ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Март—апрель 2009. Том 16, № 2. С. 42–60

УДК 519.712

О КЛАССЕ ФУНКЦИЙ, ЭЛЕМЕНТАРНЫХ ПО СКОЛЕМУ

С. А. Волков

Аннотация. Рассматриваются различные эквивалентные определения класса функций, элементарных по Сколему (аналогичные известным для класса функций, элементарных по Кальмару), и некоторые результаты, связанные с этим классом, полученные различными математиками. Некоторые определения данного класса исследовались математиками независимо друг от друга, и в этой работе доказана их эквивалентность. Исследуется вопрос о наличии в этом классе конечных базисов по суперпозиции. Доказывается, что проблема наличия таких базисов эквивалентна известной проблеме из теории сложности вычислений.

Ключевые слова: классификация рекурсивных функций, вычислительная сложность.

Введение

В 1943 г. Кальмар на основе операций суперпозиции, ограниченного суммирования и ограниченного умножения определил класс функций (обозначим его K), который назван классом элементарных функций (см. [17]). Этот класс исследовался многими математиками, получено много различных эквивалентных определений этого класса, например, на основе порождающих операций, примененных к некоторому базовому набору функций [4, 6, 7–9, 16, 18, 19, 21], выразимости логико-арифметическими формулами [10, 11, 16], сложности вычислений на машинах Тьюринга и их модификациях [4, 20].

В 1962 году Сколем предложил исследовать класс функций (обозначим его S), который получается, если из определения класса K убрать операцию ограниченного умножения [22, 23]. Функции из этого класса были названы “lower elementary functions”. В отечественной терминологии принято вместо этого использовать словосочетание «функции, элементарные по Сколему». Нетрудно показать, что S существенно меньше, чем K. В частности, S не содержит функцию 2^x. Однако Сколем доказал, что любое рекурсивно перечислимое множество перечислимо функциями из этого класса.

Класс S исследовался математиками значительно меньше, чем K. Однако, как выяснилось, этот класс, как и K, имеет много различных эквивалентных определений.

В [3, 9] показано, что S может быть порождён с использованим различных видов ограниченного суммирования (подробности см. в разд. 2).

Особый интерес представляет соответствующий классу функций S класс предикатов S_*. В [5] доказано, что все предикаты из S_* лежат в классе $\mathcal{E}^0_*$ предикатов, соответствующих классу $\mathcal{E}^0$ иерархии Гжегорчика [9, 16], несмотря на то, что $S \nsubseteq \mathcal{E}^0$. Кроме того, интерес представляет вопрос о соотношении между S_* и классом рудиментарных предикатов R [9, 24]. Несложно доказывается, что $R \subseteq S_*$. В [15] на основе операции подсчёта введён класс $R^{\#}$ и доказано, что этот класс замкнут относительно подстановки полиномов. На основе данного результата легко доказывается, что $R^{\#} = S_*$. Кроме того, этот результат даёт альтернативное доказательство включения $S_* \subseteq \mathcal{E}^0_*$. Вопрос о соотношении классов R и $R^{\#}$ (или S_*) на данный момент открыт. Однако есть некоторые убедительные аргументы в пользу того, что эти классы не совпадают. Например, на основе техники из [25] сколь угодно большое количество перемен кванторов, ограниченных функциями вида $2^{(\log x)^n}$, можно «моделировать» с помощью одной операции, являющейся разновидностью операции подсчёта, ограниченной для некоторого достаточно большого m функцией вида $2^{(\log x)^m}$.

Отметим, что как доказательство соотношения $S_* \subseteq \mathcal{E}^0_*$ в [5], так и доказательство замкнутости $R^{\#}$ относительно подстановки полиномов в [15] используют китайскую теорему об остатках и нетривиальный результат о распределении простых чисел. В разд. 3 приведено достаточно простое доказательство эквивалентности $R^{\#} = S_*$ без ссылок на какие-либо нетривиальные результаты из теории чисел (из этой эквивалентности сразу следуют оба приведённых выше утверждения).

В [14] введён класс R^{Maj} на основе обобщённого квантора мажорирования (подробнее об этом в разд. 3), а также иерархии сложностных классов $\mathrm{LTH}^{\#}$ (количественная линейная иерархия по времени) и PLTH (вероятностная линейная иерархия по времени), и доказано, что $R^{\#} = R^{\mathrm{Maj}} = \mathrm{LTH}^{\#}_* = \mathrm{PLTH}$ аналогично тому, как было сделано в [26] для рудиментарных предикатов (см. разд. 5).

Особый интерес представляет вопрос о существовании конечных базисов по суперпозиции в классе S. Для класса K этот вопрос очень хорошо изучен: в [21] доказано существование таких базисов, в [6–8, 18] и др. приведены примеры базисов, состоящих из функций очень простого вида. Для класса S этот вопрос на данный момент открыт и представляется очень трудным для разрешения. В разд. 5 показано, что существование такого базиса эквивалентно вырожденности иерархии $\mathrm{LTH}^{\#}$. Однако существует другой подход к описанию класса S в терминах суперпозиции функций из конечного набора. В работе [2] введён класс XS, являющийся расширением класса S, состоящий из функций, ограниченных функциями вида $2^{p(\tilde{x})}$, где p — полином, причём все функции из XS, ограниченные полиномами, лежат в S. Этот класс назван экспоненциальным расширением S. Данный класс оказался достаточно «естественным». В частности, на основе результатов [13] можно показать, что он замкнут относительно ограниченного суммирования и умножения. Доказано [2], что при наложении ограничений на структуру формул XS имеет базис по суперпозиции, состоящий из функций простого вида, аналогичный известным для класса K. Этот результат интересен ещё и тем, что даёт эквивалентное определение класса S, не содержащее какой-либо разновидности суммирования или подсчёта. Подробности см. в разд. 6.

1. Основные понятия

Рассматриваются всюду определённые функции (произвольного числа аргументов) на множестве $\mathbb{N} = \{0, 1, 2, \ldots\}$. Под операцией *суперпозиции* будем подразумевать подстановку функций в функцию, перестановку и отождествление переменных, введение фиктивных переменных.

Через $[Q]$ будем обозначать *замыкание по суперпозиции* класса Q. *Базисом по суперпозиции* в классе Q будем называть полную относительно суперпозиции систему в этом классе.

Векторы из переменных будем иногда для сокращения обозначать символами типа $\tilde{x}$, $\tilde{y}$ и т. п., например, $\tilde{x}$ вместо $(x_1, \ldots, x_n)$.

Графиком функции $f(\tilde{x})$ будем называть предикат $(y = f(\tilde{x}))$.

Положим

$$\begin{aligned}
&x \dot{-} y = \max(x - y, 0),\\
&\mathrm{sg}(x) = \begin{cases} 1 \text{ при } x > 0, \\ 0 \text{ в противном случае}, \end{cases}\\
&\overline{\mathrm{sg}}(x) = 1 \dot{-} x,\\
&[x/y] = \begin{cases} \text{целой части от деления } x \text{ на } y \text{ при } y > 0, \\ 0 \text{ в противном случае}, \end{cases}
\end{aligned}$$

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

Класс S функций, *элементарных по Сколему* [9, 22, 23], — это минимальный класс функций, содержащий функции $x+1$, $x \dot{-} y$ и замкнутый относительно суперпозиции и ограниченного суммирования вида $\sum\limits_{x\leqslant y}$. Отметим, что форму суммирования в этом определении можно заменить на $\sum\limits_{x<y}$, при этом получаемый класс не изменится (считаем, что сумма по пустому множеству равна нулю).

