COMBINATORICS AND GRAPH THEORY
BANACH CENTER PUBLICATIONS, VOLUME 25
PWN-POLISH SCIENTIFIC PUBLISHERS
WARSAW 1989

ПРОСТЫЕ ПРИМЕРЫ БАЗИСОВ ПО СУПЕРПОЗИЦИИ В КЛАССЕ ФУНКЦИЙ, ЭЛЕМЕНТАРНЫХ ПО КАЛЬМАРУ

С. С. МАРЧЕНКОВ

Институт прикладной математики АН СССР, Москва, СССР

Вопрос о существовании конечных базисов по суперпозиции в классе K функций, элементарных по Кальмару, был поставлен А. Гжегорчиком [1]. Положительный ответ на него получил Д. Рёддинг [10]. Несколько позднее Ч. Парсонс [8] более простыми средствами построил систему из 19 функций, образующую базис по суперпозиции в классе K. В определение большинства функций этого базиса явно входят операции ограниченного суммирования и ограниченного умножения. В работе [4] было доказано, что базис по суперпозиции в классе K образуют функции $\{x+1, x^y, [x/y], \varphi(x, y)\}$, где $\varphi(x, y)$ при $x > 1$ равно наименьшему номеру нулевого разряда в представлении y в позиционной системе с основанием x. Там же было установлено, что суперпозициями функций $\{x+1, x^y, x \dot{-} y, [x/y]\}$ можно заведомо реализовать все функции из K, принимающие конечное число значений. В работе Дж. Джонса и Ю. В. Матиясевича [2] указано еще пять систем функций, обладающих этим свойством. Приведем одну из них:

$$\{x+y,\ x \dot{-} y,\ [x/y],\ \sigma(x),\ 2^x\}. \tag{1}$$

Здесь $\sigma(x)$ равно числу единиц в двоичном представлении x. Ниже мы доказываем, что базис по суперпозиции в классе K образует система

$$S_1 = \{x \dot{-} 1,\ [x/y],\ 2^{x+y},\ \sigma(x)\}.$$

Тем самым базисом в классе K оказывается и система (1). Кроме того, мы приводим еще один простой пример базиса по суперпозиции в классе K — систему

$$S_2 = \{x+1,\ [x/y],\ x^y,\ \tau(x)\},$$

где $\tau(x)$ равно показателю числа 2 в разложении x на простые множители, если $x > 0$, и $\tau(0) = 0$.

В дальнейшем нам удобно считать, что $[x/0]=0$. Пусть $[S_1]$ обозначает класс всех функций, полученных суперпозициями функций системы S_1.

Лемма 1. *Функции* 1, $x+y$, $x \dot{-} y$, xy *принадлежат классу* $[S_1]$.

Доказательство. Имеем

$$1=[2^{2x}/2^{2x}], \quad x+y=\sigma(2^{x+y} \dot{-} 1), \quad 0=1 \dot{-} 1,$$
$$2^x=2^{x+0}, \quad x \dot{-} y=\sigma([2^x/2^y] \dot{-} 1).$$

Пусть $x>0$, $y>0$,

$$a(x, y)=[2^{x+y+1}/x], \tag{2}$$

$$b(x, y)=[a(x, y)/y]. \tag{3}$$

Тогда

$$2^{x+y+1}=b(x, y)xy+p(x, y)x+q(x, y),$$

где $0 \leqslant p(x, y)<y$, $0 \leqslant q(x, y)<x$. Так как $p(x, y)x+q(x, y)<xy$ и $2^{x+y+1}>xy(xy+1)$, то при $x>0$, $y>0$ будет также $b(x, y)>xy$. Следовательно, в этом случае

$$xy=[2^{x+y+1}/b(x, y)]. \tag{4}$$

Равенство (4) будет справедливым и при $xy=0$, если воспользоваться соглашением $[x/0]=0$. Лемма доказана.

Следующее утверждение представляет собой некоторый вариант леммы 3.1 из работы [5].

Лемма 2. *Пусть целые неотрицательные (не обязательно различные) числа* $v_0, v_1, \ldots, v_s$ *удовлетворяют неравенствам*

$$v_0, v_1, \ldots, v_s<2^l, \tag{5}$$

где l — *целое неотрицательное число. Тогда если последовательность* $v_0, v_1, \ldots, v_s$ *содержит ровно* q *нулей,* h — *натуральное число,*

$$V=\sum_{i=0}^{s}(2^{h+l}-v_i)2^{(h+l+1)i}$$

и

$$l(s+1-q)+q<h, \tag{6}$$

то $q=s+1-[\sigma(V)/h]$.

