МАТЕМАТИЧЕСКАЯ ЛОГИКА И ЕЕ ПРИМЕНЕНИЯ
1982 ВЫПУСК 2

УДК 510.52+511.5

АРИФМЕТИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ КЛАССОВ МАШИННОЙ СЛОЖНОСТИ

Стасис ШКНА

I. Введение. Как известно, любое перечислимое множество натуральных чисел арифметично, т.е. представимо некоторой формулой в сигнатуре $(0,1,+,\cdot,=)$. При этом под арифметической сложностью множества понимается любая функция, ограничивающая все связанные переменные в некотором арифметическом представлении этого множества.

С прикладной точки зрения важной представляется задача определения машинной сложности распознавания множества исходя из его арифметического представления. Одним из возможных путей решения этой задачи является исследование обратной задачи - задачи установления арифметической сложности субрекурсивных классов машинной сложности. Такой подход может оказаться полезным и для целей привлечения теоретико-числовых методов к решению известных проблем машинных классов сложности, таких как $\mathbb{P} \stackrel{?}{=} \mathbb{NP}$, и др.

К этому направлению относится, например, работа К. Мандерса и Л. Эдлимэна [I], где приведены два интересных примера $\mathbb{NP}$ -полных теоретико-числовых проблем. Ими же в работе [2] получена некоторая неполная диафантова характеризация класса $\mathbb{NP}$. Интересное исследование диафантовой сложности примитивно рекурсивных предикатов

из классов $\mathcal{E}^n_n$ Гжегорчика при $n \geq 3$ проведено А. Виноградовым и Н. Косовским в работе [3]. Н. Косовским в [4] анонсируется полная характеризация класса $\mathbb{NP}$ в терминах логико-арифметических уравнений.

В настоящей работе предлагается один общий метод получения верхних оценок арифметической сложности для множеств, задаваемых сложностью их распознавания на машинах Тьюринга. В качестве применения этого метода дается полная арифметическая характеризация класса $\mathbb{NP}$: множество натуральных чисел $\mathcal{M}$ распознается недетерминированной машиной Тьюринга за время, полиномиально зависящее от длины входа тогда и только тогда, когда $\mathcal{M}$ представимо в виде

$$x \in \mathcal{M} \Leftrightarrow \exists y_1 \leq 2^{|x|^{k_1}} \forall z \leq |x|^{\ell} \exists y_2 \leq 2^{|x|^{k_2}} \dots \exists y_\nu \leq 2^{|x|^{k_\nu}} \left[P(x, y_1, \dots, y_\nu, z) = 0 \right],$$

где $\ell, k_1, \dots, k_\nu \geq 0$, $|x|$ - длина двоичного кода числа x , $P(x, y_1, \dots, y_\nu, z)$ - некоторый полином с целыми коэффициентами (причем ν не зависит от $\mathcal{M}$). Тем самым получено сведение известной проблемы К. Мандерса и Л. Эдлимэна (см.,напр.,[I]) о совпадении класса $\mathbb{NP}$ с классом $\mathfrak{D}$ множеств, представимых в виде

$$x \in \mathcal{M} \Leftrightarrow \exists y_1 \leq 2^{|x|^{k_1}} \dots \exists y_\nu \leq 2^{|x|^{k_\nu}} \left[P(x, y_1, \dots, y_\nu) = 0 \right]$$

к теоретико-числовой проблеме о замкнутости класса $\mathfrak{D}$ относительно навешивания ограниченного квантора всеобщности вида $\forall z \leq |x|^{\ell}$.

Получена также строгая иерархия элементарных по Кальмару множеств из класса $\mathcal{E}^3_*$ по их арифметической сложности. Полученная иерархия является арифметическим аналогом иерархии предсказуемо вычислимых предикатов Р. Ричи и может быть использована для установления сложности вычисления таких предикатов исходя из их арифметических представлений.

2. Предварительные сведения. В дальнейшем $\bar{x}_n$ – кортеж вида $(x_1, \dots, x_n)$, $|x|$ – длина двоичной записи числа x, $|\bar{x}_n| = |x_1 + \dots + x_n|$, $\mathcal{P}$ – класс полиномов с натуральными коэффициентами, $\omega = \{0, 1, \dots\}$.

Если Φ – некоторый класс функций, то положим

$$exp_0(\Phi) = \Phi, \quad exp_{i+1}(\Phi) = \{ f(2^g) : f, g \in exp_i(\Phi) \}.$$

Через Φ_* будем обозначать класс графиков функций из Φ.

