ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2006. Серия 1. Том 13, № 4. 33–48

УДК 519.712

СУПЕРПОЗИЦИИ ЭЛЕМЕНТАРНЫХ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ*)

С. С. Марченков

Найдено новое компактное доказательство теоремы: система функций $\{x+y, x \dot{-} y, \lfloor x/y \rfloor, 2^x\}$ порождает класс функций, элементарных по Кальмару. В доказательстве использован приём устранения оператора ограниченного суммирования.

Введение

Элементарные арифметические функции — константы, сложение, вычитание, умножение, деление, возведение в степень — играют важную роль в любом разделе математики. Как правило, эти функции рассматриваются на множествах комплексных, действительных или рациональных чисел. Однако во многих построениях в теории алгоритмов, комбинаторике и теории чисел необходимо рассматривать варианты этих функций, определенные на множестве N целых неотрицательных чисел. При этом вычитание заменяется функцией $x \dot{-} y$, равной $\max(x-y, 0)$, а деление — функцией $\lfloor x/y \rfloor$, равной целой части от деления x на y.

Возникает естественный вопрос: каковы порождающие возможности системы функций

$$\{1,\ x+y,\ x \dot{-} y,\ xy,\ \lfloor x/y \rfloor,\ x^y\}, \tag{1}$$

рассматриваемых на множестве N? Иными словами, каково множество всех функций, которые можно получить из функций системы (1) с помощью операции суперпозиции?

Довольно давно предполагалось (см. в этой связи [4]), что система (1) порождает класс K функций, элементарных по Кальмару [1, 6, 10, 11, 14]. В подтверждение этой гипотезы в работе [4] (см. также [5]) были указаны некоторые системы функций, близкие к системе (1), которые порождают класс K. Опираясь на результаты работы [4], завершить доказательство

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

этой гипотезы сумел С. Маззанти [13]. К сожалению, полное доказательство гипотезы получается довольно громоздким: помимо результатов работ [4, 13] оно включает также результаты Ю. В. Матиясевича [7, 8], относящиеся к однократным экспоненциально диофантовым представлениям рекурсивно перечислимых множеств.

В этой статье рассматривается менее общая система функций

$$\{x+y,\ x \dot{-} y,\ \lfloor x/y \rfloor,\ 2^x\}, \tag{2}$$

которая обозначается через S. Доказано, что замыкание $[S]$ системы S относительно операции суперпозиции совпадает с классом K. Доказательство этого утверждения довольно компактно, базируется на идее исключения оператора ограниченного суммирования и не использует результатов о диофантовых или экспоненциально диофантовых представлениях рекурсивно перечислимых множеств. Более того, наш подход позволяет получить новое доказательство существования однократных экспоненциально диофантовых представлений рекурсивно перечислимых множеств.

1. Основные понятия

Пусть $N = \{0, 1, 2, \ldots\}$. Все функции и отношения, если не оговаривается иное, рассматриваются на множестве N.

Функцию $\lfloor x/y \rfloor$ — целую часть от деления x на y — полагаем равной x при $y = 0$ (в следующем параграфе увидим, что значения $\lfloor x/0 \rfloor$ можно определять почти произвольно; мы остановились на данном определении по чисто техническим причинам).

Пусть

$$\mathrm{sg}(x) = \begin{cases} 0 \text{ при } x = 0, \\ 1 \text{ при } x \geqslant 1; \end{cases} \qquad \overline{\mathrm{sg}}(x) = \begin{cases} 1 \text{ при } x = 0, \\ 0 \text{ при } x \geqslant 1; \end{cases}$$

$\mathrm{rm}(x,y)$ есть остаток от деления x на y, если $y > 0$, и $\mathrm{rm}(x,0) = x$; $\text{нод}(x,y)$ есть наибольший общий делитель чисел x, y, если $x + y > 0$, и $\text{нод}(0,0) = 0$; $\exp_2 x$ есть показатель числа 2 в разложении x на простые множители, если $x > 0$, и $\exp_2 0 = 0$. Биномиальные коэффициенты $\binom{x}{y}$ будем рассматривать при $x \geqslant y$, полагая $\binom{0}{0} = 0$. Через $\sigma(x)$ обозначаем функцию, равную числу единиц в двоичной записи числа x. Селекторной функцией (или проекцией) называем функцию $I_i^n(x_1, \ldots, x_i, \ldots, x_n)$, равную значениям переменной x_i $(1 \leqslant i \leqslant n,\ n = 1, 2, \ldots)$. Множество всех селекторных функций обозначим через I.

Говорим, что функция f есть («регулярная») суперпозиция функций $g, h_1, \ldots, h_m$, если $f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$. Отметим, что при наличии селекторных функций «нерегулярную» суперпозицию $f(x_1, \ldots, x_n) = g(h_1(x_1^1, \ldots, x_n^1), \ldots, h_m(x_1^m, \ldots, x_n^m))$, где $\{x_1, \ldots, x_n\} = \{x_1^1, \ldots, x_n^1, \ldots, x_1^m, \ldots, x_n^m\}$, можно заменить «регулярной» суперпозицией.