Доказательство. Из неравенства (5) и определения V вытекает, что

$$\sigma(V)=\sum_{i=0}^{s}\sigma(2^{h+l}-v_i).$$

При $v_i = 0$ имеем, очевидно, $\sigma(2^{h+l}-v_i) = 1$, а при $v_i > 0$ — $h < \sigma(2^{h+l}-v_i) \leqslant h+l$. Поэтому

$$h(s+1-q)+q \leqslant \sigma(V) \leqslant (h+l)(s+1-q)+q.$$

Следовательно, ввиду неравенства (6) получаем $[\sigma(V)/h] = s+1-q$. Лемма доказана.

Пусть $P(x_1, \ldots, x_m)$, $Q(x_1, \ldots, x_m, y_1, \ldots, y_n)$ — числовые предикаты. Говорим, что формула

$$(\exists y_1)\ldots(\exists y_n)\ Q(x_1, \ldots, x_m, y_1, \ldots, y_n) \tag{7}$$

однократно представляет предикат $P(x_1, \ldots, x_m)$, если

$$P(x_1, \ldots, x_m) \equiv (\exists y_1)\ldots(\exists y_n)\ Q(x_1, \ldots, x_m, y_1, \ldots, y_n),$$

причем для любого набора $(x_1, \ldots, x_m)$ в случае истинности (7) существует единственный набор $(y_1, \ldots, y_n)$, для которого истинно значение $Q(x_1, \ldots, x_m, y_1, \ldots, y_n)$.

Пусть предикат P однократно представим формулой (7) и в классе K существуют такие функции $C_1(x_1, \ldots, x_m), \ldots, C_n(x_1, \ldots, x_m)$ что

$$P(x_1, \ldots, x_m) \equiv (\exists y_1)_{y_1 \leqslant C_1(x_1,\ldots,x_m)} \ldots \\ \ldots (\exists y_n)_{y_n \leqslant C_n(x_1,\ldots,x_m)}\ Q(x_1, \ldots, x_m, y_1, \ldots, y_n). \tag{8}$$

Тогда будем говорить, что однократное представление (7) предиката P *ограничено* в классе K. Формулу из правой части эквивалентности (8) в этом и только в этом случае также будем называть однократным представлением предиката P. Если предикат P однократно представим формулой (7) и выполняется эквивалентность (8), то, очевидно, вместо фигурирующих в ней функций $C_1, \ldots, C_n$ можно взять любые бо́льшие функции (например, из класса K).

Лемма 3. *Пусть $f(x_1, \ldots, x_m)$ — всюду определенная функция, а формула*

$$(\exists y_1)\ldots(\exists y_n)\ (y_1 = 2^{y_2}\ \&\ D(x_1, \ldots, x_m, y_0, y_1, \ldots, y_n) = 0), \tag{9}$$

где D — многочлен с целыми коэффициентами, задает однократное представление предиката $y_0 < f(x_1, \ldots, x_m)$, ограниченное в классе K. Тогда $f \in [S_1]$.

Доказательство. Пусть $C_1(x_1, \ldots, x_m, y_0), \ldots, C_n(x_1, \ldots, x_m, y_0)$ — такие функции из класса K, что справедлива эквивалентность

$$(y_0 < f(x_1, \ldots, x_m)) \equiv (\exists y_1)_{y_1 \leqslant C_1(x_1,\ldots,x_m,y_0)} \ldots \\ \ldots (\exists y_n)_{y_n \leqslant C_n(x_1,\ldots,x_m,y_0)} (y_1 = 2^{y_2} \\ \&\ D(x_1, \ldots, x_m, y_0, y_1, \ldots, y_n) = 0). \tag{10}$$

Суперпозициями функции 2^{x+y} можно определить в классе $[S_1]$ такую функцию $C(x_1, \ldots, x_m)$, что она мажорирует любую из функций

$$f(x_1, \ldots, x_m), \qquad \max_{0 \leqslant y_0 \leqslant f(x_1, \ldots, x_m)} C_i(x_1, \ldots, x_m, y_0) \quad (i = 1, \ldots, n).$$