Пусть G, H – некоторые классы неубывающих функций.

Обозначим через $\mathcal{A}\{G, H\}$ класс множеств M, $M \subseteq \omega^m$, $m \geq 1$, имеющих арифметическое представление вида

$$\bar{x}_m \in M \iff \Delta \left[P(\bar{x}_m, y_1, \dots, y_k, z_1, \dots, z_l) = 0 \right],$$

где P – полином с целыми коэффициентами, Δ – кванторный префикс, состоящий из расположенных в некотором порядке ограниченных кванторов существования $\exists y_i \leq g_i(|\bar{x}_m|)$, $g_i \in G$, $i = 1, \dots, k$ и ограниченных кванторов всеобщности $\forall z_j \leq h_j(|\bar{x}_m|)$, $h_j \in H$, $j = 1, \dots, l$.

В дальнейшем без особых оговорок будем пользоваться очевидным свойством замкнутости классов $\mathcal{A}\{G, H\}$ относительно объединений и пересечений множеств, следующим из очевидных соотношений $(a = 0) \vee (b = 0) \iff a \cdot b = 0$ и $(a = 0) \& (b = 0) \iff a^2 + b^2 = 0$.

Будем рассматривать следующую модель машин Тьюринга (МТ). МТ состоит из входной ленты и рабочей ленты. При этом на рабочей ленте можно считывать и записывать, тогда как на входной ленте – только считывать. Использованная при работе память считается по числу использованных ячеек рабочей ленты.

Пусть S и T – классы неубывающих функций. Следуя [5], посредством $F\{S, T\}$ обозначим класс функций, вычислимых на МТ с памятью, ограниченной функцией из S (от длины входа), за время, ограниченное функцией из T (от длины входа).

В настоящей работе мы ограничимся рассмотрением классов S и T, удовлетворяющих приводимым ниже условиям, достаточными для того, чтобы классы $F\{S, T\}$ обладали некоторыми "естественными" свойствами замкнутости (см. [5]).

Во-первых, не будем рассматривать классы S и T слишком медленно растущих функций, а именно, предположим, что*)

$$\exists s \; \forall n \quad [s(n) \geq \log_2 n + 1] \tag{2.1}$$

$$\exists t \; \forall n \quad [t(n) \geq n + 2]. \tag{2.2}$$

Так как при любом вычислении на МТ память s и время t связаны соотношением $s(n) \leq t(n)$, то предположим, что

$$\forall s \; \exists t \; \forall n \quad [s(n) \leq t(n)]. \tag{2.3}$$

Будем предполагать, что сами функции из классов S и T достаточно просто вычислимы, а именно:

$$T \cup S \subseteq F\{S, T\} \tag{2.4}$$

Наконец, следующие четыре условия достаточны для замкнутости классов $F\{S, T\}$ относительно явных преобразований, подстановки и некоторого типа рекурсии (см. [5]):

$$\forall s_1 s_2 k \; \exists s_3 \; \forall n \quad [s_1(kn) + s_2(kn) \leq s_3(n)] \tag{2.5}$$

$$\forall t_1 t_2 k \; \exists t_3 \; \forall n \quad [t_1(kn) \cdot t_2(kn) \leq t_3(n)] \tag{2.6}$$

$$\forall s_1 s_2 \; \exists s_3 \; \forall n \quad [s_1(s_2(n)) \leq s_3(n)] \tag{2.7}$$

$$\forall s \, t_1 \; \exists t_2 \; \forall n \quad [t_1(s(n)) \leq t_2(n)]. \tag{2.8}$$

Заметим также, что для любой функции $f(\bar{x}_n)$ из класса $F\{S, T\}$ имеется $s \in S$ такая, что

*) Переменные s, t и они же с индексами будут использоваться в качестве переменных для функций из классов S и T соответственно.

$$\forall \bar{x}_n \qquad f(\bar{x}_n) \le 2^{s(|\bar{x}_n|)} \tag{2.9}$$

В дальнейшем мы воспользуемся следующим машинно-независимым описанием классов $F\{S,T\}$, полученным С.В. Пахомовым в [5].