Функция $f(x_1, \ldots, x_n, y)$ получается из функции $g(x_1, \ldots, x_n, z)$ операцией ограниченного суммирования (по переменной z), если

$$f(x_1, \ldots, x_n, y) = \sum_{z \leqslant y} g(x_1, \ldots, x_n, z).$$

Аналогично, функция $f(x_1, \ldots, x_n, y)$ получается из функции $g(x_1, \ldots, x_n, z)$ операцией ограниченного мультиплицирования (по переменной z), если

$$f(x_1, \ldots, x_n, y) = \prod_{z \leqslant y} g(x_1, \ldots, x_n, z).$$

Класс K функций, элементарных по Кальмару, есть наименьший класс функций, которые можно получить из функций

$$x + 1, \quad x \dot{-} y, \quad I \tag{3}$$

с помощью операций суперпозиции, ограниченного суммирования и ограниченного мультиплицирования.

Отметим, что при определении класса $[S]$ к числу исходных функций (2) можно добавить селекторные функции I и рассматривать только «регулярные» суперпозиции, а можно ограничиться системой (2), допуская при этом «нерегулярные» суперпозиции. В целях упрощения изложения мы выбираем второй путь. Те же самые замечания можно сделать и по поводу определения класса K.

Легко доказыватся, что функции системы (2) элементарны по Кальмару. Тем самым получаем, что $[S] \subseteq K$. Кроме того, известно (см., например, [6, утверждение 2.13]), что в определении класса K можно отказаться от операции ограниченного мультиплицирования, добавив к исходным функциям (3) функцию 2^x. Этим определением класса K мы воспользуемся в дальнейшем.

2. Построение в классе $[S]$ простейших функций

Докажем принадлежность классу $[S]$ некоторых простейших функций.

Имеем

$$0 = x \mathbin{\dot{-}} x, \quad 1 = 2^0, \quad \overline{\mathrm{sg}}(x) = 1 \mathbin{\dot{-}} x, \quad \mathrm{sg}(x) = \overline{\mathrm{sg}}(\overline{\mathrm{sg}}(x)),$$
$$|x - y| = (x \mathbin{\dot{-}} y) + (y \mathbin{\dot{-}} x).$$

Убедимся в том, что функция $(x+1)(y+1)$ принадлежит классу $[S]$. Пусть $a(x,y) = \lfloor 2^{x+y+4}/(x+1) \rfloor$, $b(x,y) = \lfloor a(x,y)/(y+1) \rfloor$. Тогда $2^{x+y+4} = b(x,y)(x+1)(y+1) + p(x,y)(x+1) + q(x,y)$, где $0 \leqslant p(x,y) \leqslant y$, $0 \leqslant q(x,y) \leqslant x$. Из неравенств

$$p(x,y)(x+1) + q(x,y) < (x+1)(y+1), \quad 2^{x+y+4} \geqslant (x+1)^2(y+1)^2$$

следует, что $b(x,y) \geqslant (x+1)(y+1)$. Поэтому

$$(x+1)(y+1) = \lfloor 2^{x+y+4}/b(x,y) \rfloor.$$

Теперь образуем функцию xy:

$$xy = (x+1)(y+1) \mathbin{\dot{-}} (x+y+1).$$

Для функции rm имеем соотношение $\mathrm{rm}(x,y) = x \mathbin{\dot{-}} \lfloor x/y \rfloor y$.

Получим функцию x^y. Заметим, что для любых $x, y > 0$

$$2^{xy+x+1} - x > x^y, \ 2^{(xy+x+1)y} = (x + 2^{xy+x+1} - x)^y$$
$$= \sum_{i=0}^{y} \binom{y}{i} x^{y-i} (2^{xy+x+1} - x)^i.$$

Поэтому $x^y = \mathrm{rm}(2^{(xy+x+1)y}, 2^{xy+x+1} \mathbin{\dot{-}} x)$. Отметим, что из последней формулы следует, что $x^0 = 1$ при любом $x \in N$.

Рассмотрим биномиальные коэффициенты $\binom{x}{y}$. Чтобы не вводить ограничение $x \geqslant y$, будем рассматривать биномиальные коэффициенты вида $\binom{x+y}{x}$. При $x + y \geqslant 1$ выполняется неравенство $\binom{x+y}{x} < 2^{x+y}$. Поэтому при любом $w \geqslant 2^{x+y}$ имеем

$$\binom{x+y}{x} = \mathrm{rm}\left(\left\lfloor \frac{(1+w)^{x+y}}{w^x} \right\rfloor, w \right).$$

В частности, $\binom{x+y}{x} = \mathrm{rm}\left(\left\lfloor \frac{(1+2^{x+y})^{x+y}}{2^{x(x+y)}} \right\rfloor, 2^{x+y} \right)$.