Будем говорить, что функция $f(x_1, \ldots, x_n, y)$ получена из функций $g(x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n, y, z)$, $j(x_1, \ldots, x_n, y)$ с помощью операции *ограниченной рекурсии*, если выполняются соотношения

$$\begin{aligned}&f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n),\\ &f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)),\\ &f(x_1, \ldots, x_n, y) \leqslant j(x_1, \ldots, x_n, y).\end{aligned}$$

Определим класс $\mathcal{E}^0$ иерархии Гжегорчика [9, 16] как наименьший класс функций, содержащий функции 0, $x+1$ и замкнутый относительно операций суперпозиции и ограниченной рекурсии.

Под *явными преобразованиями* будем подразумевать перестановку и отождествление переменных, введение фиктивных переменных и подстановку констант.

Класс R *рудиментарных предикатов* [9, 24] определим как множество всех предикатов, которые можно получить из предикатов $(x+y=z)$ и $(xy=z)$ с помощью явных преобразований, логических операций $\&$, $\vee$, $\neg$ и ограниченных квантификаций вида $(\forall x)_{x<y}$ и $(\exists x)_{x<y}$ (будем считать, что результатом применения квантификации $(\forall x)_{x<0}$ является тождественно истинный предикат, а $(\exists x)_{x<0}$ — тождественно ложный).

Будем говорить, что предикат $\rho(x_1,\ldots,x_n,y)$ получается из предиката $\varphi(x_1,\ldots,x_n)$ с помощью *операции подсчёта* по переменной x_i, если при любых $x_1,\ldots,x_n,y$ имеет место

$$\rho(x_1,\ldots,x_n,y) \equiv (|\{x<x_i \mid \varphi(x_1,\ldots,x_{i-1},x,x_{i+1},\ldots,x_n)\}| = y).$$

Класс $\mathrm{R}^{\#}$ *количественно-рудиментарных предикатов* [14, 15] определим как множество всех предикатов, которые можно получить из предикатов $(x+y=z)$ и $(xy=z)$ с помощью явных преобразований, логических операций $\&$, $\vee$, $\neg$, ограниченных квантификаций вида $(\forall x)_{x<y}$ и $(\exists x)_{x<y}$ и операций подсчёта.

Введём *обобщённый квантор мажорирования* M: если $\varphi(x, y, \tilde{z})$ — некоторый предикат, то положим

$$(\mathrm{M}x)_{x<y}\varphi(x, y, \tilde{z}) \equiv (|\{x < y \mid \varphi(x, y, \tilde{z})\}| > y/2).$$

Пусть $\mathrm{R}^{\mathrm{Maj}}$ [14] — множество всех предикатов, которые можно получить из предикатов $(x + y = z)$ и $(xy = z)$ с помощью явных преобразований, логических операций &, $\vee$, $\neg$ и ограниченных квантификаций вида $(\forall x)_{x<y}$, $(\exists x)_{x<y}$ и $(\mathrm{M}x)_{x<y}$.

Если Q — некоторый класс функций, то через Q_* будем обозначать множество всех предикатов, характеристические функции которых лежат в Q (под *характеристической функцией* будем подразумевать функцию, равную 1 в точках, где значение предиката истинно, 0 в остальных точках).

Будем рассматривать недетерминированные многоленточные односторонние (с бесконечными вправо лентами) машины Тьюринга с одной входной лентой (только для чтения), двумя лентами для обращения к оракулу и несколькими рабочими лентами. В качестве входного и рабочего алфавитов будем использовать алфавит $\{0, 1, *\}$ (для упрощения будем считать, что в каждый момент времени в начале каждой ленты записано некоторое слово в этом алфавите, все остальные ячейки лент заполнены пустыми символами Λ; этот символ может быть прочитан, но не может быть записан). У машины будет несколько выделенных состояний: q_0 (начальное состояние), q_a (заключительное состояние, означающее, что машина успешно завершила работу), q_{call} (состояние обращения к оракулу), q_{yes} (оракул выдал ответ «да»), q_{no} (оракул выдал ответ «нет»).

Кодом вектора $(x_1, \ldots, x_n)$ будем называть слово $s_1 * s_2 * \ldots * s_n$, где s_i — двоичная запись x_i $(1 \leqslant i \leqslant n)$.

Через $\mathrm{len}(x_1, \ldots, x_n)$ будем обозначать длину кода вектора $(x_1, \ldots, x_n)$.

Если Q — некоторый класс функций, то через $\#\mathrm{LinTime}(Q)$ обозначим множество всех функций $f(x_1, \ldots, x_n)$, для которых существуют функция $q \in Q$, недетерминированная машина Тьюринга M, обращающаяся к оракулу q, и константы $C_1, C_2 \in \mathbb{N}$ такие, что для любых $x_1, \ldots, x_n$ значение $f(\tilde{x})$ есть число ветвей вычисления машины M (на вход подаётся код вектора $\tilde{x}$), на которых она успешно завершает работу за не более $C_1\mathrm{len}(\tilde{x}) + C_2$ шагов; обращение к оракулу $q(y_1, \ldots, y_m)$ происходит с использованием двух выделенных лент следующим образом: если в состоянии q_{call} на первой ленте записан код некоторого вектора $(y_1, \ldots, y_m)$, на второй — двоичная запись некоторого числа z и

$z = q(y_1, \ldots, y_m)$, то машина переходит в состояние q_{yes}, в противном случае она переходит в q_{no}. Класс #LinTime определим аналогичным образом, рассматривая машины Тьюринга без оракула.

Пусть

$$\Sigma_1^{\#\text{lin}} = \#\text{LinTime},\ \Sigma_{n+1}^{\#\text{lin}} = \#\text{LinTime}(\Sigma_n^{\#\text{lin}}),\ n \geqslant 1,\ \text{LTH}^{\#} = \bigcup_{n=1}^{\infty} \Sigma_n^{\#\text{lin}}.$$

Класс $\text{LTH}^{\#}$ [14]* будем называть *количественной линейной иерархией по времени* (Counting Linear Time Hierarchy).

2. Разновидности ограниченного суммирования

Теорема 1. S *есть множество всех функций, которые можно получить из исходных функций* $x + 1,\ x \dot{-} y,\ xy$ *с помощью операции суперпозиции и суммирования вида* $\sum\limits_{x \leqslant y} \overline{\text{sg}}(f)$.

Доказательство можно найти в [9]. Следующая теорема впервые доказана в [3], доказательство можно также найти в [9].