Пусть $W\{S,T\}$ – класс функций, получаемых из исходных функций $\min\left(\left[\frac{x}{2^y}\right], 2^{s(|x|)}\right)$, $\min\left(2^y, 2^{s(|x|)}\right)$, $\min\left(rest(x,2^y), 2^{s(|x|)}\right)$, $2^{s(|x|)}$, $\mu(x,i)$ –ый знак в двоичном разложении числа x, $\min(x\cdot y, 2^{s(|x|)})$, $\min(x+y, 2^{s(|x|)})$, где s – произвольная функция из класса S, посредством операций явних преобразований, подстановки и рекурсии вида

$$(*)\quad \begin{cases} f(\bar{x}_n, 0) = g(\bar{x}_n), \\ f(\bar{x}_n, y+1) = h(\bar{x}_n, f(\bar{x}_n, y)), \\ f(\bar{x}_n, y) \le 2^{s(|\bar{x}_n|)}, \\ \varphi(\bar{x}_n, y) = f(\bar{x}_n, t(|y|)), \end{cases}$$

где $s \in S$ и $t \in T$.

Теорема (Пахомов [5]). Пусть классы неубывающих функций S и T удовлетворяют условиям (2.I)-(2.8).

Тогда классы функций $F\{S,T\}$ и $W\{S,T\}$ совпадают.

И, наконец, для $i,j \in \omega$ положим

$$A[i,j] = A\{exp_i(\pi), exp_j(\pi)\},$$

$$D[i] = A\{exp_i(\pi), \varnothing\},$$

$$F[i,j] = F\{exp_i(\pi), exp_j(\pi)\}.$$

Легко видеть, что

$$A[i,j] \subseteq F_*[\max(i,j)-1, \max(i,j)] \tag{2.10}$$

для всех $i+j \ge 1$.

3. Основные результаты.

Теорема 3.I. Пусть S, T – классы неубывающих функций, удов-

летворяющие условиям (2.I),(2.3)-(2.8), $\pi \subseteq T$ и $S_* \cup T_* \subseteq A\{exp_1(S \cup T), T\}$. Тогда графики функций из класса $F\{S,T\}$ являются $A\{exp_1(S \cup T), T\}$-множествами.

Следствие 3.I. Для любых $i,j \ge 0$ имеют место включения

$$F_*[i,j] \subseteq A[\max(i,j)+1, j].$$

Следствие 3.2. Любое множество натуральных чисел, распознаваемое детерминированной машиной Тьюринга за время, полиномиально зависящее от длины входа, является $A[1,0]$-множеством.

Следствие 3.2 и результаты работы [I] позволяют получить полную арифметическую характеризацию класса NP.

Теорема 3.2*). Класс NP совпадает с классом $A[1,0]$-множеств.

Теорема 3.3. Пусть $i \ge 0$. Тогда любое множество $M \subseteq \omega^m$, $m \ge 1$ из класса $A[i+1, i]$ представимо в виде

$$\bar{x}_m \in M \iff \exists y_1\, \forall z \le q(|\bar{x}_m|)\, \exists y_2 \ldots \exists y_\nu \left[\&_{i=1}^{\nu} y_i \le f_i(|\bar{x}_m|) \,\&\, P(\bar{x}_m, z, \bar{y}_\nu) = 0 \right]$$

где $g \in exp_i(\pi)$, $f_i \in exp_{i+1}(\pi)$, $i = 1, \ldots, \nu$.
и P – полином с целыми коэффициентами.

Следствие 3.3. Существует $\nu_0 \ge 0$ такое, что класс NP совпадает с классом множеств $M \subseteq \omega^m$, $m \ge 1$, представимых в виде $\bar{x}_m \in M \iff \exists y_1\, \forall z \le p(|\bar{x}_m|)\, \exists y_2 \ldots \exists y_{\nu_0} \left[\&_{i=1}^{\nu_0+m} y_i \le 2^{q_i(|\bar{x}_m|)} \,\&\, P(\bar{x}_m, z, \bar{y}_{\nu_0+m}) = 0 \right]$,

где $p, q_i \in \pi$, P – полином с целыми коэффициентами.

4. Доказательства

Доказательство теоремы 3.I. Пусть классы неубывающих функций

*) См. Примечание на стр. I06.

S, T удовлетворяют условиям теоремы 3.I. Тогда утверждение теоремы прямо следует из теоремы Пахомова [5] и следующих трех лемм.

Лемма 4.I. Графики всех исходных функций класса $W\{S,T\}$ являются $A\{exp_1(SUT), T\}$ -множествами.