Тогда из эквивалентности (10) и замечания перед леммой 3 следует, что для любого набора $(a_1, \ldots, a_m)$ предикат

$$y_1 = 2^{y_2} \mathbin{\&} D(a_1, \ldots, a_m, y_0, y_1, \ldots, y_n) = 0$$

истинен ровно в $f(a_1, \ldots, a_m)$ точках куба

$$\{(y_0, y_1, \ldots, y_n)\colon 0 \leqslant y_0, y_1, \ldots, y_n \leqslant C(a_1, \ldots, a_m)\}. \tag{11}$$

Эти точки отвечают значениям y_0 из отрезка $(0, 1, \ldots, f(a_1, \ldots, a_m) - 1)$. Положим

$$E(x_1, \ldots, x_m, y_0, y_1, \ldots, y_n) = (y_1 - 2^{y_2})^2 + (D(x_1, \ldots, x_m, y_0, y_1, \ldots, y_n))^2.$$

Функция E неотрицательна и для любого набора $(a_1, \ldots, a_m)$ принимает в кубе (11) ровно $f(a_1, \ldots, a_m)$ раз значение 0. Мы хотим далее рассмотреть в качестве последовательности $v_0, v_1, \ldots, v_s$ из леммы 2 последовательность значений, принимаемых функцией E в кубе (11). Положим

$$F(x_1, \ldots, x_m, h, l, z) = \sum_{0 \leqslant y_0, \ldots, y_n \leqslant z} (2^{h+l} - E) 2^{(h+l+1)(y_0(z+1)^n + \ldots + y_{n-1}(z+1) + y_n)}.$$

Имея в виду неравенства (5) и (6), суперпозициями функции 2^{x+y} определим в классе $[S_1]$ такие функции $l(x_1, \ldots, x_m)$, $h(x_1, \ldots, x_m)$, чтобы выполнялись неравенства

$$\max_{0 \leqslant y_0, \ldots, y_n \leqslant C(x_1, \ldots, x_m)} E(x_1, \ldots, x_m, y_0, \ldots, y_n) < 2^{l(x_1, \ldots, x_m)}, \tag{13}$$

$$(1 + l(x_1, \ldots, x_m))(1 + C(x_1, \ldots, x_m))^{n+1} < h(x_1, \ldots, x_m). \tag{14}$$

Тогда если ввести обозначение

$$G(x_1, \ldots, x_m) = F(x_1, \ldots, x_m, h(x_1, \ldots, x_m), l(x_1, \ldots, x_m), C(x_1, \ldots, x_m)),$$

то на основании неравенств (13), (14), леммы 2 и свойств функции E будем иметь

$$f(x_1, \ldots, x_m) = (1 + C(x_1, \ldots, x_m))^{n+1} \dot{-} \left[\frac{\sigma(G(x_1, \ldots, x_m))}{h(x_1, \ldots, x_m)} \right].$$

Таким образом, для завершения доказательства леммы достаточно установить, что классу $[S_1]$ принадлежит функция G. Для этого рассмотрим сумму из правой части равенства (12). Ее можно представить в виде конечной линейной комбинации (с коэффициентами, являющимися многочленами от переменных $x_1, \ldots, x_m$) сумм вида

$$\sum_{y_0=0}^{z} \ldots \sum_{y_n=0}^{z} y_0^{i_0} \ldots y_n^{i_n} 2^{y_0 p_0(h,l,z) + \ldots + y_n p_n(h,l,z)}, \tag{15}$$

где $i_0, \ldots, i_n$ — целые неотрицательные числа, $p_0, \ldots, p_n$ — многочлены с натуральными коэффициентами. Сумму (15) можно далее переписать в виде

$$\prod_{k=0}^{n} \sum_{y_k=0}^{z} y_k^{i_k} 2^{y_k p_k(h,l,z)}.$$

Для сумм вида

$$\sum_{w=0}^{z} w^i q^w$$

легко выводятся формулы типа

$$\sum_{w=0}^{z} w^i q^w = \frac{A_i(q, z) q^{z+1} + B_i(q, z)}{(q-1)^{i+1}}, \tag{16}$$

где A_i, B_i — многочлены с целыми коэффициентами.