Теорема 2. S *есть множество всех функций, которые можно получить из набора* $1,\ x + y,\ x \dot{-} [\sqrt{x}]^2$ *с помощью суперпозиции и ограниченного суммирования вида* $\sum\limits_{x \leqslant y}$, *которое можно применять только к одноместным функциям.*

Теорема 3. *Все одноместные функции класса* S *и только они могут быть получены из функций* $1,\ x \dot{-} [\sqrt{x}]^2$ *с помощью следующих трёх операций, действующих на множестве одноместных функций: композиции* $(f(g)(x) = f(g(x)))$, *сложения двух функций* $((f + g)(x) = f(x) + g(x))$ *и одноместного ограниченного суммирования вида* $\sum\limits_{x \leqslant y}$.

Доказательство можно найти в [9]. Отметим, что все три теоремы верны и для суммирования вида $\sum\limits_{x < y}$.

3. Количественно-рудиментарные предикаты и мажорирование

Через $\text{R}_{\text{Pol}}^{\#f}$ ($\text{R}_{\text{Max}}^{\#f}$) обозначим множество всех функций $f(x_1, \ldots, x_n)$, ограниченных сверху полиномами (функциями вида $\max(x_1, \ldots, x_n) + C$, где C — константа, соответственно), графики которых лежат в $\text{R}^{\#}$.

---

*Определение в [14] немного отличается от данного, но эквивалентность этих определений легко доказывается.

Пусть $\mathrm{R}^{\#}_{\mathrm{psub}}$ — множество всех таких предикатов, что при любой подстановке в них полиномов получается предикат из $\mathrm{R}^{\#}$.

Через $\mathrm{R}^{\#f}_{\mathrm{psub}}$ обозначим множество всех функций, ограниченных полиномами, графики которых лежат в $\mathrm{R}^{\#}_{\mathrm{psub}}$.

Если $f(\tilde{x})$ — некоторая функция, i — число, то через $\mathrm{Pos}_{f,i}(\tilde{x})$ обозначим i-ю цифру (нумерация с младшего разряда) записи числа $f(\tilde{x})$ в системе счисления с основанием $[\sqrt{\max(\tilde{x},4)}]$.

Функцию $f(\tilde{x})$ будем называть POS-*представимой*, если для любого i имеет место $\mathrm{Pos}_{f,i} \in \mathrm{R}^{\#f}_{\mathrm{Max}}$. Заметим, что POS-представимость функции может, вообще говоря, не сохраняться при введении фиктивных переменных.

Утверждение 1. $\mathrm{R}^{\#} \subseteq \mathrm{S}_*$, $\mathrm{R}^{\#} \subseteq \mathcal{E}^0_*$, $\mathrm{R}^{\#f}_{\mathrm{psub}} \subseteq \mathrm{R}^{\#f}_{\mathrm{Pol}} \subseteq \mathrm{S}$.

Это утверждение легко доказывается на основе стандартной техники, например, из [9].

Утверждение 2. $\mathrm{R}^{\#}$ *замкнут относительно подстановки функций вида $x + a$, где a — константа.*

Доказательство легко провести индукцией по построению формулы на основе того, что любой предикат вида $p(\tilde{x}) = q(\tilde{x})$, где p, q — полиномы, рудиментарен (см. [9]), и на основе тождеств

$$\begin{gathered}(\forall x)_{x<y+a}\varphi(x,y,\tilde{z}) \equiv \varphi(0,y,\tilde{z})\& \dots \&\varphi(a-1,y,\tilde{z}) \;\&\; (\forall x)_{x<y}\varphi(x+a,y,\tilde{z}),\\ ((y+a) = |\{x < x'' + b \mid \varphi(\tilde{x}',x,\tilde{x}''')\}|) \equiv (x'' = 0 \;\&\; \Psi) \vee (\exists z)_{z<x''}\\ (\exists t)_{t<x''}((t+1 = x'')\&(z = |\{x < t \mid \varphi(\tilde{x}',x+b+1,\tilde{x}''')\}|) \;\&\; \Phi),\end{gathered}$$

где Φ и Ψ суть

$$(y + a = z + |\{x \leqslant b \mid \varphi(\tilde{x}',x,\tilde{x}''')\}|), \quad (y + a = |\{x < b \mid \varphi(\tilde{x}',x,\tilde{x}''')\}|)$$

соответственно (Φ и Ψ можно представить с помощью разбора всех возможных комбинаций значений $\varphi(\tilde{x}',x,\tilde{x}''')$, $x \leqslant b$, с использованием только логических операций и подстановки констант). Утверждение 2 доказано.

Утверждение 3. *Класс* $\mathrm{R}^{\#}$ *замкнут относительно подстановки функций вида* $\max(x_1,\dots,x_n)$.

Доказательство. Утверждение следует из того, что имеет место

$$\begin{aligned}\rho(\max(x_1,\dots,x_n),\dots) \equiv (\rho(x_1,\dots) \;\&\; x_1 = \max(x_1,\dots,x_n)) \vee \dots\\ \vee (\rho(x_n,\dots) \;\&\; x_n = \max(x_1,\dots,x_n))\end{aligned}$$

и предикаты вида $(x_i = \max(x_1, \ldots, x_n))$, $1 \leqslant i \leqslant n$, принадлежат классу R. Утверждение 3 доказано.

Из утверждений 2 и 3 вытекает

Утверждение 4. $\mathrm{R}^{\#}$ *замкнут относительно квантификаций вида* $(\forall x)_{x<\max(y_1,\ldots,y_n)+C}$ *и* $(\exists x)_{x<\max(y_1,\ldots,y_n)+C}$, *где* C *— константа.*

Утверждение 5. $\mathrm{R}^{\#f}_{\mathrm{Max}}$ *замкнут относительно суперпозиции. Кроме того,* $\mathrm{R}^{\#}$ *замкнут относительно подстановки функций из* $\mathrm{R}^{\#f}_{\mathrm{Max}}$.

Доказательство. Докажем первую часть. Достаточно рассмотреть случай подстановки функции g в функцию вида $h(\tilde{x}) = f(\tilde{x}, g(\tilde{x}))$, где $f, g \in \mathrm{R}^{\#f}_{\mathrm{Max}}$. Очевидно, что функции $g(\tilde{x})$ и $h(\tilde{x})$ ограничены некоторой функцией вида $\max(\tilde{x}) + C$. Имеем

$$(y = h(\tilde{x})) \equiv (\exists t)_{t\leqslant\max(\tilde{x})+C}(g(\tilde{x}) = t \ \&\ f(\tilde{x}, t) = y).$$

Вторая часть утверждения доказывается аналогично. Утверждение 5 доказано.

Утверждение 6. *Функции* $\mathrm{rm}(x + y, z)$, $\min\left(\left[\frac{x+y}{z}\right], z\right)$, $[\sqrt{x}]$, $x \mathbin{\dot{-}} y$, $x \cdot \mathrm{sg}(y)$, *а также функции вида* $\max(x_1, \ldots, x_n) + C$ *лежат в* $\mathrm{R}^{\#f}_{\mathrm{Max}}$. *Кроме того,* $(x < y) \in \mathrm{R}^{\#}$.

Доказательство. Действительно, рассматриваемый предикат и графики рассматриваемых функций рудиментарны (см., например, [9]) и $\mathrm{R} \subseteq \mathrm{R}^{\#}$. Утверждение 6 доказано.

