УДК 517.11; 519.6

В. К. Булитко, В. В. Булитко (Одес. ун-т)

О КРИТЕРИИ $\mathcal{NP}$-ПОЛНОТЫ*

The problem of construction of criteria of complete sets with respect to polynomial-bounded reducibilities is considered. A nonstandard description of sets from the class $\mathcal{NP}$, a brief proof of analog of the well-known Cook theorem, and certain criterion of $\mathcal{NP}$-completeness are suggested.

Розглядається проблема побудови критеріїв повних множин відносно поліноміально обмежених звідностей. Запропоновані нестандартний опис множин класу $\mathcal{NP}$, коротке доведення відомої теореми Кука та деякий критерій $\mathcal{NP}$-повноти.

В настоящей работе рассматриваются алгоритмические сводимости с полиномиальным ограничением времени работы сводящего алгоритма, являющиеся более сильными, чем классические алгоритмические сводимости $\leq_1$, $\leq_m$, $\leq_{tt}$, $\leq_T$ и т.п. [1]. Действительно, в классе рекурсивных множеств сложностные иерархии, задаваемые классической сводимостью $\leq_1$ (и тем более слабыми сводимостями $\leq_m$, $\leq_{tt}$, $\leq_T$ и т.п.) тривиальны. Не так обстоит дело с полиномиально ограниченной сводимостью $\leq_{pol}$ [2]. Соответствующая иерархия множеств весьма сложна.

Но, как показал С. Кук, в классе рекурсивных множеств можно указать подкласс — аналог класса рекурсивно перечислимых множеств (так называемый класс $\mathcal{NP}$), в котором существуют полные по $\leq_{pol}$ множества (они называются $\leq_{pol}$-полными множествами или $\mathcal{NP}$-полными). В свою очередь, в классе $\mathcal{NP}$ можно выделить подкласс $\mathcal{P}$ множеств, для которых проблема вхождения решается за полиномиально ограниченное время. Эти множества аналогичны в ряде отношений рекурсивным множествам классической теории рекурсии.

Указанная аналогия не является полной и достаточно интенсивно изучается; хотя на этом пути получено важные результаты [2,3], имеется еще много неясного. Например, насколько нам известно, в литературе нет критериев $\leq_{pol}$-полноты, отличных от определения, в то время как в классической теории рекурсии построена достаточно развитая теория полных множеств. В настоящей статье построен некоторый такой критерий. Для этого нам пришлось найти нестандартное описание класса $\mathcal{NP}$, естественное, впрочем, с точки зрения классической теории рекурсии и представляющее, по нашему мнению, самостоятельный интерес.

Полученные результаты расширяют указанную аналогию между классом $\mathcal{NP}$ множеств и классом рекурсивно перечислимых множеств (р.п.м) как в от-

* Частично поддержана грантом №GSU051239 Международной научно-образовательной программы Сороса (ISSEP).

ношении критериев полноты, так и в отношении способа представления проблем класса $\mathcal{NP}$ и, в частности, проблем, полных относительно $\leq_{pol}$.

Основным объектом теории рекурсивных функций является множество частичных вычислимых арифметических функций $\varphi_z\colon \mathbb{N}^n \to \mathbb{N}$, $z \in \mathbb{N}$, где z называется индексом (или номером) частично рекурсивной функции φ_z и является номером ее программы w в фиксированной нумерации всех возможных программ для выбранного алгоритмического языка. Поскольку мы будем иметь дело непосредственно со словарными функциями, то удобно считать индексом функции также слово w. Таким образом, φ_w обозначает далее функцию φ_z, если z есть стандартный номер программы w.