Заметим теперь, что $G(x_1, \ldots, x_m)$ есть всегда целое неотрицательное число. Аналогичным образом, суммы (15) также задают целые неотрицательные числа. Поэтому при вычислении $G(x_1, \ldots, x_m)$ все вычитания и деления (в частности, при использовании формул типа (16)) можно производить в области целых неотрицательных чисел, то есть с помощью функций $x \dot{-} y$, $[x/y]$. Лемма доказана.

Теорема. $[S_1] = K$.

Доказательство. Включение $[S_1] \subseteq K$ очевидно. Установим обратное включение. В силу леммы 3 для этого достаточно доказать, что всякий предикат из класса K имеет однократное представление вида (9), ограниченное в классе K.

В работе [6] доказано, что всякий рекурсивно перечислимый предикат $P(x_1, \ldots, x_m)$ имеет однократное экспоненциально диофантово представление, то есть однократное представление формулой вида

$$(\exists y_1) \ldots (\exists y_n)\ (A = B), \tag{17}$$

где выражения A, B получены из натуральных чисел и переменных $x_1, \ldots, x_m$, $y_1, \ldots, y_n$ с помощью сложения, умножения и возведения в степень (этот результат получен ранее в работе [7], однако доказательство из [7] не подходит для наших целей). Несложный анализ доказательства из [6] показывает, что в случае элементарного по Кальмару предиката P однократное представление (17) ограничено в классе K. Отметим лишь основные моменты этого анализа. В качестве исходного представления предикатов в работе [6] рассматривается представление с помощью одноленточных машин Тьюринга. Если предикат P элементарен по Кальмару, то, как хорошо известно (см., например, [9]), его можно распознать на одноленточной машине Тьюринга $\mathfrak{M}$, работающей с зоной и временем, которые являются элементарными по Кальмару функциями. Из однократного экспоненциально диофантова представления вида (17) для предиката P, которое устанавливается в [6], непосредственно вытекает, что в случае истинности значения $P(x_1, \ldots, x_m)$ значения переменных $y_1, \ldots, y_n$ в формуле (17) можно выбрать не превосходящими величины, которая элементарно (то есть с помощью функций из K) определяется через время работы машины $\mathfrak{M}$ над входом $(x_1, \ldots, x_m)$ (более точно, через длину слова M из словарного экспоненциального представления предиката P, приведенного в [6] на стр. 80–81; слово M там по существу является конкатенацией конфигураций машины $\mathfrak{M}$, работающей над входом $(x_1, \ldots, x_m)$). Так как время работы машины $\mathfrak{M}$ является функцией из K, то тем самым мы приходим к однократному экспоненциально диофантовому представлению (17), ограниченному в классе K.

Проведем дальнейшие преобразования представления (17). Во-первых, за счет введения новых переменных вынесем из выражений A, B все выражения вида $E_1^{E_2}$, где E_2 отлично от константы. Этого можно достичь путем использования очевидной эквивалентности:

$$(18)\quad A(\ldots E_1^{E_2}\ldots) = B(\ldots E_1^{E_2}\ldots) \equiv (\exists a)_{a\leqslant E_1}(\exists b)_{b\leqslant E_2}(\exists d)_{d\leqslant E_1^{E_2}}$$
$$\big(a = E_1 \,\&\, b = E_2 \,\&\, d = a^b \,\&\, A(\ldots d\ldots) = B(\ldots d\ldots)\big).$$

Ясно, что предикат, стоящий в левой части эквивалентности (18), однократно представим формулой, стоящей в правой части эквивалентности. Последовательное применение указанного приема позволяет получить для указанного элементарного по Кальмару предиката $P(x_1, \ldots, x_m)$ из представления (17) однократное представление вида

$$(19)\quad (\exists y_1)_{y_1\leqslant C_1}\ldots(\exists y_n)_{y_n\leqslant C_n}(\exists a_1)_{a_1\leqslant F_1}(\exists b_1)_{b_1\leqslant F_2}(\exists d_1)_{d_1\leqslant F_3}\ldots$$
$$\ldots(\exists a_s)_{a_s\leqslant F_{3s-2}}(\exists b_s)_{b_s\leqslant F_{3s-1}}(\exists d_s)_{d_s\leqslant F_{3s}}\Big(\mathop{\&}_{i=1}^{s}(d_i = a_i^{b_i})$$
$$\&\, D_1(x_1, \ldots, x_m, y_1, \ldots, y_n, a_1, b_1, d_1, \ldots, a_s, b_s, d_s) = 0\Big),$$

где $C_1, \ldots, C_n, F_1, \ldots, F_{3s}$ — функции из K, а D_1 — многочлен с целыми коэффициентами.

