ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 510.52

АЛГОРИТМИЧЕСКАЯ СЛОЖНОСТЬ NP-ТРУДНЫХ МНОЖЕСТВ[1]

Дудаков С.М.
Кафедра информатики

Поступила в редакцию 07.04.2009, после переработки 05.06.2009.

Работа усиливает результаты, ранее полученные в работах Дехтяря. Показано, что колмогоровская алгоритмическая сложность распознавания начального отрезка длины n **NP**-трудного по Тьюрингу множества не может быть меньше $O(\lg\lg n)$, если $\mathbf{NP} \neq \mathbf{P}$.

We strengthen results of Dekhtyar. The paper contains a new result on structure of **NP**-hard sets. We prove that the kolmogorov recognition complexity (with polynomially bound time) of **NP**-hard sets (with polynomial Turing reducibility) can't be less than $O(\lg\lg n)$ if $\mathbf{NP} \neq \mathbf{P}$ for initial segment with n elements.

Ключевые слова: сводимость, **NP**-трудное множество, алгоритмическая сложность.
Keywords: reducibility, **NP**-hard set, information content.

Введение

В данной работе исследуются некоторые общие свойства трудноразрешимых проблем, связанные с их внутренней структурой и алгоритмической сложностью. Теория алгоритмической сложности была создана в работах Колмогорова, Соломонова, Чейтина и их учеников. Основы этой теории и ее современное состояние изложены в [1] и [9]. Работа [5] посвящена исследованию алгоритмической сложности рекурсивных множеств при ограничении на время вычисления. [3, 7] представляют собой обзоры результатов по структурной теории сложности. Так в [8] показано, что если есть **NP**-полное редкое множество, то все высшие классы полиномиальной иерархии совпадают с Δ_2^P. В [2] показано, что при $\mathbf{P} \neq \mathbf{NP}$ не существует трудных по Тьюрингу для **NP** множеств, имеющих очень низкую алгоритмическую сложность: меньше $k \lg\lg\lg n$ для начального отрезка множества длины n.

В нашей работе получен результат о структуре трудных множеств, который является усилением результата из [2] и отвечает на открытый вопрос из этой работы: «Для произвольного $k \in \omega$ любое **NP**-трудное множество имеет сложность

[1]Работа выполнена при финансовой поддержке РФФИ, проекты 07-01-00637 и 08-01-00241.

распознавания при полиномиальном ограничении на время вычисления большую чем $k \lg\lg n$ для $A^{(n)}$ в бесконечном числе точек, если только $\mathbf{P} \neq \mathbf{NP}$.»

1. Определения

С помощью записи вида $\mathfrak{M}^{()}$ обозначаем машину Тьюринга, имеющую некоторый оракул. Напомним, что машина Тьюринга с оракулом — это двухленточная машина. Оракул — множество, состоящее из натуральных чисел. Одна из лент используется обычным образом, а вторая предназначена для вопросов. Чтобы задать вопрос, машина пишет на второй ленте натуральное число и переходит в специальное состояние $q_?$. На следующем шаге она оказывается в одном из состояний q_+ или q_- в зависимости от того, принадлежит записанное число оракулу или нет. Для конкретного оракула, например, B пишем $\mathfrak{M}^{(B)}$.

Напомним, что **NP** — класс множеств натуральных чисел, распознаваемых на недетерминированных машинах Тьюринга за полиномиальное относительно длины входа время, а **P** — на детерминированных. Будем полагать, что для записи данных используется двоичная система.

Определение 1 (см.[4]). *Пусть $A, B \subseteq \omega$. Множество A* сводится по Тьюрингу *к множеству B за полиномиальное время ($\leq_T^P$-сводимость), если существует машина Тьюринга с оракулом $\mathfrak{N}$ такая, что $\mathfrak{N}^{(B)}$ работает полиномиальное время на любом входе и*

$$(\forall x \in \omega)(x \in A \iff \mathfrak{N}^{(B)} \text{ принимает } x).$$

Обозначение $A \leq_T^P B$.