Неопределяемые в статье термины и обозначения можно найти в [1, 2]. Мы используем следующие обозначения: $\| w \|$ — длина слова w; если w есть n-ка $\langle v_1, \ldots, v_n \rangle$ слов, то $\| w \| \rightleftharpoons \| v_1 \| + \ldots + \| v_n \|$; Σ^* — множество всех конечных слов в выбранном конечном алфавите Σ, где $(,), \cdot, 0, 1, @ \in \Sigma$ и $\Omega \notin \Sigma$, а в остальном Σ произволен. Положим $\mathbb{V} = (\Sigma \setminus \{(, \cdot,)\})^*$, $W^+ = W \cup \{\Omega\}$ для любого $W \subseteq \Sigma^*$ и $\mathbb{U} = (\Sigma^*)^+$.

Будем рассматривать вычислимые частичные словарные функции $\psi : \mathbb{U}^n \to \mathbb{U}$. Предполагаем, что программы нашего алгоритмического языка написаны в алфавите Σ и вычисляют ограничения функций ψ на $(\Sigma^*)^n$.

Пусть $t_w(w)$ — время вычисления $\varphi_w(u)$ по программе w, $T_w(u) = \max(\| u \|, t_w(u))$, $\operatorname{Arg} \varphi$ — область определения, $\operatorname{Val} \varphi$ — множество значений функции φ.

Определим следующие классы функций:

$AP = \{\varphi \mid \exists w (\exists p \in \mathbb{P})(\forall u \in \Sigma^*)[(\varphi(u) \text{ определено}) \ \& \ \varphi = \varphi_w \ \& \ T_w(u) \leq p(\| u \|)]\}$;

$VP = \{\varphi \mid \exists w (\exists p \in \mathbb{P})(\forall u \in \operatorname{Arg} \varphi)[\varphi = \varphi_w \ \& \ T_w(u) \leq p(\| \varphi(u) \|)]\}$,

$AVP = AP \cap VP$.

Если $\varphi \in VP(AP, AVP)$ и $w \in \Sigma^*$, $p \in \mathbb{P}$ таковы, что $\varphi = \varphi_w$ и соответствующие условия из определения $VP(AP, AVP)$ выполнены для φ_w и p, то будем говорить, что p есть ассоциированный полином φ, а w — свидетель принадлежности φ соответствующему классу.

Очевидно, что классы AP, VP, AVP замкнуты относительно суперпозиции.

Характеристическая функция множества W обозначается далее через C_W.

Определим массовую проблему выполнимости (или распознавания) как тройку $\langle W^+, \varphi, V^+ \rangle$, где $W, V \subset \mathbb{V}$, $C_W, C_V \in AP$, $\varphi \in VP$ и, наконец, $\varphi^{-1}(\Omega) = \{\Omega\}$. Тогда каждое $u \in V$ определяет частную задачу $W^+ \cap \varphi^{-1}(v) \neq \varnothing$? этой массовой проблемы. (Введение множеств W и V вместо рассмотрения одного и того же универсума (например $\mathbb{V}$) вызвано соображениями удобства кодирования для конкретных приложений).

Теорема 1. *Каждая массовая проблема распознавания (в смысле данного нами определения) принадлежит классу $\mathcal{NP}$. Обратно, каждую проблему из класса $\mathcal{NP}$ можно представить в указанном виде.*

Доказательство. Пусть $\langle W^+, \varphi, V^+ \rangle$ — данная проблема распознавания и p_φ, p_W, p_V — ассоциированные полиномы для φ, C_W, C_V соответственно. Тогда $\| w \| \leq p_\varphi(\| v \|)$ истинно для любого $w \in \varphi^{-1}(v)$. Кроме того, чтобы вычис-

лить $\varphi(w)$, $C_V(v)$, $C_W(w)$, необходимо не больше, чем $p_W(p_\varphi(\|v\|)) + p_\varphi(\|v\|) + p_V(v)$ времени.