В дальнейшем, получая новые функции в классе $[S]$, мы не будем особо заботиться о значениях этих функций при некоторых выделенных значениях переменных. В самом деле, если, например, в классе $[S]$ получены функции $f(x,y), g(y)$ и мы хотим «исправить» значения $f(1,y)$ на значения $g(y)$, в классе $[S]$ достаточно образовать функцию

$$f(x,y)\cdot \mathrm{sg}|x-1| + g(y)\cdot \overline{\mathrm{sg}}|x-1|.$$

3. Построение в классе $[S]$ функций нод, exp_2 и σ

Леммы 1–4 принадлежат С. Маззанти [13].

Лемма 1. *Пусть $a, b > 0$. Тогда* нод(a,b) *равно числу решений уравнения*

$$ax = by, \tag{4}$$

удовлетворяющих неравенствам

$$1 \leqslant x \leqslant b, \quad 1 \leqslant y \leqslant a. \tag{5}$$

Доказательство. В самом деле, уравнение (4) эквивалентно уравнению

$$\frac{ax}{\text{нод}(a,b)} = \frac{by}{\text{нод}(a,b)}, \tag{6}$$

где числа $\dfrac{a}{\text{нод}(a,b)}, \dfrac{b}{\text{нод}(a,b)}$ взаимно просты. Все решения уравнения (6) имеют вид

$$\left(\frac{bt}{\text{нод}(a,b)}, \frac{at}{\text{нод}(a,b)}\right),$$

где $t = 0, \pm 1, \pm 2, \ldots$ Решения уравнения (6), удовлетворяющие неравенствам (5), получаются при $t = 1, 2, \ldots, \text{нод}(a,b)$. Лемма 1 доказана.

Для $a, b > 0$ положим

$$F(a,b) = \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)}.$$

Лемма 2. *При любых $a, b > 0$ справедливо равенство*

$$F(a,b) = \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2} - 1)}{(2^{a^2b} - 1)(2^{ab^2} - 1)2^{a^2b^2}}. \tag{7}$$

Доказательство. Суммируя геометрические прогрессии, получаем

$$\sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)} = \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{a^2bx}\cdot 2^{-ab^2y} = \sum_{x=1}^{b} 2^{a^2bx}\sum_{y=1}^{a} 2^{-ab^2y}$$
$$= \left(\frac{2^{a^2b(b+1)}-2^{a^2b}}{2^{a^2b}-1}\right)\left(\frac{2^{-ab^2}-2^{-ab^2(a+1)}}{1-2^{-ab^2}}\right)$$
$$= \left(\frac{2^{a^2b(b+1)}-2^{a^2b}}{2^{a^2b}-1}\right)\left(\frac{1-2^{-a^2b^2}}{2^{ab^2}-1}\right) = \frac{(2^{a^2b(b+1)}-2^{a^2b})(2^{a^2b^2}-1)}{(2^{a^2b}-1)(2^{ab^2}-1)2^{a^2b^2}}.$$

Лемма 2 доказана.

Лемма 3. *Для любых $a, b > 0$ справедливо равенство*

$$\text{нод}(a,b) = \mathrm{rm}([F(a,b)], 2^{ab}).$$

Доказательство. Положим

$$P(a,b) = \{(x,y) \mid 1 \leqslant x \leqslant b,\ 1 \leqslant y \leqslant a,\ ax-by > 0\},$$

$$N(a,b) = \{(x,y) \mid 1 \leqslant x \leqslant b,\ 1 \leqslant y \leqslant a,\ ax-by < 0\}.$$

Используя лемму 1, получаем

$$F(a,b) = \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)} = \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}(a,b)$$
$$+ \sum_{(x,y)\in N(a,b)} 2^{ab(ax-by)} < \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}(a,b)$$
$$+ \sum_{(x,y)\in N(a,b)} 2^{-ab} < \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}(a,b) + 1.$$

Таким образом,

$$[F(a,b)] = \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}(a,b),$$

откуда непосредственно вытекает утверждение леммы 3. Лемма 3 доказана.

Из формулы (7) видно, что операцию вычитания можно выполнить в пределах множества N, т. е. с помощью функции $\dot{-}$. Применяя теперь лемму 3, получаем нод$\in [S]$.

Лемма 4. *Для любого $a > 0$ справедливо равенство*

$$\exp_2 a = \left\lfloor \frac{\mathrm{rm}(\text{нод}(a, 2^a)^{a+1}, (2^{a+1}-1)^2)}{2^{a+1}-1} \right\rfloor. \tag{8}$$

Доказательство. Очевидно, что нод$(a, 2^a) = 2^{\exp_2 a}$. Далее используя биномиальное разложение, получаем

$$\begin{aligned}
&(2^{\exp_2 a})^{a+1} = \left(2^{a+1}\right)^{\exp_2 a} = \left(1 + 2^{a+1} - 1\right)^{\exp_2 a} \\
&= \sum_{i=0}^{\exp_2 a} \binom{\exp_2 a}{i} (2^{a+1}-1)^i = (2^{a+1}-1)^2 \sum_{i=2}^{\exp_2 a} \binom{\exp_2 a}{i} (2^{a+1}-1)^{i-2} \\
&\qquad\qquad\qquad\qquad\qquad\qquad + (2^{a+1}-1)\exp_2 a + 1,
\end{aligned}$$

откуда справедливость леммы следует при $\exp_2 a \geqslant 1$. При $\exp_2 a = 0$ (в частности, при $a = 0$) формула (8) проверяется непосредственно. Лемма 4 доказана.