Утверждение 7. *Пусть функция* $g(x, y, \tilde{z}) \in \mathrm{R}^{\#f}_{\mathrm{Max}}$ *такова, что при любых* $x, y, \tilde{z}$ *имеет место* $g(x, y, \tilde{z}) < [\sqrt{\max(y, 4)}]$. *Кроме того, пусть*

$$f(y, \tilde{z}) = \sum_{x<[\sqrt{\max(y,4)}]} g(x, y, \tilde{z}). \tag{1}$$

Тогда $f \in \mathrm{R}^{\#f}_{\mathrm{Max}}$.

Доказательство. Имеем

$$\begin{aligned} &(a = f(y, \tilde{z})) \\ &\equiv (a = |\{t < \max(y, 4) \mid (\exists p)_{p<M}(\exists q)_{q<M}(t = pM + q \ \&\ q < g(p, y, \tilde{z}))\}|), \end{aligned}$$

где $M = [\sqrt{\max(y, 4)}]$. Из утверждений 5 и 6 следует, что $f \in \mathrm{R}^{\#f}_{\mathrm{Max}}$. Утверждение 7 доказано.

Утверждение 8. *Если* $g(x, y, \tilde{z})$ — POS-*представимая функция, и выполнено* (1), *то* f *тоже* POS-*представима.*

Доказательство. Положим

$$\mathrm{Pos}'_{g,i}(x, y, \tilde{z}, t) = \begin{cases} \min(\mathrm{Pos}_{g,i}(x, y, \tilde{z}), \nu \dot{-} 1) \text{ при } x < \nu, \\ 0 \text{ в противном случае,} \end{cases}$$

где $\nu = [\sqrt{\max(t, 4)}]$.

На основе утверждений 5 и 6 легко показать, что $\mathrm{Pos}'_{g,i} \in \mathrm{R}^{\#f}_{\mathrm{Max}}$ при любом i.

Пусть

$$s_i(y, \tilde{z}, t) = \sum_{x < [\sqrt{\max(t,4)}]} \mathrm{Pos}'_{g,i}(x, y, \tilde{z}, t), \;\; p_i(y, \tilde{z}) = s_i(y, \tilde{z}, \max(y, \tilde{z})).$$

Из утверждения 7 следует, что $s_i \in \mathrm{R}^{\#f}_{\mathrm{Max}}$ при любом i. Кроме того, из утверждений 5 и 6 вытекает $p_i \in \mathrm{R}^{\#f}_{\mathrm{Max}}$.

Заметим, что для любых $i \in \mathbb{N}$, $x < [\sqrt{\max(y, 4)}]$ значение $\mathrm{Pos}_{g,i}(x, y, \tilde{z})$ в системе счисления с основанием $[\sqrt{\max(y, \tilde{z}, 4)}]$ равно i-й цифре числа $g(x, y, \tilde{z})$. На основе этого легко видеть, что $p_i(y, \tilde{z})$ есть сумма по всем $x < [\sqrt{\max(y, 4)}]$ i-х цифр $g(x, y, \tilde{z})$ в системе счисления с основанием $[\sqrt{\max(y, \tilde{z}, 4)}]$.

Сложением «в столбик» легко получить функции $\mathrm{Pos}_{f,i}(y, \tilde{z})$:

$$\begin{aligned} &\mathrm{Pos}_{f,0}(y, \tilde{z}) = \mathrm{rm}(p_0(y, \tilde{z}), L), \;\; h_0(y, \tilde{z}) = [p_0(y, \tilde{z})/L], \\ &\mathrm{Pos}_{f,1}(y, \tilde{z}) = \mathrm{rm}(p_1(y, \tilde{z}) + h_0(y, \tilde{z}), L), \;\; h_1(y, \tilde{z}) \\ &\qquad\qquad = \min([(p_1(y, \tilde{z}) + h_0(y, \tilde{z}))/L], L), \\ &\qquad\qquad \ldots \end{aligned}$$

(минимум тут нужен только для доказательства принадлежности классу $\mathrm{R}^{\#f}_{\mathrm{Max}}$), где $L = [\sqrt{\max(y, \tilde{z}, 4)}]$. Здесь h_i означает число для переноса в следующий разряд. На основе этих формул и утверждений 5, 6 легко видеть, что $\mathrm{Pos}_{f,i}(y, \tilde{z}) \in \mathrm{R}^{\#f}_{\mathrm{Max}}$ при любом i. Утверждение 8 доказано.

Очевидно следующее

Утверждение 9. *Класс* $\mathrm{R}^{\#}_{\mathrm{psub}}$ *замкнут относительно явных преобразований, логических операций, подстановки полиномов и квантификаций вида* $(\forall x)_{x<p(\tilde{y})}$, $(\exists x)_{x<p(\tilde{y})}$, *где* p — *полином.*

Утверждение 10. $\mathrm{R}^{\#f}_{\mathrm{psub}}$ *замкнут относительно суперпозиции. Кроме того,* $\mathrm{R}^{\#}_{\mathrm{psub}}$ *замкнут относительно подстановки функций из* $\mathrm{R}^{\#f}_{\mathrm{psub}}$.

Доказательство. Аналогично доказательству утверждения 5 докажем первую часть, рассмотрев суперпозицию вида $h(\tilde{x}) = f(\tilde{x}, g(\tilde{x}))$. График этой функции после подстановки полиномов будет иметь вид

$$(q(\tilde{y}) = f(p_1(\tilde{y}), \ldots, p_n(\tilde{y}), g(p_1(\tilde{y}), \ldots, p_n(\tilde{y}))))$$
$$\equiv (\exists z)_{z<r(\tilde{y})}(g(p_1(\tilde{y}), \ldots, p_n(\tilde{y})) = z \;\&\; q(\tilde{y}) = f(p_1(\tilde{y}), \ldots, p_n(\tilde{y}), z)),$$

где r — полином, ограничивающий сверху $g(p_1(\tilde{y}), \ldots, p_n(\tilde{y}))$. Далее пользуемся утверждением 9. Вторая часть утверждения доказывается аналогично. Утверждение 10 доказано.

Утверждение 11. *Полиномы, функции* $\max(x_1, \ldots, x_n)$, $\mathrm{sg}(x)$, $[\sqrt{x}]$ *и* $x \dot{-} y$ *принадлежат* $\mathrm{R}^{\#f}_{\mathrm{psub}}$.

Доказательство. Утверждение следует из рудиментарности графиков этих функций и из замкнутости R относительно подстановки полиномов (см. [9]). Утверждение 11 доказано.