Воспользуемся теперь результатами работы [7], согласно которым предикат

$$(20)\qquad \mathop{\&}_{i=1}^{s} (d_i = a_i^{b_i})$$

однократно представим формулой вида

$$(21)\qquad (\exists y_1)\ldots(\exists y_{4s})(\exists v)(\exists w)\,(w = 2^v$$
$$\& D_2(a_1, b_1, d_1, \ldots, a_s, b_s, d_s, y_1, \ldots, y_{4s}, v, w) = 0),$$

где D_2 — многочлен с целыми коэффициентами. Как вытекает из доказательства, приведенного в [7], в случае истинности предиката (20) значения переменных $y_1, \ldots, y_{4s}$, v, w в формуле (21) можно взять не превосходящими величины

$$2^{20\sum_{i=1}^{s}(2a_i+1)(b_i^2+1)(d_i+1)}.$$

Учитывая этот факт, для элементарного по Кальмару предиката P получаем из (19), (21) однократное представление вида (9), ограниченное в классе K.

Сделаем еще одно замечание технического характера. Большинство утверждений из работы [6] и работы [7] доказано дла случая, когда переменные принимают лишь натуральные значения. Чтобы иметь возможность рассматривать также и значение 0, можно поступить следующим образом. Для произвольного элементарного по Кальмару предиката $P(x_1, \ldots, x_m)$ определить предикат $P'(x_1, \ldots, x_m)$, переменные в котором принимают натуральные значения, соотношением

$$P'(x_1, \ldots, x_m) \equiv P(x_1 - 1, \ldots, x_m - 1),$$

а затем перенести утверждения о предикате P' на предикат P. Теорема доказана.

Следствие. $[S_2] = K$.

Доказательство. Так как, очевидно, $[S_2] \subseteq K$, то, согласно теореме, достаточно установить, что $S_1 \subset [S_2]$. Имеем

$$1 = [(x+1)/(x+1)], \qquad x \dot{-} y = \tau([2^x/2^y])$$

(напомним, что в силу нашего соглашения $\tau(0) = 0$). Пусть $\binom{x+y}{x}$ обозначает функцию, равную числу сочетаний из $x+y$ по x. В работе [4] доказано, что функцию $\binom{x+y}{x}$ можно получить суперпозициями функций $\{x+1, x \dot{-} y, [x/y], x^y\}$. Наконец, из одной теоретико-числовой теоремы Э. Куммера [3] следует, что

$$\sigma(x) = \tau\left(\binom{2x}{x}\right).$$

Цитированная литература

[1] A. Grzegorczyk, *Some classes of recursive functions*, Rozprawy Mat. 4 (1953).

[2] J. P. Jones and Ju. V. Matijasevič, *A new representation for the symmetric binomial coefficient and its applications*, Ann. Sci. Math. Québec 6 (1) (1982), 81–97.

[3] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[4] С. С. Марченков, *Об одном базисе по суперпозиции в классе функций, элементарных по Кальмару*, Матем. заметки 27 (3) (1980), 321–332.

[5] Ю. В. Матиясевич, *Один класс критериев простоты, формулируемых в терминах делимости биномиальных коэффициентов*, Записки научн. семинаров Ленинград. отдел. матем. ин-та АН СССР 67 (1977), 167–183.

[6] —, *Новое доказательство теоремы об экспоненциально диофантовом представлении перечислимых предикатов*, там же, 60 (1976), 75–92.

[7] —, *Существование неэффективизируемых оценок в теории экспоненциально диофантовых уравнений*, там же, 40 (1974), 77–93.

[8] Ch. Parsons, *Hierarchies of primitive recursive functions*, Z. Math. Logik Grundlag. Math. 14 (4) (1968), 357–376.

[9] R. W. Ritchie, *Classes of predictably computable functions*, Trans. Amer. Math. Soc. 106 (1963), 139–173.

[10] D. Rödding, *Über die Eliminierbarkeit von Definitionsschemata in der Theorie der rekursiven Funktionen*, Z. Math. Logik Grundlag. Math. 10 (4) (1964), 315–330.

Presented to the Semester
Combinatorics and Graph Theory
September 14 — December 17, 1987