Известно [12], что $\sigma(x) = \exp_2\binom{2x}{x}$ при $x > 0$. Поэтому $\sigma \in [S]$.

4. Однократные экспоненциально диофантовы представления отношений

Пусть $\rho(x_1, \ldots, x_n)$ — отношение на множестве N. Представление отношения ρ в виде

$$\begin{aligned}
\rho(x_1, \ldots, x_n) \equiv (\exists z_1) \ldots (\exists z_r)((2^{z_1} = z_2) \& \ldots (2^{z_{2k-1}} = z_{2k}) \\
\&(D(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0)),
\end{aligned} \tag{9}$$

где D — полином с целыми коэффициентами, называем экспоненциально диофантовым представлением (отметим, что это определение отличается от аналогичного определения, традиционно рассматриваемого в литературе [2, 7, 9]). Экспоненциально диофантово представление (9) называем однократным, если для любого набора $(x_1, \ldots, x_n)$, удовлетворяющего отношению ρ, существует ровно один набор $(z_1, \ldots, z_r)$, при котором выполняется (9).

Понятно, что для экспоненциально диофантова представления (9) можно найти такую всюду определённую функцию $w(x_1, \ldots, x_n)$ (вообще говоря, невычислимую), что будет справедлива эквивалентность

$$\rho(x_1, \ldots, x_n) \equiv (\exists z_1)_{z_1 \leqslant w(x_1, \ldots, x_n)} \ldots (\exists z_r)_{z_r \leqslant w(x_1, \ldots, x_n)}((2^{z_1} = z_2)\&$$

$$\ldots\&(2^{z_{2k-1}} = z_{2k})\&(D(x_1,\ldots,x_n,z_1,\ldots,z_r) = 0)). \tag{10}$$

В этом представлении функцию $w(x_1,\ldots,x_n)$ можно, разумеется, заменить любой большей функцией $w'(x_1,\ldots,x_n)$.

В дальнейшем нас будут интересовать монотонные функции $w_l(x_1,\ldots,x_n)$ следующего вида:

$$w_1(x_1,\ldots,x_n) = 2^{x_1+\ldots+x_n}, \quad w_{l+1}(x_1,\ldots,x_n) = 2^{w_l(x_1,\ldots,x_n)}.$$

С использованием функций w_l определим класс отношений R: отношение ρ принадлежит классу R тогда и только тогда, когда ρ имеет однократное экспоненциально диофантово представление (9), в котором переменные $z_1,\ldots,z_r$ можно ограничить некоторой функцией $w_l(x_1,\ldots,x_n)$ (т. е. при $w = w_l$ имеет место представление (10)).

Из определения класса R сразу следует, что R замкнут относительно операции конъюнкции. В самом деле, пусть отношения $\rho_1(x_1,\ldots,x_n)$, $\rho_2(x_1,\ldots,x_n)$ класса R определяются формулами (в целях упрощения формул часть переменных опускаем)

$$(\exists z_1)_{z_1\leqslant w_l}\ldots(\exists z_r)_{z_r\leqslant w_l}((2^{z_1} = z_2)\&\ldots\&(2^{z_{2k-1}} = z_{2k})\&(D_1 = 0)),$$
$$(\exists v_1)_{v_1\leqslant w_l}\ldots(\exists v_p)_{v_p\leqslant w_l}((2^{v_1} = v_2)\&\ldots\&(2^{v_{2m-1}} = v_{2m})\&(D_2 = 0)),$$

где $\{z_1,\ldots,z_r\}\cap\{v_1\ldots,v_p\} = \varnothing$. Тогда отношение

$$\rho_1(x_1,\ldots,x_n)\&\rho_2(x_1,\ldots,x_n)$$

имеет однократное экспоненциально диофантово представление, причём

$$\rho_1\&\rho_2 \equiv (\exists z_1)_{z_1\leqslant w_l}\ldots(\exists z_r)_{z_r\leqslant w_l}(\exists v_1)_{v_1\leqslant w_l}\ldots(\exists v_p)_{v_p\leqslant w_l}\&((2^{z_1} = z_2)\&$$
$$\ldots\&(2^{z_{2k-1}} = z_{2k})\&(2^{v_1} = v_2)\&\ldots\&(2^{v_{2m-1}} = v_{2m})\&(D_1^2 + D_2^2 = 0)).$$

(Нетрудно понять, что установленный факт будет верным и в том случае, когда отношения ρ_1,ρ_2 зависят от различных переменных.)