Утверждение 12. *Все функции из* $\mathrm{R}^{\#f}_{\mathrm{psub}}$ *являются* POS-*представимыми.*

Доказательство. Пусть $f(\tilde{x}) \in \mathrm{R}^{\#f}_{\mathrm{psub}}$, $L = [\sqrt{\max(\tilde{x}, 4)}]$. Выберем $n > 0$ такое, что $f(\tilde{x}) \leqslant L^n$. При любом $i < n$ имеем

$$(y = \mathrm{Pos}_{f,i}(\tilde{x}))$$
$$\equiv (\exists u_0)_{u_0<L} \ldots (\exists u_{n-1})_{u_{n-1}<L}(f(\tilde{x}) = u_0 + u_1 L + \ldots + u_{n-1} L^{n-1} \;\&\; u_i = y),$$

при $i \geqslant n$ справедливо $(y = \mathrm{Pos}_{f,i}(\tilde{x})) \equiv (y = 0)$. Далее пользуемся утверждениями 10 и 11. Утверждение 12 доказано.

Утверждение 13. *Если* $f(\tilde{x})$ *— ограниченная полиномом* POS-*представимая функция,* $p(\tilde{x})$ *— некоторый полином, то* $(p(\tilde{x}) = f(\tilde{x})) \in \mathrm{R}^{\#}$.

Доказательство. Пусть $L = [\sqrt{\max(\tilde{x}, 4)}]$. Выберем n аналогично тому, как это сделано в доказательстве утверждения 12. Имеем

$$(p(\tilde{x}) = f(\tilde{x})) \equiv (\exists u_0)_{u_0<L} \ldots (\exists u_{n-1})_{u_{n-1}<L}(u_0 = \mathrm{Pos}_{f,0}(\tilde{x}) \& \ldots$$
$$\& \; u_{n-1} = \mathrm{Pos}_{f,n-1}(\tilde{x}) \& p(\tilde{x}) = u_0 + u_1 L + \ldots + u_{n-1} L^{n-1}).$$

Далее пользуемся утверждениями 5, 6, 10 и 11. Утверждение 13 доказано.

Утверждение 14. $\mathrm{R}^{\#f}_{\mathrm{psub}}$ *замкнут относительно ограниченного суммирования.*

Доказательство. Пусть $f(y,z_1,\ldots,z_n) = \sum\limits_{x<y} g(x,y,z_1,\ldots,z_n)$, $g \in \mathrm{R}^{\#f}_{\mathrm{psub}}$. Рассмотрим подстановку полиномов в f:

$$r(\tilde{u}) = f(p(\tilde{u}), q_1(\tilde{u}),\ldots,q_n(\tilde{u})) = \sum_{x<p(\tilde{u})} g(x, p(\tilde{u}), q_1(\tilde{u}),\ldots,q_n(\tilde{u})),$$

$\tilde{u} = (u_1,\ldots,u_m)$. Выберем $k > 0$, $1 \leqslant i_1,\ldots,i_k \leqslant m$, такие, что

$$p(\tilde{u}) < L_1 L_2 \ldots L_k$$

при любом $\tilde{u}$, где $L_j = [\sqrt{\max(u_{i_j},4)}](1 \leqslant j \leqslant k)$. Имеем

$$r(\tilde{u}) = \sum_{v_1<L_1} \ldots \sum_{v_k<L_k} (\mathrm{sg}(p(\tilde{u}) \dot{-} H) \cdot g(H, p(\tilde{u}), q_1(\tilde{u}),\ldots,q_n(\tilde{u}))),$$

где $H = v_1 + v_2L_1 + v_3L_1L_2 + \ldots + v_kL_1\ldots L_{k-1}$. Из утверждений 10 и 11 следует, что функция под знаками суммирования лежит в $\mathrm{R}^{\#f}_{\mathrm{psub}}$. Следовательно, она POS-представимая (утверждение 12). Воспользовавшись k раз утверждением 8, получаем, что $r(\tilde{u})$ POS-представимая. Из утверждения 13 вытекает, что для любого полинома $w(\tilde{u})$ имеет место $(w(\tilde{u}) = r(\tilde{u})) \in \mathrm{R}^{\#}$. Утверждение 14 доказано.

Теорема 4. $\mathrm{R}^{\#} = \mathrm{R}^{\#}_{\mathrm{psub}} = \mathrm{S}_*$, $\mathrm{R}^{\#f}_{\mathrm{Pol}} = \mathrm{R}^{\#f}_{\mathrm{psub}} = \mathrm{S}$.

Доказательство. Результат теоремы следует из утверждений 1, 11, 10, 14 и того, что S есть множество всех функций с графиками из S_*, ограниченных полиномами (см. [9]). Теорема 4 доказана.

Из утверждения 1 и теоремы 4 вытекает

Следствие 1. $\mathrm{S}_* \subseteq \mathcal{E}^0_*$.

В [14] доказана

Теорема 5. $\mathrm{R}^{\#} = \mathrm{R}^{\mathrm{Maj}}$.

Следствие 2. $\mathrm{R}^{\#} = \mathrm{R}^{\mathrm{Maj}} = \mathrm{S}_*$.

4. Машинное описание

Нам потребуется доказанное в [14]

Утверждение 15. *Характеристические функции всех предикатов из* $\mathrm{R}^{\#}$ *лежат в* $\mathrm{LTH}^{\#}$. *Графики всех функций из* $\mathrm{LTH}^{\#}$ *лежат в* $\mathrm{R}^{\#}$.

Теорема 6. $\mathrm{S} = \mathrm{LTH}^{\#}$.

Доказательство. Докажем, что $\mathrm{LTH}^{\#} \subseteq \mathrm{S}$. Пусть $f(\tilde{x}) \in \mathrm{LTH}^{\#}$. Тогда $(y = f(\tilde{x})) \in \mathrm{R}^{\#} = \mathrm{S}_*$. Отсюда и из того, что, очевидно, f ограничена некоторым полиномом, следует, что $f \in \mathrm{S}$ (см. [9]).

Теперь докажем $\mathrm{S} \subseteq \mathrm{LTH}^{\#}$. Пусть $f(\tilde{x}) \in \mathrm{S}$. Тогда $(y = f(\tilde{x})) \in \mathrm{S}_* = \mathrm{R}^{\#}$. Пусть $h(\tilde{x}, y) \in \mathrm{LTH}^{\#}$ — характеристическая функция предиката $(y = f(\tilde{x}))$. Выберем такую константу C, что $\mathrm{len}(f(\tilde{x})) < C \cdot \mathrm{len}(\tilde{x})$. Опишем машину Тьюринга M, обращающуюся к оракулу h, вычисляющую $f(\tilde{x})$ по правилам из определения $\#\mathrm{LinTime}(Q)$.

`Вход:` $\tilde{x}$

`Недетерминированно выбрать` y, z `такие, что` $\mathrm{len}(y) < C \cdot \mathrm{len}(\tilde{x})$ `и` $z < y$`.` *

`Проверить, верно ли, что` $h(\tilde{x}, y) = 1$ `(вызов оракула), если да, успешно завершить работу, в противном случае бесконечный пустой цикл.`

Очевидно, что $f(\tilde{x})$ — количество ветвей вычисления, на которых машина успешно завершает работу. Теорема 6 доказана.

Следствие 3. $\mathrm{R}^{\#} = \mathrm{R}^{\mathrm{Maj}} = \mathrm{LTH}^{\#}_* = \mathrm{S}_*$.

5. Существует ли конечный базис по суперпозиции в классе S?

