано.

Теорема 2. *Имеет место включение*

$$\mathrm{XS} \subseteq [T]_{2^x}.$$

Доказательство. Пусть $f(x_1, \ldots, x_n) \in \mathrm{XS}$. Тогда

$$g(x_1, \ldots, x_n, y) = f(x_1, \ldots, x_n)\langle y \rangle \in \mathrm{S}.$$

Из утверждения 16 следует, что $g(x_1, \ldots, x_n, y)$ есть характеристическая функция некоторого предиката $\psi \in \mathrm{BA}^{\#}$. Из утверждения 38 следует, что ψ — правильный предикат. Из определения производящей функции следует, что

$$f_\psi(z) = \sum_{0 \leqslant x_1, \ldots, x_n, y < z} g(x_1, \ldots, x_n, y) 2^{x_1 + x_2 z + \ldots + x_n z^{n-1} + y z^n}.$$

Таким образом, при любых $x_1, \ldots, x_n, y, z$ таких, что $x_1, \ldots, x_n, y < z$ и $z \geqslant 1$, y-й двоичный разряд числа $f(x_1, \ldots, x_n)$ равен двоичному разряду числа $f_\psi(z)$ с номером $x_1 + x_2 z + \ldots + x_n z^{n-1} + y z^n$. Если дополнительно длина двоичной записи $f(x_1, \ldots, x_n)$ не превосходит t, то из утверждения 28 следует, что

$$f(x_1, \ldots, x_n) = \mathrm{decr}\left(\left[\frac{f_\psi(z)}{2^{x_1 + x_2 z + \ldots + x_n z^{n-1}}} \right], t z^n, z^n \right).$$

Подставив вместо z выражение $x_1 + \ldots + x_n + 1$, а вместо t полином $t(x_1, \ldots, x_n)$ такой, что при любых $x_1, \ldots, x_n$ имеет место

$$f(x_1, \ldots, x_n) < 2^{t(x_1, \ldots, x_n)},$$

получим выражение для f. Из правильности предиката ψ и из утверждений 28 и 19 следует, что $f \in [T]_{2^x}$. Теорема доказана.

§ 7. Доказательство основной теоремы

Имеет место включение

$$[T]_{2^x} \subseteq [T]_{x^y}.$$

Кроме того, из теоремы 1 следует, что $[T]_{x^y} \subseteq \mathrm{XS}$, а из теоремы 2 вытекает, что $\mathrm{XS} \subseteq [T]_{2^x}$. Таким образом,

$$[T]_{x^y} \subseteq \mathrm{XS} \subseteq [T]_{2^x} \subseteq [T]_{x^y}.$$

Поэтому

$$\mathrm{XS} = [T]_{2^x} = [T]_{x^y}.$$

Основная теорема доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Гжегорчик А. Некоторые классы рекурсивных функций // Проблемы математической логики. — М.: Мир. — 1970. — С. 9–49.
2. Марченков С. С. Об одном базисе по суперпозиции в классе функций, элементарных по Кальмару // Матем. заметки. — 1980. — Т. 27, № 3. — С. 321–332.
3. Марченков С. С. Простые примеры базисов по суперпозиции в классе функций, элементарных по Кальмару // Banach Center Publication. Warsaw. — 1989. — Т. 25. — С. 119–126.
4. Марченков С. С. Элементарные рекурсивные функции. — М.: МЦНМО, 2003.
5. Allender E., Barrington D. A. M., Hesse W. Uniform constant-depth threshold circuits for division and iterated multiplication // Journal of Computer and System Sciences. — 2002. — V. 65. — P. 695–716.
6. Barrington D. A. M., Immerman N., Straubing H. On uniformity within NC^1 // Journal of Computer and System Sciences. — 1990. — V. 41. — P. 274–306.
7. Mazzanti S. Plain bases for classes of primitive recursive functions // Mathematical Logic Quarterly. — 2002. — V. 48. — P. 93–104.
8. Parsons Ch. Hierarchies of primitive recursive functions // Zeitschr. math. Logik u. Grundlag. Math. — 1968. — B. 14, № 4. — S. 357–376.
9. Rödding D. Über die Eliminierbarkeit von Definitionsschemata in der Theorie der rekursiven Funktionen // Zeitschr. math. Logik. u. Grundlag. Math. — 1964. — B. 10, № 4. — S. 315–330.

Поступило в редакцию 4 II 2006