Лемма 5. *Пусть*

$$f(x_1,\ldots,x_n) = g(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n)),$$

отношения

$$y = g(y_1,\ldots,y_m),\ y = h_1(x_1,\ldots,x_n),\ldots,y = h_m(x_1,\ldots,x_n)$$

принадлежат классу R и каждая из функций $g,h_1,\ldots,h_m$ ограничена сверху некоторой функцией типа w_l. Тогда отношение $y = f(x_1,\ldots,x_n)$

принадлежит классу R.

Доказательство. Будем считать, что каждая функция $h_1, \dots, h_m$ ограничена сверху одной и той же функцией w_i. Тогда имеет место эквивалентность

$$(y = f(x_1, \dots, x_n)) \equiv (\exists y_1)_{y_1 \leqslant w_i(x_1,\dots,x_n)} \dots (\exists y_m)_{y_m \leqslant w_i(x_1,\dots,x_n)}$$
$$((y_1 = h_1(x_1, \dots, x_n))\& \dots \&(y_m = h_m(x_1, \dots, x_n))\&(y = g(y_1, \dots, y_m))).$$

Понятно, что в этой эквивалентности функцию w_i можно заменить любой большей функцией w_j. Далее пользуемся замкнутостью класса R относительно операции конъюнкции, ограничениями для функций $g, h_1, \dots, h_m$ функциями типа w_l и тем, что суперпозиции функций типа w_l мажорируются функцими того же типа. Лемма 5 доказана.

Теорема 1. *Если $f \in [S]$, то отношение $y = f$ принадлежит классу R.*

Доказательство. Проведём индукцию по построению функций в классе $[S]$. Рассмотрим функции множества S. Имеем

$$(y = x_1 + x_2) \equiv (y - x_1 - x_2 = 0), \quad (y = 2^x) \equiv (y - 2^x = 0).$$

Последнюю формулу легко привести к стандартному виду (10) введением новых переменных z_1, z_2:

$$(y = 2^x) \equiv (\exists z_1)_{z_1 \leqslant w_1(x)}(\exists z_2)_{z_2 \leqslant w_1(x)}((2^{z_1} = z_2)\&((x - z_1)^2 + (y - z_2)^2 = 0)).$$

В дальнейшем подобные очевидные преобразования мы опускаем.

Для функции $\lfloor x_1/x_2 \rfloor$ нужное представление получим в несколько этапов. Сначала рассмотрим функцию $\lfloor x_1/(x_2+1) \rfloor$:

$$(y = \lfloor x_1/(x_2+1) \rfloor) \equiv ((x_2+1)y \leqslant x_1)\&((x_2+1)(y+1) > x_1) \equiv$$
$$(\exists z_1)_{z_1 \leqslant w_1(x_1,x_2)}(\exists z_2)_{z_2 \leqslant w_1(x_1,x_2)}((x_2+1)y + z_1 = x_1)$$
$$\&((x_2+1)(y+1) = x_1 + z_2 + 1)).$$

Далее получим представление для функции $(x \dot{-} 1)$:

$$(y = x \dot{-} 1) \equiv (2^y = \lfloor (2^x+1)/2 \rfloor) \equiv$$

$$(\exists z_1)_{z_1 \leqslant w_1(x)}(\exists z_2)_{z_2 \leqslant w_1(x)}((2^y = z_1)\&(2^x = z_2)\&(z_1 = \lfloor (z_2+1)/2 \rfloor)).$$

Теперь имеем $\lfloor x_1/x_2 \rfloor \equiv \lfloor x_1/((x_2 \dot{-} 1)+1) \rfloor$ (напомним, что $\lfloor x/0 \rfloor = x$).

Перед функцией $x_1 \dot{-} x_2$ рассмотрим еще одну вспомогательную функцию $\lfloor \log_2(x+1) \rfloor$:

$$(y = \lfloor \log_2(x+1) \rfloor) \equiv ((2^y \leqslant x+1) \& (2^{y+1} > x+1)).$$

Заметим, что

$$\lfloor \log_2((x \dot{-} 1)+1) \rfloor = \begin{cases} \lfloor \log_2 x \rfloor & \text{при } x \geqslant 1, \\ 0 & \text{при } x = 0. \end{cases}$$

Поэтому

$$(y = x_1 \dot{-} x_2) \equiv (y = \lfloor \log_2((\lfloor 2^{x_1}/2^{x_2} \rfloor \dot{-} 1)+1) \rfloor).$$

Доказательство теоремы 1 завершаем обращением к лемме 5.

5. Суммирование экспоненциально полиномиальных выражений

Следующая лемма является некоторым вариантом леммы 3.1 из [8].