Иерархию классов будем называть *вырожденной*, если в ней содержится лишь конечное число различных классов.

Теорема 7. *Следующие два утверждения эквивалентны:*
(i) *иерархия* $\{\Sigma_n^{\#\mathrm{lin}}\}$ *вырождена;*
(ii) S *имеет конечный базис по суперпозиции.*

Перед доказательством введём некоторые понятия. Определим $\#\mathrm{LinTime}'(Q)$ аналогично $\#\mathrm{LinTime}(Q)$, заменив в определении требование существования оракула-функции $q \in Q$ требованием существования константы v и набора оракулов-функций $q_1, \ldots, q_k \in Q$, имеющих одинаковое число аргументов; для каждого оракула выделено состояние машины Тьюринга, в котором производится его вызов; при работе машины Тьюринга количество «перемен оракула» (т. е. моментов времени обращения к оракулу, для которых предыдущее обращение происходило к другому оракулу) не должно превосходить v.

Заметим, что для любого множества функций Q, замкнутого относительно добавления и изъятия фиктивных переменных, имеет место

$$\#\mathrm{LinTime}'(\#\mathrm{LinTime}(Q)) \subseteq \#\mathrm{LinTime}(\#\mathrm{LinTime}'(Q)).$$

* z выбирается только для того, чтобы набрать нужное количество ветвей вычисления.

Действительно, пусть $f \in \#\mathrm{LinTime}'(\#\mathrm{LinTime}(Q))$, f вычисляется машиной Тьюринга с оракулами $q_1, \ldots, q_k \in \#\mathrm{LinTime}(Q)$, при этом при работе машины происходит не более v «перемен оракула», каждый из оракулов q_i $(1 \leqslant i \leqslant k)$ вычисляется своей машиной Тьюринга с оракулом $q_i' \in Q$. Применив к функциям $q_1', \ldots, q_k'$ необходимое число раз операцию добавления фиктивных переменных слева, получим функции $q_1'', \ldots, q_k'' \in Q$, имеющие одинаковое число аргументов. Очевидно, что каждая из функций q_i $(1 \leqslant i \leqslant k)$ может быть вычислена машиной Тьюринга с оракулом q_i''. Таким образом, оракулы-функции $q_1, \ldots, q_k$ можно заменить одним оракулом-функцией q, вычисляемым машиной Тьюринга с оракулами $q_1'', \ldots, q_k''$, на вход которой подаётся номер i $(1 \leqslant i \leqslant k)$ нужной функции и вход для неё. Данная машина читает номер i и моделирует машину, вычисляющую q_i. Машину, вычисляющую f, модифицируем соответствующим образом. Линейность времени работы полученной машины следует из того, что при работе исходной машины количество «перемен оракула» ограничено константой v. Аналогично можно показать, что $\#\mathrm{LinTime}'(\#\mathrm{LinTime}) \subseteq \Sigma_2^{\#\mathrm{lin}}$.

Доказательство импликации (ii)⇒(i). Пусть $f_1, \ldots, f_n$ — базис в S. Выберем $m \geqslant 2$ такое, что $f_1, \ldots, f_n \in \Sigma_m^{\#\mathrm{lin}}$. Пусть $F(x_1, \ldots, x_k)$ представляется некоторой формулой над $f_1, \ldots, f_n$. Покажем, что тогда $F(\tilde{x}) \in \Sigma_{m+1}^{\#\mathrm{lin}}$. Заметим, что график F можно представить в виде

$$(y = F(\tilde{x})) \equiv (\exists z_1) \ldots (\exists z_s) \Phi,$$

где Φ есть

$$((z_1 = f_{i_1}(t_{1,1}, \ldots, t_{1,r_1})) \mathbin{\&} \ldots \mathbin{\&} (z_s = f_{i_s}(t_{s,1}, \ldots, t_{s,r_s})) \mathbin{\&} (z_s = y))), \quad (2)$$

при любых i, j $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant r_i)$ $t_{i,j}$ — переменная $(z_p,\ 1 \leqslant p \leqslant s$, или $x_p,\ 1 \leqslant p \leqslant k)$, причём если набор $(z_1, \ldots, z_s)$ существует, то он единственен и существует такая константа C (не зависящая от $\tilde{x}$), что $\mathrm{len}(z_i) < C \cdot \mathrm{len}(\tilde{x})$ $(1 \leqslant i \leqslant s)$.* На основе этого построим недетерминированную машину Тьюринга M с оракулами f_i, $1 \leqslant i \leqslant n$.

`Вход:` $x_1, \ldots, x_n$

`Недетерминированно выбрать` $y, u, z_1, \ldots, z_s$`, удовлетворяющие условию`

$$\mathrm{len}(y), \mathrm{len}(u), \mathrm{len}(z_1), \ldots, \mathrm{len}(z_s) < C \cdot \mathrm{len}(\tilde{x}).^{**}$$

---

*Например, если $F(x_1, x_2, x_3) = f_1(f_2(x_1, x_2), x_3)$, то можно положить $\Phi \equiv (z_1 = f_2(x_1, x_2) \mathbin{\&} z_2 = f_1(z_1, x_3))$.

**u выбирается только для того, чтобы набрать нужное количество ветвей вычисления.

`Вызывая оракулы, проверить (2).`

`Если формула истинна и` $u < y$`, то успешно завершить работу, в противном случае бесконечный пустой цикл.`

Нетрудно заметить, что $F(\tilde{x})$ есть количество ветвей вычисления M с входом $\tilde{x}$, на которых машина успешно завершает работу. Таким образом,

$$F(\tilde{x}) \in \#\mathrm{LinTime}'(\Sigma_m^{\#\mathrm{lin}}) \subseteq \#\mathrm{LinTime}(\#\mathrm{LinTime}'(\Sigma_{m-1}^{\#\mathrm{lin}})) \subseteq \ldots \subseteq \Sigma_{m+1}^{\#\mathrm{lin}}.$$

Импликация (ii)⇒(i) доказана.

Перед тем как доказывать импликацию в другую сторону, введём ещё несколько обозначений.

Ветви вычисления машины Тьюринга будем кодировать числами, имеющими запись $b_1 \ldots b_n$ в некоторой системе счисления с основанием R (зависящим от машины Тьюринга), причём $b_1, \ldots, b_n > 0$ и каждый разряд b_i $(1 \leqslant i \leqslant n)$ содержит информацию о состоянии машины в момент i, перемещении головок в этот момент и о том, какие символы записали головки машины в этот момент времени.

Слова на ленте в алфавите $\{0, 1, *\}$ будем кодировать числами, используя систему счисления с основанием 4 (каждому символу соответствует один ненулевой разряд).

Кроме того, некоторым естественным образом будем кодировать числами недетерминированные машины Тьюринга, работающие линейное время и имеющие возможность обращаться к оракулу; код включает программу, количество лент, тип оракула (количество аргументов соответствующей ему функции*), ограничение на время работы (коэффициенты линейной функции).