Доказательство. Известно (см.[2]), что график экспоненты x^y является $\mathbb{D}[1]$ -множеством. Но $\mathbb{D}[1] \subseteq A\{exp_1(T), \phi\}$, поскольку $\mathfrak{T} \subseteq T$. Поэтому утверждение леммы следует из следующих представлений графиков исходных функций класса $W\{S,T\}$:

I) $z = \min(x,y) \iff (z = x) \& (x \le y) \vee (z = y)$,

где $x \le y \iff \exists w \le y\,[y - x - w = 0]$;

2) $\left[\frac{x}{2^y}\right] = z \iff z = 0 \vee \exists u \le x\left[u = 2^y \& z \cdot u \le x \& (z+1)\cdot u > x\right]$;

3) $y = 2^{\lambda(|x|)} \iff \exists z \le x\, \exists w \le x\, \exists u \le \lambda(|x|)\left[y = 2^u \& u = \lambda(w) \& 2^z \le x \& 2^{z+1} > x \& w = z+1\right]$,

где, в силу условия $S_* \subseteq A\{exp_1(SUT), T\}$, график функции $\lambda(w)$ является $A\{exp_1(SUT), T\}$ -множеством;

4) $\min\left(rest(x, 2^y), 2^{\lambda(|x|)}\right) = w \iff \exists u \le 2^{\lambda(|x|)}\left[u = 2^y \& x = \left[\frac{x}{2^y}\right]\cdot u + w\right] \& w \le 2^{\lambda(|x|)} \vee w = 2^{\lambda(|x|)}$;

5) $x \dot{-} y = z \iff y + z - x = 0 \vee (x < y \& z = 0)$;

6) $\mu(x,i) = y \iff \exists u \le x\, \exists v \le x\left[y < 2^i \& x = u \cdot 2^{i+1} + y \cdot 2^i + v\right]$. □

Лемма 4.2. Пусть функция $f(\bar{x}_m)$ получена путем подстановки из функций $h(\bar{y}_m), g_1(\bar{x}_m), \dots, g_n(\bar{x}_m)$ класса $W\{S,T\}$, графики которых входят в $A\{exp_1(SUT), T\}$. Тогда график функции $f(\bar{x}_m)$ является $A\{exp_1(SUT), T\}$ множеством.

Доказательство следует из представления

$$f(\bar{x}_m) = y \iff \exists z_1 \dots \exists z_n\left[z_1 = g_1(\bar{x}_m) \& \dots \& z_n = g_n(\bar{x}_m) \& y = h(z_1, \dots, z_n)\right]$$

имея в виду свойство (2.9). □

Лемма 4.3. График функции $\varphi(\bar{x}_n, y)$, полученной рекурсией вида (*) из $g(\bar{x}_n), h(\bar{x}_n, z), \lambda, t$ класса $W\{S,T\}$, графики которых входят в класс $A\{exp_1(SUT), T\}$, является $A\{exp_1(SUT), T\}$ -множеством.

Доказательство. Рассмотрим функцию $\beta(p, a, k) = k$-ая цифра в записи числа a в p -ичной системе счисления; счет ведется начиная с младших разрядов - $\beta(p, a, 0)$ есть цифра в разряде единиц; функция не определена при $a = 0$ и $p = 1$.

Воспользуемся следующим очевидным свойством функции β:

(**) Каковы бы ни были числа $n, a_0, \dots, a_n$, можно найти числа p, a такие, что $\beta(p, a, i) = a_i$ при $i = 0, \dots, n$ (в качестве p можно взять любое число, превосходящее числа $1, a_0, \dots, a_n$, и положить $a = \sum_{i=0}^{n} a_i p^i$).

Таким образом, функцией β можно кодировать конечные последовательности чисел.

В частности, для любых фиксированных $\bar{x}_n$ и y существуют числа p и a, обладающие следующим свойством:

$$\forall i \le t(|y|)\left[\beta(p, a, i) = f(\bar{x}_n, i)\right]. \tag{4.I}$$

Для этого ввиду (2.9) в качестве p достаточно взять любое число, превосходящее $2^{\lambda(|\bar{x}_n|)}$, и положить

$$a = \sum_{i=0}^{t(|y|)} f(\bar{x}_n, i) \cdot p^i \tag{4.2}$$

откуда $p \le \sigma_1(|\bar{x}_n, y|)$ и $a \le \sigma_2(|\bar{x}_n, y|)$ при подходящих σ_1, σ_2 из $exp_1(SUT)$.