Лемма 6. *Пусть числа $v_0, \dots, v_s, w$ удовлетворяют неравенствам*

$$0 \leqslant v_0, \dots, v_s < 2^w \tag{11}$$

и q — число нулей в последовательности $v_0, \dots, v_s$. Тогда

$$\sigma(\sum_{i \leqslant s} (2^{2w} - 2^w v_i + v_i - 1) 2^{2wi}) = w(s+1+q). \tag{12}$$

Доказательство. Из неравенств (11) вытекает, что при любом $i \leqslant s$

$$0 \leqslant 2^{2w} - 2^w v_i + v_i - 1 < 2^{2w}.$$

Поэтому в выражении

$$\sum_{i \leqslant s} (2^{2w} - 2^w v_i + v_i - 1) 2^{2wi}$$

числа

$$2^{2w} - 2^w v_i + v_i - 1$$

можно рассматривать как «цифры» в позиционной системе счисления с основанием 2^{2w}. Отсюда следует, что

$$\sigma\left(\sum_{i \leqslant s} (2^{2w} - 2^w v_i + v_i - 1) 2^{2wi}\right) = \sum_{i \leqslant s} \sigma(2^{2w} - 2^w v_i + v_i - 1).$$

Если $v_i = 0$, то, очевидно,

$$\sigma(2^{2w} - 2^w v_i + v_i - 1) = 2w.$$

В противном случае

$$\sigma(2^{2w} - 2^w v_i + v_i - 1) = \sigma(2^w - v_i) + \sigma(v_i - 1) = w,$$

поскольку двоичное представление числа $2^w - v_i$ получается из двоичного представления числа v_i сохранением младших двоичных разрядов вплоть до первого единичного разряда и инвертированием остальных двоичных разрядов, а двоичное представление числа $(v_i - 1)$ — из двоичного представления v_i инвертированием младших разрядов вплоть до первого единичного разряда и сохранением остальных двоичных разрядов. Отсюда вытекает доказываемое равенство (12). Лемма 6 доказана.

Вариант леммы 7 доказан в [4].

Лемма 7. *Пусть $D(x_1, \ldots, x_n, z_1, \ldots, z_r)$ — полином с целыми коэффициентами и $d(x_1, \ldots, x_n, t)$ — число наборов $(z_1, \ldots, z_r)$, принадлежащих кубу*

$$0 \leqslant z_1, \ldots, z_r \leqslant t \tag{13}$$

и удовлетворяющих отношению

$$(2^{z_1} = z_2) \& \ldots \& (2^{z_{2k-1}} = z_{2k}) \& (D(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0).$$

Тогда функция d принадлежит классу $[S]$.

Доказательство. Положим

$$E(x_1, \ldots, x_n, z_1, \ldots, z_r) \\ = (2^{z_1} - z_2)^2 + \ldots + (2^{z_{2k-1}} - z_{2k})^2 + D^2(x_1, \ldots, x_n, z_1, \ldots, z_r).$$

Функция E неотрицательна и, очевидно, $d(x_1, \ldots, x_n, t)$ равно числу решений уравнения

$$E(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0,$$

лежащих в кубе (13). Мы хотим применить лемму 6 к последовательности значений функции E, принимаемых ею в кубе (13). С этой целью положим (см. сумму в левой части равенства (12))

$$F(x_1, \ldots, x_n, t, w) = \sum_{0 \leqslant z_1, \ldots, z_r \leqslant t} (2^{2w} - 1 - (2^w - 1)E(x_1, \ldots, x_n, z_1, \ldots, z_r)) \times$$

$$2^{2w(z_1(t+1)^{r-1}+z_2(t+1)^{r-2}+\ldots+z_{r-1}(t+1)+z_r)}). \qquad (14)$$

Если выбрать величину w так, чтобы в кубе (13) выполнялось неравенство

$$E(x_1,\ldots,x_n,z_1,\ldots,z_r) < 2^w, \qquad (15)$$

то на основании леммы 6 будем иметь

$$\sigma(F(x_1,\ldots,x_n,t,w)) = w((t+1)^r+1+d(x_1,\ldots,x_n,t)),$$

т. е. $d(x_1,\ldots,x_n,t) = \left\lfloor \frac{\sigma(F(x_1,\ldots,x_n,t,w))}{w} \right\rfloor \dot{-} ((t+1)^r+1)$.

Поскольку переменные $z_1,\ldots,z_r$ удовлетворяют неравенствам (13), для выполнения неравенства (15) значение w можно выбрать как функцию (от переменных $x_1,\ldots,x_n,t$), принадлежащую классу $[S]$. Следовательно, чтобы завершить доказательство леммы, достаточно показать, что функция F принадлежит классу $[S]$.

Учитывая структуру функции E, сумму из правой части равенства (14) можно представить как конечную линейную комбинацию (с коэффициентами — полиномами от переменных $x_1,\ldots,x_n$) сумм вида

$$\sum_{z_1\leqslant t}\cdots\sum_{z_r\leqslant t} z_1^{i_1}\ldots z_r^{i_r}2^{z_1p_1(t,w)+\ldots+z_rp_r(t,w)}, \qquad (16)$$

где $i_1,\ldots,i_r$ — натуральные числа, а $p_1,\ldots,p_r$ — полиномы с натуральными коэффициентами. Сумму (16) можно переписать в виде

$$\prod_{k=1}^{r}\sum_{z_k\leqslant t} z_k^{i_k}2^{z_kp_k(t,w)}. \qquad (17)$$

Для сумм вида $\sum\limits_{z\leqslant t} z^iq^z$ в комбинаторике хорошо известны формулы типа

$$\frac{Q_i(q,q^t,t)}{(q-1)^{i+1}},$$

где Q_i — полином с целыми коэффициентами. Таким образом, сумма (16), равная (17), также будет представима в виде произведения выражений типа

$$\frac{Q_{i_k}(2^{p_k(t,w)},2^{tp_k(t,w)},t)}{(2^{p_k(t,w)}-1)^{i_k+1}}.$$

Остаётся заметить, что во всех приведённых выше формулах вычитание можно выполнить в пределах множества N, т. е. с помощью функции

$\dot{-}$. Лемма 7 доказана.