Введём следующие предикаты:

$\mathrm{Accept}(x, n, b)$ — машина Тьюринга с кодом n и входом с кодом x имеет ветвь вычисления с кодом b (ответы оракула могут быть произвольными), заканчивающуюся успешным завершением в отведённое время;

$\mathrm{Oracle}^{\mathrm{yes}}(x, n, b, y, z)$ — при подаче входа x у машины с номером n существует ветвь вычисления с кодом b, при данном вычислении во все моменты обращения к оракулу, когда на лентах для оракула были записаны слова с кодами y и z соответственно, оракул выдавал ответ «да»;

*Если оракул является функцией от n переменных, то при обращении к нему на первой ленте должно быть записано слово, являющееся кодом вектора из n чисел, а на второй ленте — двоичная запись числа; в противном случае машина Тьюринга переходит в состояние q_{no}; это важно, потому что мы будем оракулы-функции задавать реализующими их машинами Тьюринга, которые могут и не проверять корректность входа.

$\mathrm{Oracle}^{\mathrm{no}}(x, n, b, y, z)$ — аналогично $\mathrm{Oracle}^{\mathrm{yes}}$, оракул выдаёт «нет»;

$\mathrm{OracleInput}(n, y, z)$ — пара слов с кодами y и z соответственно является корректным входом для обращения к оракулу (если оракул вызывается машиной с кодом n).

Кроме того, введём следующие функции:

$\mathrm{Code}(x)$ — код слова, являющегося двоичной записью x;

$\mathrm{Decode}(x)$ — число, двоичной записью которого является слово с кодом x (0, если такого числа не существует);

$\mathrm{Concat}(x, y)$ — код строки $s_1 * s_2$, где s_1 — строка с кодом x, s_2 — строка с кодом y (0, если либо x, либо y не является кодом строки).

Ясно, что нетрудно выбрать все способы кодирования так, чтобы все введённые функции лежали в S, а предикаты — в S_* (см. [9, 12, 26]).

Доказательство импликации (i)⇒(ii). Пусть иерархия $\Sigma_n^{\#\mathrm{lin}}$ вырождена. Выберем $k \geqslant 2$ такое, что $\mathrm{LTH}^{\#} = \Sigma_k^{\#\mathrm{lin}}$. Введём последовательность функций $f_1, f_2, \ldots$ следующим образом:

$$\begin{aligned}
&f_1(x, n_1, m) = |\{b < m \mid \mathrm{Accept}(x, n_1, b)\}|,\\
&f_i(x, n_1, \ldots, n_i, m) = |\{b < m \mid \mathrm{Accept}(x, n_i, m) \& \ (\forall y)_{y<m} (\forall z)_{z<m}\\
&((\mathrm{Oracle}^{\mathrm{yes}}(x, n_i, b, y, z) \& \Psi) \vee (\mathrm{Oracle}^{\mathrm{no}}(x, n_i, b, y, z) \& \neg\Psi))\}|, \ i \geqslant 2,
\end{aligned}$$

где $\Psi = (\mathrm{OracleInput}(n_i, y, z) \ \& \ \mathrm{Decode}(z) = f_{i-1}(y, n_1, \ldots, n_{i-1}, m))$.

Докажем, что система

$$\{f_k(x, n_1, \ldots, n_k, m), \ \mathrm{Code}(x), \ \mathrm{Concat}(x, y), \ x + 1, \ xy\}$$

полна в S. Пусть $g(x_1, \ldots, x_s) \in \mathrm{S} = \Sigma_k^{\#\mathrm{lin}}$, $g = g_k$ вычисляется недетерминированной машиной Тьюринга M_k с оракулом-функцией $g_{k-1} \in \Sigma_{k-1}^{\#\mathrm{lin}}$ (т. е. значение g_k равно количеству успешных ветвей вычисления), g_{k-1} вычисляется НМТ M_{k-1} с оракулом $g_{k-2} \in \Sigma_{k-2}^{\#\mathrm{lin}}, \ldots, g_2$ вычисляется НМТ M_2 с оракулом g_1, g_1 вычисляется НМТ M_1 без оракула, все машины работают линейное время (от длины входа). Будем полагать, что $n_1, \ldots, n_k$ — номера машин Тьюринга $M_1, \ldots, M_k$ соответственно. Индукцией по i можно показать, что при любом i ($1 \leqslant i \leqslant k$) для любого x, являющегося кодом некоторого слова w, и любого m, превосходящего коды всех ветвей вычислений и слов на лентах, получающихся при запуске M_i на w с оракулом (при $i \geqslant 2$), описанным выше (при обращении к оракулу запускается соответствующая машина Тьюринга; учитываются коды ветвей вычисления и слов на лентах, получающихся при работе всех запускаемых машин $M_1, \ldots, M_i$), результат запуска M_i на w (количество успешных ветвей) есть $f_i(x, n_1, \ldots, n_i, m)$.

С помощью суперпозиции функций xy, $x+1$ построим полином $p(\tilde{x})$, ограничивающий сверху коды всех ветвей вычислений и слов на лентах, получающихся при работе машин $M_1, \ldots, M_k$ в процессе вычисления $g(\tilde{x})$. Пусть $\mathrm{Code}(x_1, \ldots, x_s)$ — код строки $\mathrm{Code}(x_1) * \ldots * \mathrm{Code}(x_s)$. Заметим, что $\mathrm{Code}(x_1, \ldots, x_s)$ представляется в виде суперпозиции функций $\mathrm{Code}(x)$ и $\mathrm{Concat}(x, y)$.

На основе описанного выше свойства для функции f_k легко видеть, что при любых $x_1, \ldots, x_s$ справедливо

$$g(x_1, \ldots, x_s) = f_k(\mathrm{Code}(x_1, \ldots, x_s), n_1, \ldots, n_k, p(\tilde{x})).$$

Теорема 7 доказана.

6. Экспоненциальное расширение класса S и простые конечные базисы по суперпозиции

Пусть $x\langle y\rangle_r$ — y-я цифра числа x в системе счисления с основанием r (нумерация начинается с младшего разряда, имеющего номер 0).

Определим функцию $x \wedge y$ — поразрядную конъюнкцию двоичных представлений чисел x и y. Пусть $a_n a_{n-1} \ldots a_0$, $b_n b_{n-1} \ldots b_0$ — 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

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

Через XS_r ($r \geqslant 2$) обозначим множество всех функций $f(\tilde{x})$, ограниченных сверху функциями вида $2^{p(\tilde{x})}$, где p — полином, для которых имеет место

$$f(\tilde{x})\langle y\rangle_r \in \mathrm{S}.$$

Положим $\mathrm{XS} = \mathrm{XS}_2$. Класс XS будем называть *экспоненциальным расширением* класса S.

Для произвольного класса функций Q индуктивно определим классы $[Q]_{2^x}$ и $[Q]_{x^y}$.

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

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

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

Отметим некоторые свойства класса XS.

Теорема 8. S *есть множество всех функций из* XS, *ограниченных полиномами.*

Доказательство. Очевидно, что $\mathrm{S} \subseteq \mathrm{XS}$. Докажем в обратную сторону. Пусть $f(\tilde{x}) \in \mathrm{XS}$ и $f(\tilde{x})$ ограничена полиномом $p(\tilde{x})$. Тогда имеем

$$f(\tilde{x}) = \sum_{y=0}^{[\log_2 p(\tilde{x})]} \min(2^y, p(\tilde{x})) \cdot f(\tilde{x})\langle y\rangle_2.$$

Из этого следует $f \in \mathrm{S}$. Теорема 8 доказана.