Обратно, как известно [2], произвольное множество $L \in \mathcal{NP}$ слов в алфавите $\Sigma_1 = \Sigma\setminus\{(,\cdot,), @\}$ можно представить в виде $\{v \mid \exists w\,[(w, v) \in M' \;\&\; \|w\| \le p(\|v\|)]\}$ для подходящих полинома p и множества $M' \in \mathcal{P}$, слова — элементы пар которого записаны в том же алфавите Σ_1. Рассмотрим $M \in \mathcal{P}$ такое, что любое $u \in M$ имеет вид $w@v$, $(w, v) \in M'$. Тогда $L = \{v \mid \exists w\,[w@v \in M \;\&\; \|w\| \le p(\|v\|)]\}$. Определим $M_p = \{w@v \mid w@v \in M \;\&\; \|w\| \le p(\|v\|)]\}$ и построим функцию φ:

$$\varphi(u) = \begin{cases} v, & \text{если } u = w@v,\ w@v \in M_P; \\ \Omega, & \text{если } u = \Omega; \\ \uparrow & \text{— в остальных случаях.} \end{cases}$$

Тогда $\varphi \in VP$ и $v \in L \Leftrightarrow v \ne \Omega \;\&\; \varphi^{-1}(v) \ne \varnothing$. Осталось положить $V = (\Sigma_1^*)^+$, $W = \mathbb{V}^+$. Теорема доказана.

Пусть $\bar{z}$ обозначает унарный код 1^{z+1} числа $z \in \mathbb{N}$. Если $p = a_0 + a_1x + \ldots + a_nx^n$, то пусть $\hat{p}$ обозначает слово $\overline{a_0}0\overline{a_1}0\ldots0\overline{a_n}$ и $\hat{\mathbb{P}} = \{\hat{p} \mid p \in \mathbb{P}\}$.

Отображение ν^F катенации $\hat{\mathbb{P}}\{@\}\Sigma^*$ множеств $\hat{\mathbb{P}}$, $\{@\}$, Σ^* в множество функций $F \in \{VP, AP\}$ будем называть нумерацией F, если каждый элемент F имеет прообраз. $\nu^F_{\hat{p}@w}$ обозначает функцию $\varphi \in F$ с номером (индексом) $\hat{p}@w$, где слово w является программой φ и p — ее ассоциированный полином.

В [4] показано, что существует вычислимая нумерация класса AP. Обозначим некоторую такую нумерацию через ν^{AP}.

Лемма. *Существует вычислимая нумерация ν^{VP} класса VP.*

Доказательство. Предлагается следующий алгоритм вычисления $\nu^{VP}_{\hat{p}@w}$ на входе u. Запустим программу w на u и отметим в унарном алфавите время $T_w(u)$. Если $\varphi_w(u)\downarrow$, то проверим неравенство $T_w(u) \le p(\|\varphi_w(u)\|)$. Если оно выполнено, результатом возьмем $\varphi_w(u)$, иначе — $1^{T_w(u)}$. Все это можно сделать за время, ограниченное значением некоторого фиксированного полинома на $T_w(u) + \|\hat{p}\| + \|w\|$. Поэтому $\nu^{VP}_{\hat{p}@w} \in VP$. Если $\varphi_w \in VP$ и p — ассоциированный полином для φ_w, то $\nu^{VP}_{\hat{p}@w} = \varphi_w$. В обоих случаях некоторый ассоциированный полином для $\nu^{VP}_{\hat{p}@w}$ можно найти эффективно. Лемма доказана.

Пусть $F \in \{AP, VP\}$, $\theta \in F$. Будем говорить, что θ является полуверсальной для класса F, если существуют функции $\alpha, \beta : (\hat{\mathbb{P}}\{@\}\Sigma^*) \times \Sigma^* \to \Sigma^*$, для которых верно, что: 1) α, β принадлежат AVP как функции второго аргумента для всех значений первого аргумента; 2) $\beta(\hat{p}@w, \nu^{VP}_{\hat{p}@w}(v)) = \theta(\alpha(\hat{p}@w, v))$, $v \in \Sigma^*$.