Теорема 2. *Пусть функция* $f(x_1,\dots,x_n)$ *удовлетворяет условию*

$$\max_{i_1\leqslant x_1,\dots,i_n\leqslant x_n} f(i_1,\dots,i_n)\leqslant w_l(x_1,\dots,x_n), \tag{18}$$

отношение $y=f(x_1,\dots,x_n)$ *принадлежит классу* R, *выразимо формулой* (10) *и* $g(x_1,\dots,x_n)=\sum\limits_{i\leqslant x_n} f(x_1,\dots,x_{n-1},i)$. *Тогда* $g\in[S]$.

Доказательство. В самом деле, учитывая неравенство (18), заключаем, что величина $g(x_1,\dots,x_n)$ равна числу троек (i,j,y), принадлежащих кубу

$$0\leqslant i,j,y\leqslant w_l(x_1,\dots,x_n)$$

и удовлетворяющих отношению

$$(i\leqslant x_n)\&(y=f(x_1,\dots,x_{n-1},i))\&(j<y).$$

Очевидно, что $g(x_1,\dots,x_n)$ равна числу пятерок (i,i_1,j,j_1,y) из куба $0\leqslant i,i_1,j,j_1,y\leqslant w_l(x_1,\dots,x_n)$, которые удовлетворяют отношению

$$(i+i_1=x_n)\&(y=f(x_1,\dots,x_{n-1},i))\&(j+j_1+1=y). \tag{19}$$

Пользуясь далее принадлежностью отношения $y=f(x_1,\dots,x_{n-1},i)$ классу R, получаем его однократное экспоненциально диофантово представление:

$$\begin{multline}(y=f(x_1,\dots,x_{n-1},i))\equiv(\exists z_1)\dots(\exists z_r)((2^{z_1}=z_2)\&\dots\&(2^{z_{2k-1}}=z_{2k})\\ \&(D(x_1,\dots,x_{n-1},i,y,z_1,\dots,z_r)=0)). \tag{20}\end{multline}$$

Будем предполагать, что число l с самого начала выбрано так, что при $i\leqslant x_n$ в представлении (20) переменные $z_1,\dots,z_r$ можно ограничить функцией $w_l(x_1,\dots,x_n)$ (ввиду соотношения (18) функцию w_l считаем зависящей только от переменных $x_1,\dots,x_n$). Тогда из (19), (20) следует, что $g(x_1,\dots,x_n)$ есть число решений системы уравнений

$$\begin{multline}(2^{z_1}=z_2)\&\dots\&(2^{z_{2k-1}}=z_{2k})\&((x_n-i-i_1)^2+(y-j-j_1-1)^2\\ +D^2(x_1,\dots,x_{n-1},i,y,z_1,\dots,z_r)=0),\end{multline}$$

заключенных в кубе

$$0\leqslant i,i_1,j,j_1,y,z_1,\dots,z_r\leqslant w_l(x_1,\dots,x_n).$$

Теперь применяем лемму 7. Теорема 2 доказана.

Следствие 1. *Справедливо равенство* $[S] = K$.

Доказательство. Из теорем 1, 2 следует, что класс $[S]$ замкнут относительно операции ограниченного суммирования. Однако, как отмечалось в разделе 1, замыкание системы S относительно операций суперпозиции и ограниченного суммирования совпадает с классом K. Следствие 1 доказано.

Следствие 2. *Система функций*

$$\{x + y,\ x^2,\ \mathrm{rm}(x, y),\ 2^x\} \tag{21}$$

порождает класс K.

Доказательство. Достаточно установить, что суперпозициями функций системы (21) можно получить функции $x \dot{-} y$ и $\lfloor x/y \rfloor$.

Имеем

$$0 = \mathrm{rm}(x, x),\ 1 = 2^0,\ \overline{\mathrm{sg}}(x) = \mathrm{rm}(2^x, 2),\ x \cdot \overline{\mathrm{sg}}(y) = \mathrm{rm}(x, \mathrm{sg}(y))$$

(напомним, что $\mathrm{rm}(x, 0) = x$).