Поскольку $\varphi(\bar{x}_n, y)$ получена рекурсией вида (*) из $g(\bar{x}_n)$

и $h(\bar{x}_n, z)$, то свойство (4.I) можно записать так:

$$\forall i \le t(|y|)\,\big[i = 0 \,\&\, \beta(p,a,i) = g(\bar{x}_n) \vee \exists j < i\,\big[i = j+1 \,\&\, \beta(p,a,i) = h(\bar{x}_n, \beta(p,a,j))\big]\big]. \tag{4.3}$$

В результате имеем

$$\varphi(\bar{x}_n, y) = z \iff \exists p \le \sigma_1(|\bar{x}_n, y|)\ \exists a \le \sigma_2(|\bar{x}_n, y|)\ \big[\Theta \,\&\, \beta(p,a,t(|y|)) = z\big], \tag{4.4}$$

где в силу условия $T_* \subseteq \mathbb{A}\{exp_1(SUT), T\}$ график функции $t(|y|)$ является $\mathbb{A}\{exp_1(SUT), T\}$ -множеством.

И, наконец, как следует из представления

$$\beta(p,a,k) = d \iff p > 1 \,\&\, p > d \,\&\, \exists x \le a\ \exists y \le a\ \big[p^k > x \,\&\, (a = y \cdot p^{k+1} + d \cdot p^k + x)\big], \tag{4.5}$$

график функции β является $\mathbb{A}\{exp_1(SUT), T\}$ -множеством. □

Доказательство теоремы 3.2. В работе [I] доказано существование множества $N \subseteq \omega^6$ такого, что

а) $N \in \mathbb{P}$, т.е. N распознается детерминированной машиной Тьюринга за полиномиальное время, и

б) любое множество $M \subseteq \omega$, $M \in \mathbb{NP}$ представимо в виде

$$x \in M \iff \exists y_1 \le 2^{q_1(|x|)} \ldots \exists y_8 \le 2^{q_8(|x|)}\big[P(x, y_1, \ldots, y_8) = 0 \,\&\, (y_1, \ldots, y_6) \in N\big],$$

где $q_i \in \mathcal{T}$ и P - полином с целыми коэффициентами.

Совершенно аналогично можно доказать, что для любого $m \ge 1$ существует $N_m \subseteq \omega^{m+5}$ такое, что $N_m \in \mathbb{P}$, и любое множество $M \subseteq \omega^m$, $M \in \mathbb{NP}$ представимо в виде

$$\bar{x}_m \in M \iff \exists y_1 \le 2^{q_1(|\bar{x}_m|)} \ldots \exists y_{m+7} \le 2^{q_{m+7}(|\bar{x}_m|)}\big[P(\bar{x}_m, \bar{y}_{m+7}) = 0 \,\&\, (y_1, \ldots, y_{m+5}) \in N_m\big]. \tag{4.6}$$

Отсюда в силу следствия 3.2

$$\mathbb{NP} \subseteq \mathbb{A}[1,0]. \tag{4.7}$$

Справедливость обратного включения $\mathbb{A}[1,0] \subseteq \mathbb{NP}$ очевидна.

Для иллюстрации рассмотрим, например, частный случай, когда $M \subseteq \omega$ является множеством, представленным в виде

$$x \in M \iff \exists y \le 2^{q_1(|x|)} \forall z \le q_2(|x|)\ \exists w \le 2^{q_3(|x|)}\big[P(x,y,z,w) = 0\big].$$

Множество M распознается следующей недетерминированной процедурой:

```
Вход: x
  begin  z := 0;
       недетерминированного угадать y ( y ≤ 2^{q1(|x|)} );
    L: недетерминированно угадать w ( w ≤ 2^{q3(|x|)} );
       вычислить ξ := P(x,y,z,w);
       if ξ =0 then begin if  z < q2(|x|)  then z := z+1;
                          go to L else принять
                    end
                    else  отвергнуть
  end.
```

При этом время распознавания равняется по порядку

$$q_1(|x|) + q_2(|x|)\,(q_3(|x|) + t),$$

где t - максимальное время вычисления значения полинома $P(x,y,z,w)$ при $|y| \le q_1(|x|)$, $|z| \le |q_2(|x|)|$, $|w| \le q_3(|x|)$ и, следовательно, является некоторым полиномом от $|x|$. □

Доказательство теоремы 3.3. Прежде всего заметим, что, используя функцию $\beta(p,a,k)$, в $A[i+1, i]$ -представлениях множеств можно "проталкивать" вправо ограниченные кванторы всеобщности. Поясним это на типичном примере.