Теорема 9. XS *замкнут относительно ограниченного суммирования вида* $\sum\limits_{x\leqslant y}$ *и ограниченного умножения вида* $\prod\limits_{x\leqslant y}$.

Доказательство. Утверждение теоремы следует из результатов о сложности сложения и умножения произвольного количества чисел (см. [13]), а также из связи этих результатов с классом XS (см. [2]). Теорема 9 доказана.

Теорема 10. *При любом* $r \geqslant 2$ *имеет место* $\mathrm{XS} = \mathrm{XS}_r$.

Доказательство. В самом деле, если $f(\tilde{x}) < 2^{p(\tilde{x})}$ при любом $\tilde{x}$, то при любых $l, k \geqslant 2$ справедливо тождество

$$f(\tilde{x})\langle y\rangle_l = \mathrm{rm}\left(\left[\left(\sum_{i=0}^{p(\tilde{x})} k^i f(\tilde{x})\langle i\rangle_k\right) \Big/ l^y\right], l\right).$$

Остаётся воспользоваться результатами из [13] и [2]. Теорема 10 доказана.

Теперь сформулируем основную теорему о базисе по суперпозиции в классе XS при наложении ограничений на формулы.

Теорема 11. $\mathrm{XS} = [x+1,\ xy,\ x \dot{-} y,\ t[x/y],\ x \wedge y]_{2^x} = [x+1,\ xy,\ x \dot{-} y,$ $[x/y],\ x \wedge y]_{x^y}$.

Доказательство этой теоремы можно найти в [2]. Некоторые обобщения этого результата сформулированы в [1].

ЛИТЕРАТУРА

1. **Волков С. А.** Порождение некоторых классов рекурсивных функций суперпозициями простых арифметических функций // Докл. РАН. — 2007. — Т. 415, № 4. — С. 439–440.
2. **Волков С. А.** Экспоненциальное расширение класса функций, элементарных по Сколему, и ограниченные суперпозиции простых арифметических функций // Мат. вопросы кибернетики. — М.: Физматлит, 2007. — Вып. 16. — С. 163–190.
3. **Косовский Н. К.** Возможности операций одноместного суммирования и одноместного ограниченного умножения // Зап. науч. сем. ЛОМИ им. В. А. Стеклова АН СССР. — 1975. — Т. 49 — С. 3–6.
4. **Марченков С. С.** Об ограниченных рекурсиях // Mathematica Balkanica. — 1972. — Т. 2. — С. 124–142.
5. **Марченков С. С.** О функциях, элементарных по Сколему // Мат. заметки. — 1975. — Т. 17, № 1. — С. 133–141.
6. **Марченков С. С.** Об одном базисе по суперпозиции в классе функций, элементарных по Кальмару // Мат. заметки. — 1980. — Т. 27, № 3. — С. 321–332.
7. **Марченков С. С.** Простые примеры базисов по суперпозиции в классе функций, элементарных по Кальмару // Banach Center Publication. Warsaw. — 1989. — Т. 25. — С. 119–126.
8. **Марченков С. С.** Базисы по суперпозиции в классах рекурсивных функций // Мат. вопросы кибернетики. — М.: Наука, 1991. — Вып. 3. — С. 115–139.
9. **Марченков С. С.** Элементарные рекурсивные функции. — М.: МЦНМО, 2003. — 112 с.
10. **Матиясевич Ю. В.** Существование неэффективизируемых оценок в теории экспоненциально диофантовых уравнений // Зап. науч. сем. ЛОМИ АН СССР. — 1974. — Т. 40. — С. 77–93.
11. **Матиясевич Ю. В.** Новое доказательство теоремы об экспоненциально диофантовом представлении перечислимых предикатов // Зап. науч. сем. ЛОМИ АН СССР. — 1976. — Т. 60. — С. 75–92.
12. **Непомнящий В. А.** Рудиментарное моделирование недетерминированных тьюринговых вычислений // Кибернетика. — 1973. — № 2. — С. 23–29.
13. **Allender E., Barrington D. A. M., Hesse W.** Uniform constant-depth threshold circuits for division and iterated multiplication // J. Comp. System Sci. — 2002. — Vol. 65. — P. 695–716.
14. **Durand A., More M.** Non-erasing, counting and majority over the linear time hierarchy // Information and Computation. — 2002. — Vol. 174, N 2. — P. 132–142.

15. **Esbelin H.-A., More M.** Rudimentary relations and primitive recursion: A toolbox // Theoret. Comp. Sci. — 1998. — Vol. 193. — P. 129–148.
16. **Grzegorczyk A.** Some classes of recursive functions // Rozprawy Mathematyczne. — 1953. — Vol. 4. — P. 1–46. (Русск. пер.: **Гжегорчик А.** Некоторые классы рекурсивных функций // Проблемы математической логики. — М.: Мир, 1970. — С. 9–49.)
17. **Kalmar L.** Egyszerü pelda eldönthetelen aritmetikai problemara // Matematikai es fizikai lapok. — 1943. — Vol. 50. — P. 1–23.
18. **Mazzanti S.** Plain bases for classes of primitive recursive functions // Mathematical Logic Quarterly. — 2002. — Vol. 48. — P. 93–104.
19. **Parsons Ch.** Hierarchies of primitive recursive functions // Zeitschr. math. Logik und Grundlag. Math. — 1968. — Bd 14, Heft 4. — S. 357–376.
20. **Ritchie R. W.** Classes of predicably computable functions // Trans. Amer. Math. Soc. — 1963. — Vol. 106. — P. 139–173. (Русск. пер.: **Ричи Р. В.** Классы предсказуемо вычислимых функций // Проблемы математической логики. — М.: Мир, 1970. — С. 50–93.)
21. **Rödding D.** Über die Eliminierbarkeit von Definitionsschemata in der Theorie der rekursiven Funktionen // Zeitschr. math. Logik und Grundlag. Math. — 1964. — Bd 10, Heft 4. — S. 315–330.
22. **Skolem Th.** A theorem on recursively enumerable sets // Abstract of Short Comm. Int. Congress Math. — Stockholm, 1962. — P. 11.
23. **Skolem Th.** Proof of some theorems on recursively enumerable sets // Notre Dame J. Formal Logic. — 1962. — Vol. 3, N 2. — P. 65–74.
24. **Smullyan R. M.** Theory of Formal Systems. Princeton, 1961. — 156 p. (Русск. пер.: **Смальян Р.** Теория формальных систем. — М.: Наука, 1981. — 207 с.)
25. **Toda S.** On the computational power of PP and $\oplus$P // IEEE Symposium on founations of computer science. — 1989. — P. 514–519.
26. **Wrathall C.** Rudimentary predicates and relative computation // SIAM J. Comp. — Vol. 7, N 2. — 1978. — P. 194–209.

Волков Сергей Александрович

Статья поступила
24 октября 2008 г.