Положим $f(x, y) = \mathrm{rm}(2^{x+y} + x, 2^{x+y} + y)$. Тогда

$$f(x, y) = \begin{cases} x - y, & \text{если } x \geqslant y, \\ 2^{x+y} + x & \text{в противном случае.} \end{cases}$$

Поскольку

$$\mathrm{rm}(2^x, 2^y) = \begin{cases} 0 \text{ при } x \geqslant y, \\ 2^x \quad \text{в противном случае,} \end{cases}$$

получаем $x \dot{-} y = \mathrm{rm}(f(x, y), \mathrm{sg}(\mathrm{rm}(2^x, 2^y)))$. Далее имеем

$$2xy = ((x + y)^2 \dot{-} x^2) \dot{-} y^2.$$

При $y > 0$ справедливо равенство

$$\lfloor x/y \rfloor = \mathrm{rm}(2(x + 1)(x \dot{-} \mathrm{rm}(x, y)), 2(x + 1)y \dot{-} 1).$$

Согласно определению функция $\lfloor x/y \rfloor$ должна быть равна x при $y = 0$. Поэтому полученную функцию $\lfloor x/y \rfloor$ следует сложить с функцией $x \cdot \overline{\mathrm{sg}}(y)$. Следствие 2 доказано.

Говорят, что множество $M \subseteq N$ имеет однократное экспоненциально диофантово представление, если подобное представление имеется для отношения $x \in M$.

Следствие 3. *Любое рекурсивно перечислимое множество имеет однократное экспоненциально диофантово представление.*

Доказательство. Пусть M — рекурсивно перечислимое множество, $|M| > 2$ (в остальных случаях искомое представление для отношения $x \in M$ определяется очевидным образом), a_1, a_2 — неравные элементы из M. Выберем машину Тьюринга $\mathcal{M}$, областью определения которой является множество M. Используя, например, технику работы [14], определим в классе K такие функции $f_1(z), f_2(z)$, что $f_i(z) = x$, если z есть код завершающегося вычисления на машине $\mathcal{M}$, которое отвечает входу x, и $f_i(z) = a_i$ в противном случае. Тогда

$$(x \in M) \equiv (\exists z)((x = f_1(z))\&(x = f_2(z))).$$

Отсюда следует существование однократного экспоненциально диофантова представления для отношения $x \in M$.

ЛИТЕРАТУРА

1. **Косовский Н. К.** Основы теории элементарных алгоритмов. Л.: Изд-во Ленинградского ун-та, 1987.
2. **Мальцев А. И.** Алгоритмы и рекурсивные функции. М.: Наука, 1986.
3. **Марченков С. С.** Об одном базисе по суперпозиции в классе функций, элементарных по Кальмару // Матем. заметки. 1980. Т. 27, вып. 3. С. 321–332.
4. **Марченков С. С.** Простые примеры базисов по суперпозиции в классе функций, элементарных по Кальмару // Combinatorics and Graph Theory. Banach Center Publications. 1989. V. 25. P. 119–126.
5. **Марченков С. С.** Базисы по суперпозиции в классах рекурсивных функций // Математические вопросы кибернетики. Вып. 3. М.: Наука, 1991. С. 115–139.
6. **Марченков С. С.** Элементарные рекурсивные функции. М.: МЦНМО, 2003.
7. **Матиясевич Ю. В.** Новое доказательство теоремы об экспоненциально диофантовом представлении перечислимых предикатов // Записки научных семинаров Ленинград. отделения матем. ин-та АН СССР. 1976. Т. 60. С. 75–92.
8. **Матиясевич Ю. В.** Один класс критериев простоты, формулируемых в терминах делимости биномиальных коэффициентов // Записки научных семинаров Ленинград. отделения матем. ин-та АН СССР. 1977. Т. 67. С. 167–183.
9. **Davis M., Putnam H., Robinson J.** The decision problem for exponential Diophantine equations // Ann. Math. 1961. V. 74. P. 425–436.

10. **Grzegorczyk A.** Some classes of recursive functions // Rozprawy Matemematiczne. 1953. V. 4. (Русск. пер.: **Гжегорчик А.** Некоторые классы рекурсивных функций // Проблемы математической логики. М.: Мир, 1970. С. 9–49.)

11. **Kalmar L.** Ein einfach Beispiel für unentscheibares Problem // Matematikai és fizikai lapok. 1943. B. 50. S. 1–23.

12. **Kummer E.** Über die Ergänzugssätze zu den allgemeinen Reciprocitätsgesetzen // J. Reine Angew. Math. 1852. B. 44. S. 93–146.

13. **Mazzanti S.** Plain bases for classes of primitive recursive functions // Math. Logic Quarterly. 2002. V. 48, N 1. P. 93–104.

14. **Ritchie R. W.** Classes of predictably computable functions // Trans. Amer. Math. Soc. 1963. V. 106. P. 139–173. (Русск. пер.: **Ричи Р. В.** Классы предсказуемо вычислимых функций // Проблемы математической логики. М.: Мир, 1970. С.50–93.)

Адрес автора:

Московский гос. ун-т им. М. В. Ломоносова,
Воробьевы горы, 2-й учебный корпус,
119992, Москва, Россия.
E-mail: mathcyb@cs.msu.su

Статья поступила
18 апреля 2006 г.