Пусть множество $M \subseteq \omega$ имеет $A[i+1, i]$ -представление

$$x \in M \iff \forall y_1 \le g_1(|x|)\ \exists z_1 \le f_1(|x|)\ \forall y_2 \le g_2(|x|)\ \exists z_2 \le f_2(|x|)$$
$$[\, P(x, y_1, y_2, z_1, z_2) = 0 \,],$$

где

$$g_1, g_2 \in \exp_i(\pi)\ ,\quad f_1, f_2 \in \exp_{i+1}(\pi)\ . \tag{4.8}$$

Используя свойство $(**)$ функции $\beta(p,a,k)$ (см. доказательство леммы 4.3), имеем

$$x \in M \iff \exists p \le f_1(|x|)+1\ \exists a \le h(|x|)\ \ \forall y_1 \le g_1(|x|)$$
$$\forall y_2 \le g_2(|x|)\ \exists z_2 \le f_2(|x|)\ \exists u \le f_1(|x|)$$
$$[\, P(x, y_1, y_2, u, z_2) = 0 \ \&\ u = \beta(p, a, y_1) \,],$$

где

$$h(|x|) = \sum_{n=0}^{g_1(|x|)} f_1(|x|)\cdot \left(f_1(|x|)+1\right)^n . \tag{4.9}$$

При этом в силу (4.8) $h \in \exp_{i+1}(\pi)$.

Итак, любое $A[i+1, i]$ -множество $M \subseteq \omega^m$ имеет представление вида

$$\bar{x}_m \in M \iff \exists \bar{y}_k\ \forall x_1 \le g_1(|\bar{x}_m|) \dots \forall x_l \le g_l(|\bar{x}_m|)\ \exists \bar{w}_n$$
$$\Big[\bigwedge_{a=1}^{k} y_a \le f_a(|\bar{x}_m|)\ \bigwedge_{b=1}^{n} w_b \le h_b(|\bar{x}_m|)\ \&$$
$$\&\ P(\bar{x}_m, \bar{y}_k, \bar{x}_l, \bar{w}_n) = 0\Big], \tag{4.10}$$

где $f_1, \dots, f_k, h_1, \dots, h_n \in \exp_{i+1}(\pi)$, $g_1, \dots, g_l \in \exp_i(\pi)$.

Воспользуемся далее стандартными функциями "спаривания"

$$\mathcal{J}(x,y) = \tfrac{1}{2}(x+y)(x+y+1) + x,$$

$$K(z) = z - \tfrac{1}{2}\left[\frac{\left[\sqrt{8z+1}\right]+1}{2}\right]\left[\frac{\left[\sqrt{8z+1}\right]-1}{2}\right],\quad L(z) = \left[\frac{\left[\sqrt{8z+1}\right]+1}{2}\right] - \left(K(z)+1\right). \tag{4.11}$$

Тогда

$$\mathcal{J}(K(z), L(z)) = z,\ K(\mathcal{J}(x,y)) = x\ ,\ L(\mathcal{J}(x,y)) = y. \tag{4.12}$$

Индуктивным образом определим функции "расщепления" $\tau_m^n(x)$: для любого $n \in \omega$

1) $\tau_1^1(x) = x$,

2) $\tau_i^{n+1}(x) = \tau_i^n(K(x))$ для $1 \le i \le n$,

3) $\tau_{n+1}^{n+1}(x) = L(x)$.

Пусть также $\mathcal{J}^{(1)}(x) = x$ и

$$\mathcal{J}^{(n+1)}(x_1, \dots, x_{n+1}) = \mathcal{J}\left(\mathcal{J}^{(n)}(x_1, \dots, x_n),\ x_{n+1}\right).$$

Функции τ_m^n и $\mathcal{J}^{(n)}$ связаны следующим образом:

$$\tau_i^n\left(\mathcal{J}^{(n)}(x_1, \dots, x_n)\right) = x_i \quad \text{для всех } i = 1, \dots, n\ . \tag{4.13}$$

Пусть теперь множество $M \subseteq \omega^m$ имеет $A[i+1, i]$ -представление (4.10). Тогда в силу (4.13)

$$\bar{x}_m \in M \iff \exists y \le \xi(|\bar{x}_m|)\ \forall z \le \eta(|\bar{x}_m|).\ \exists \bar{w}_n \Big[\bigwedge_{a=1}^{k} \tau_a^k(y) \le f_a(|\bar{x}_m|)$$
$$\bigwedge_{b=1}^{n} w_b \le h_b(|\bar{x}_m|)\ \&\ P(\bar{x}_m, \tau_1^k(y), \dots, \tau_k^k(y), \tau_1^l(z),$$
$$\dots, \tau_l^l(z), \bar{w}_n) = 0 \ \vee \bigvee_{c=1}^{l} \left(g_c(|\bar{x}_m|) < \tau_c^l(z)\right)\Big],$$