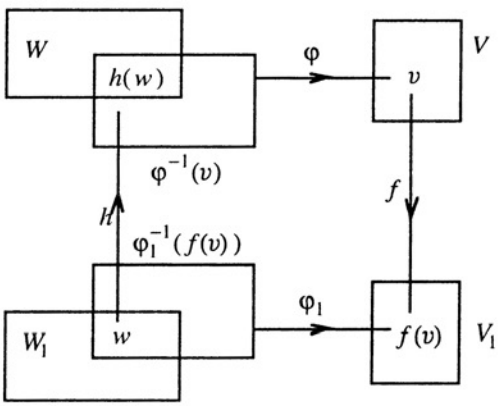
Проиллюстрируем определение диаграммой:

$$\begin{array}{ccc} \Sigma^* & \xrightarrow{\alpha(\hat{p}\,@\,w,\cdot)} & \Sigma^* \\ \Big\downarrow \nu^F_{\hat{p}\,@\,w}(\cdot) & & \Big\downarrow \theta(\cdot) \\ \Sigma^* & \xrightarrow{\beta(\hat{p}\,@\,w,\cdot)} & \Sigma^* \end{array}$$

Проблема $\langle W^+, \varphi, V^+\rangle$ называется $m\mathbb{P}$-сводимой к проблеме $\langle W_1^+, \varphi_1, V_1^+\rangle$, если существует функция $f \in AP$ такая, что $f(\Omega) = \Omega, f(V) \subseteq V_1$ и $(\forall v \in sV)[\varphi^{-1}(v) \cap W \neq \varnothing \Leftrightarrow \varphi_1^{-1}(f(v)) \cap W_1 \neq \varnothing]$.

Далее, проблема $\langle W^+, \varphi, V^+\rangle$ $cm\mathbb{P}$-сводится к $\langle W_1, \varphi_1, V_1\rangle$, если существуют такие $f, h \in AP$, что: i) $f(\Omega) = h(\Omega) = \Omega$, $f(V) \subseteq V_1$, $h(W_1) \subseteq W$;

ii) $(\forall v \in V)\, \forall w[\{\varphi^{-1}(v) \cap W \neq \varnothing \Rightarrow \varphi_1^{-1}(f(v)) \cap W_1 \neq \varnothing\}$ & $(w \in W_1 \cap \varphi_1^{-1}(f(v)) \Leftrightarrow h(w) \in \varphi^{-1}(v) \cap W)]$ (см. рисунок).



Если, кроме того, выполнено условие iii) f есть 1-1-функция на V и h является 1-1-функцией на $\varphi_1^{-1}(f(v))$, $v \in V$, то говорим, что $\langle W^+, \varphi, V^+\rangle$ $c1\mathbb{P}$-сводится к $\langle W_1^+, \varphi_1, V_1^+\rangle$.

Теорема 2. *Существует такая полуверсальная функция* φ *для* VP, *что проблема* $\langle \mathbb{V}^+, \varphi, \mathbb{V}^+\rangle$ *является* $c1\mathbb{P}$-*полной проблемой распознавания (т.е. любая проблема распознавания* $c1\mathbb{P}$-*сводится к проблеме распознавания* $\langle \mathbb{V}^+, \varphi, \mathbb{V}^+\rangle$).

Доказательство. Для произвольных $p \in \mathbb{P}$, $w, v \in (\Sigma\backslash\{@\})^*$ определим $\alpha(\hat{p}\,@w, v) = \hat{p}\,@w@v$, $\beta(\hat{p}\,@w, v) = \hat{p}\,@w@v@\overline{p(\|w\|)}$ и

$$\varphi(v) = \begin{cases} \hat{p}\,@\,w\,@\,\nu^{VP}_{\hat{p}\,@\,w}(u)\,@\,\overline{p\left(\left\|\nu^{VP}_{\hat{p}\,@\,w}(u)\right\|\right)}, & \text{если } v = \hat{p}\,@\,w\,@\,u; \\ \Omega, & \text{если } v = \Omega; \\ \uparrow & \text{— в остальных случаях.} \end{cases}$$

Нетрудно проверить, что $\alpha(\hat{p}\,@w, \cdot)$, $\beta(\hat{p}\,@w, \cdot)$ являются 1-1-функциями из AVP для каждых $p \in \mathbb{P}$, $w, v \in (\Sigma\backslash\{@\})^*$, а $\varphi \in VP$ потому, что можно за время, ограниченное значениями подходящего полинома на $p(\|(u)\|)$, вычислить $\overline{p(\|u\|)}$ [5].