где

$$\xi(n) = \mathcal{J}^{(k)}(\gamma(n), \dots, \gamma(n)),$$
$$\eta(n) = \mathcal{J}^{(l)}(\delta(n), \dots, \delta(n))$$

и

$$\gamma(n) = \max_{1 \le a \le k} f_a(n)\ ,\quad \delta(n) = \max_{1 \le c \le l} g_c(n)\ .$$

При этом из представлений (4.11) следует, что $\xi \in \exp_{i+1}(\pi)$ и $\eta \in \exp_i(\pi)$. Остается заметить, что графики функций спари-

вания и расщепления являются $A[1,0]$ -множествами. □

5. Арифметическая иерархия класса $\mathcal{E}^3_*$. Рассмотрим некоторые свойства арифметической иерархии множеств $A = \{A[i,j]\}_{i,j=0}^{\infty}$. Пусть $\mathcal{E}^3_*$ - класс графиков (элементарных по Кальмару) функций из класса $\mathcal{E}^3$ иерархии Гжегорчика [6]. Из результатов Р. Ричи [7] следует, что

$$\mathcal{E}^3_* = \bigcup_{i,j\geq 0} F_*[i,j]. \qquad (5.1)$$

Отсюда, используя теорему 3.I, легко получить

$$A = \mathcal{E}^3_*. \qquad (5.2)$$

Действительно, по (2.I0) и (5.I) имеем

$$\forall i,j \geq 0 \qquad A[i,j] \subseteq \mathcal{E}^3_*.$$

С другой стороны, ввиду (5.I) и следствия 3.I

$$\forall M \in \mathcal{E}^3_* \quad \exists i,j \geq 0 \qquad M \in A[i,j].$$

Таким образом, иерархия A - это иерархия элементарных по Кальмару множеств.

Далее, используя (2.I0), следствие 3.I и известные результаты об иерархии множеств по ленточной сложности распознавания на машинах Тьюринга, нетрудно показать, что для любых $i,j \geq 0$ таких, что $i+j \geq 1$, выполнено строгое включение

$$A[i,j] \subsetneq A[\max(i,j)+2, \max(i,j)+1]. \qquad (5.3)$$

Действительно, пусть $i,j \geq 0$ и $k = \max(i,j) \geq 1$. Тогда имеет место следующая цепочка включений:

$$\begin{aligned} A[i,j] &\subseteq F_*[k-1,k] \subseteq && \langle (2.I0) \rangle \\ &\subseteq A[k+1,k] \subseteq && \langle \text{следствие 3.I} \rangle \\ &\subseteq F_*[k,k+1] \subseteq && \langle (2.I0) \rangle \\ &\subseteq A[k+2,k+1]. && \langle \text{следствие 3.I} \rangle \end{aligned}$$

По теореме Стирнза-Хартманиса-Льюиса о ленточной иерархии функций (см.[8], теорема 6)

$$F_*[k-1,k] \subsetneq F_*[k,k+1]$$

откуда

$$A[i,j] \subsetneq A[k+2,k+1].$$

Из конструкции элиминации ограниченного квантора всеобщности в диафантовых представлениях множеств, данного Ю.В. Матиясевичем (см.[9]), нетрудно извлекается включение

$$A[i,j] \subseteq \mathbb{D}[\max(i,j+3)] \qquad (5.4)$$

для всех $i,j \geq 0$.

Таким образом, по (5.3) и (5.4) имеем

$$\forall i \geq 0 \qquad \mathbb{D}[i] \subsetneq \mathbb{D}[i+4].$$

И наконец, поскольку отношение порядка $\{(x,y) : x \leq y\}$ лежит как в классе $\mathbb{D}[1]$, так и в классе $\mathbb{P}$, то, применяя теорему 2 работы[10], имеем

$$A[0,0] \subsetneq \mathbb{P} \cap \mathbb{D}[1].$$

ЛИТЕРАТУРА

I. МАНДЕРС К.Л., ЭДЛИМЭН Л. $\mathcal{NP}$ -полные проблемы решения для квадратных уравнений с двумя неизвестными. - Кибернетический сб., № I7, нов.сер. - М.:Мир, I980, с. I24-I42.

2. ADLEMAN L., MANDERS K.L. The computational complexity of decision procedures for polynomials. - Proc. 16th IEEE Symp. on Found.of Comp.Sci., 1975, p. 169-177.

3. ВИНОГРАДОВ А.К., КОСОВСКИЙ Н.К. Иерархия диафантовых представлений примитивно рекурсивных предикатов. - Вычислительная техника и вопросы кибернетики, вып. I2, Л.:изд.ЛГУ, I975, с.99-I07.

4. КОСОВСКИЙ Н.К. Полиномиальные пределы эффективизации перебора при поиске решений логико-арифметических уравнений. - УШ Всес.конф. по логике и методологии наук. Тез.докл. "Логика и основания математики", Паланга, I982, Вильнюс:изд.ВГУ, I982, с. 36-39.

5. ПАХОМОВ С.В. Машинно-независимое описание некоторых машинных классов сложности. - Зап.науч.сем.ЛОМИ, 1979, т.88, с.176-185.

6. GRZEGORCZYK A. Some classes of recursive functions. - Rozpravy Matematiczne, Warzsawa, 1953 Русск.пер.: Гжегорчик А. Некоторые классы рекурсивных функции.- Пробл.мат.логики,М.,1970.

7. 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. - Пробл.мат. логики, М.:Мир, 1970, с. 50-93 .

8. STEARNS R.E., HARTMANIS J., LEWIS II P.M. Hierarchies of memory limited computations. - IEEE Conf.Rec.Switch.Circuit Theory and Logic Design, N.Y., 1965, p. 179-190 Русск.пер.: Стринз Р.Е., Хартманис Дж., Льюис II П.М. Иерархии вычислений с ограниченной памятью. - Пробл.мат.логики, М.:Мир, 1970, с. 301-319.

9. МАТИЯСЕВИЧ Ю.В. Диафантовы множества. - Успехи мат.наук, 1972, т. 27, вып. 5, с. 185-222.

10. ИКНА С.П. Об одном принципе получения нижних оценок арифметической сложности. - Наст.сб.

ПРИМЕЧАНИЕ. Из обзора

"D. Joseph, P. Young. A survey of some recent results on computational complexity in weak theories of arithmetic. - Lect. Notes in Comput.Sci., 1981, v. 118, p. 46-60"

автору стало известно, что аналог теоремы 3.2 опубликован в (труднодоступной) работе

"Kent C., Hodgson B. An arithmetical characterization of NP. - Likehead Univ. Technical Report, 6-80, 1981 (Dept. of Mathematics, Thunder Bay, Ontario, Canada).

MAŠININIO SUDĖTINGUMO KLASIŲ ARITMETINĖ IŠRAIŠKA

Stasys JUKNA

Plačiai klasei aibių, atpažįstamų Tiuringo mašinomis su apribojimais laikui ir erdvei, gauta bendra aritmetinė tų aibių charakterizacija.

ARITHMETICAL REPRESENTATIONS OF MACHINE COMPLEXITY CLASSES

Stasys JUKNA

Let S and T be the classes of nondecreasing functions (satisfying some natural conditions). It is proved that every set $A \subseteq \{0,1,\dots\}$ recognizable within the space bounded by a function from S and within the time bounded by a function from T is representable by

$$x \in A \iff \Delta\left[P(x, y_1, \dots, y_k, z_1, \dots, z_l) = 0\right],$$

where Δ is a quantifier prefix formed from an arbitrary permutation of bounded quantifiers $\exists_{y_i} \le 2^{f_i(|x|)}$, $f_i \in S \cup T$, $i=1,\dots,k$ and $\forall_{z_j} \le q_j(|x|)$, $q_j \in T$, $j=1,\dots,l$; $|x|$= length of x (in binary) and P is a polynomial with integer coefficients. As a corrolary a full arithmetical characterization of NP sets analogous to that of recursively enumerable sets given by M. Davis is obtained: NP coincides with the class of sets A representable by

$$x \in A \iff \exists_{y_1} \forall_{z \le |x|^c} \exists_{y_2} \dots \exists_{y_\nu} \left[\bigvee_{i=1}^{\nu} y_i \le 2^{|x|^{d_i}} \;\&\; P(x, z, y_1, \dots, y_\nu) = 0\right]$$

where $c, d_1, \dots, d_\nu \ge 0$ and P is a polynomial with integer coefficients.