Теперь пусть $\langle W \cup \{\Omega\}, \gamma, V \cup \{\Omega\}\rangle$ — данная проблема распознавания. Мы сначала ограничим область определения γ до W, получая $\gamma' \in VP$. Тогда $\gamma^{-1}(v) \cap W \neq \varnothing \Leftrightarrow (\gamma')^{-1}(v) \neq \varnothing$. Для $\hat{q}, m$ таких, что $\gamma' = \nu^{VP}_{\hat{q}@m}$, определим $\alpha'(v) = \alpha(\hat{q}@m, v), \beta'(v) = \beta(\hat{q}@m, v)$. Легко проверить, что $\varphi(\alpha'(v)) = \beta'(\gamma'(v))$, $v \in (\Sigma\setminus\{@\})^*$.

Пусть $v \in V$, $w \in (\gamma')^{-1}(v)$. Тогда $\gamma(w) = v$, $w \in W$ и $\varphi(\alpha'(w)) = \beta'(\gamma(w))$, т. е. $\varphi^{-1}(\beta'(v)) \neq \varnothing$. Следовательно, $W \cap \gamma^{-1}(v) \neq \varnothing \Rightarrow \Sigma^* \cap \varphi^{-1}(\beta'(v)) \neq \varnothing$.

Теперь предположим, что $t \in \varphi^{-1}(\beta'(v))$. Так как $\varphi(t)\downarrow$, слово t имеет вид $\hat{p}@w@u$ и $\varphi(t) = \hat{p}@w@\nu^{VP}_{\hat{q}@m}(u)@\overline{\hat{p}(\|\nu^{VP}_{\hat{q}@m}(u)\|)}$. По определению β' получаем $\hat{p} = \hat{q}$, $w = m$, и далее $\nu^{VP}_{\hat{q}@m} = \gamma'$, $v = \gamma'(u)$. Поэтому мы можем выбрать следующую функцию из AVP:

$$h'(u) = \begin{cases} (\alpha')^{-1}(u), & \text{если } u \in \{\hat{q}@m@t \mid t \in \Sigma^*\}; \\ \Omega & \text{— в противном случае} \end{cases}$$

как функцию h из определения $c1\mathbb{P}$-сведения. Здесь β' играет роль f. Теорема доказана.

Теорема 3. *Пусть $\theta \in VP$ — унарная функция и $\theta^{-1}(\Omega) = \Omega$. (Проблема распознавания $\langle \mathbb{V}^+, \theta, \mathbb{V}^+\rangle$ является $m\mathbb{P}$-полной) $\Leftrightarrow$ (существует такая функция $h\colon \hat{\mathbb{P}}\{@\}\Sigma^* \times \Sigma^* \to \Sigma^*$, что $\lambda v.[h(\hat{p}@w, v)] \in AP$ и*

$$(\forall \hat{p}@w)\{(\nu^{VP}_{\hat{p}@w})^{-1}(\hat{p}@w) \neq \varnothing \Leftrightarrow \theta^{-1}h(\hat{p}@w, \hat{p}@w) \neq \varnothing\}).$$

Доказательство. $\Rightarrow$. Пусть $\langle \mathbb{V}^+, \theta, \mathbb{V}^+\rangle$ является $m\mathbb{P}$-полной и ψ — полуверсальной функцией VP. В соответствии с определением $m\mathbb{P}$-полноты существует $f \in AP$ такая, что $\langle \mathbb{V}^+, \psi, \mathbb{V}^+\rangle \leq^f_{m\mathbb{P}} \langle \mathbb{V}^+, \theta, \mathbb{V}^+\rangle$, т. е. $\forall v[\psi^{-1}(v) \neq \varnothing \Leftrightarrow \theta^{-1}(f(v)) \neq \varnothing]$. Принимая во внимание $\beta(\hat{p}@w, \nu^{VP}_{\hat{p}@w}(u)) = \psi(\alpha(\hat{p}@w, u))$ для подходящих функций α, β, имеем $(\nu^{VP}_{\hat{p}@w})^{-1}(v) \neq \varnothing \Leftrightarrow \psi^{-1}\beta(\hat{p}@w, v) \neq \varnothing \Leftrightarrow \theta^{-1}(f(\beta(\hat{p}@w, v))) \neq \varnothing$. Следовательно, можно положить $v = \hat{p}@w$.

$\Leftarrow$. Определим следующую словарную функцию g:

$$\varphi_{g(y,\hat{p}@w,\hat{q}@v)}(u) = \begin{cases} \hat{q}@\nu^{AP}_{\hat{q}@y}(y, \hat{p}@w, \hat{q}@v), & \text{если } \nu^{VP}_{\hat{p}@w}(u) = v; \\ \uparrow & \text{— в противном случае.} \end{cases}$$

Будем считать, что g получена применением построения из классической s-m-n-теоремы. Пусть n будет программой для g. Так как n не зависит от параметров этой схемы, легко выбрать $q \in \mathbb{P}$ таким образом, что $g = \nu^{AP}_{\hat{q}@n}$. Тогда получаем

$$\varphi_{g(n,\hat{p}@w,\hat{q}@v)}(u) = \begin{cases} \hat{q}@g(n, \hat{p}@w, \hat{q}@v), & \text{если } \nu^{VP}_{\hat{p}@w}(u) = v; \\ \uparrow & \text{— в противном случае.} \end{cases}$$

Анализируя построение из s-m-n-теоремы, замечаем, что программу $g(n, \hat{p}@w, v, \hat{q})$ можно выбрать с условиями: $\lambda v.g(n, \hat{p}@w, v, \hat{q}) \in AP$, ее длина не меньше, чем $\|v\|$, и равномерно ограничена значением некоторой линейной

функции на сумме длин всех аргументов g. Тогда $\varphi_{g(n,\hat{p}@w,\hat{q}@v)} \in VP$. Можно выбрать полином q с дополнительным условием $\varphi_{g(n,\hat{p}@w,\hat{q}@v)} = \nu^{VP}_{\hat{q}@g(n,\hat{p}@w,\hat{q}@v)}$, где q не зависит от v. Теперь $(\nu^{VP}_{\hat{p}@w})^{-1}(v) \neq \varnothing \Leftrightarrow \Leftrightarrow \varphi^{-1}_{g(n,\hat{p}@w,\hat{q}@v)}(\hat{q}@g(n, \hat{p}@w, \hat{q}@v)) \neq \varnothing \Leftrightarrow (\nu^{VP}_{\hat{q}@g(n,\hat{p}@w,\hat{q}@v)})^{-1}(\hat{q}@g(n, \hat{p}@w, \hat{q}@v)) \neq \varnothing \Leftrightarrow \theta^{-1}(h(\hat{q}@g(n, \hat{p}@w, \hat{q}@v), \hat{q}@g(n, \hat{p}@w, \hat{q}@v)) \neq \varnothing$ Теорема доказана.

1. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. – М.:Мир, 1972. – 624 с.
2. *Гери М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. – М.:Мир, 1982. – 416 с.
3. *Стокмейер Л.* Классификация вычислительной сложности проблем// Киберн. сб. Новая. сер. – 1989. – Вып. 26. – С. 20 – 83.
4. *Cobham A.* The intrinistic computational difficulty of functions // Proc. 1964. Int. Congr. Logic Methodol. and Phyl. Sci. – North-Holland, 1964. – P. 24 – 30.
5. *Ямада Х.* Вычисления в реальное время и рекурсивные функции, невычислимые в реальное время // Проблемы мат. логики. – М.:Мир, 1970. – С.139 – 155.

Получено 28.10.96