Далее везде при упоминании сводимости будут подразумеваться $\leq_T^P$-сводимость, поскольку других мы не рассматриваем. **NP**-трудной называется задача, к которой сводится любая задача из **NP**.

Будем отождествлять множество $A \subseteq \omega$ с последовательностью нулей и единиц $(a_i)_{i\in\omega}$, где

$$a_i = 1 \iff i \in A.$$

С помощью $A^{(n)}$ обозначаем начальный фрагмент последовательности длины n. С помощью $|x|$ обозначаем длину слова x или двоичной записи числа x.

Зафиксируем некоторую вычислимую нумерацию машин Тьюринга: $\mathfrak{M}_i$, то есть такую, что существует универсальная машина Тьюринга $\mathfrak{M}^*$, для которой $\mathfrak{M}^*(i,j) = \mathfrak{M}_i(j)$.

Определение 2 (см.[1]). *Пусть $x = x_0 \dots x_{n-1}$ — входное слово, t — некоторая функция. Тогда*

$$M^t_{\mathfrak{M}}(x) = \min\{|i| : (\forall j < n)(\mathfrak{M}_i \text{ принимает } j \text{ за время } t(|i|) \iff x_j = 1)\} -$$

алгоритмическая сложность распознавания *слова x при ограничении t на время вычисления.*

Один из основных фактов в теории алгоритмической сложности состоит в существовании оптимальных нумераций, мы будем использовать его в следующем виде:

Теорема (см., например, [1]). *Существует нумерация машин $(\mathfrak{N}_i)_{i\in\omega}$ такая, что для любой нумерации машин $(\mathfrak{M}_i)_{i\in\omega}$ существует полином q и для всех x выполнено*

$$M^{q(t)}_{\mathfrak{N}}(x) \le M^{t}_{\mathfrak{M}}(x) + c,$$

причем константа c не зависит от x.

Если задана последовательность A, то по ней однозначно определяется функция следующим образом: $n \mapsto M^t_{\mathfrak{M}}(A^{(n)})$. Мы будем называть эту функцию сложностью распознавания последовательности A при ограничении на время t. Если f — произвольная функция, то будем писать $M^P_{\mathfrak{M}}(A^{(n)}) \le f(n)$, если $M^q_{\mathfrak{M}}\left(A^{(n)}\right) \le f(n)$ для некоторого полинома q почти для всех n. Заметим, что $M^P_A \le \mathrm{const}$ тогда и только тогда, когда множество A распознаваемо за полиномиальное время.

Поскольку алгоритмическая сложность при полиномиальном или более слабом ограничении на время вычисления и на память относительно оптимальных нумераций инвариантна (с точностью до некоторых констант), то в дальнейшем для такой сложности будем писать M^P, не указывая интерпретатор.

2. Основной результат

Теорема 1. *Пусть A — **NP**-трудное множество и $\mathbf{P} \ne \mathbf{NP}$. Тогда $M^P(A) \ge k \lg\lg n$ для всякого $k \in \omega$ для бесконечно многих n.*

Доказательство. Предположим обратное. Пусть A — это **NP**-трудное множество, и вместе с тем существует $k \in \omega$ такое, что $M^P\left(A^{(n)}\right) \le k \lg\lg n$ почти для всех n. Мы покажем, что в этом случае любое множество $B \in \mathbf{NP}$ можно распознать за полиномиальное время.

Для доказательства мы используем технику, предложенную в [6]. С помощью $\langle x, y\rangle$ обозначим функцию, нумерующую пары натуральных чисел обычным образом:

$$\langle x, y\rangle = \frac{(x+y)(x+y+1)}{2} + y.$$

Заметим, что эта функция полиномиально ограничена:

$$|\langle x, y\rangle| \le p(|x|, |y|)$$

для некоторого полинома p.

Пусть $M^p\left(A^{(n)}\right) \le k \lg\lg n$ для полинома p почти для всех n. Так как $B \in \mathbf{NP}$, то существует множество $W \in \mathbf{P}$ и полином r такие, что

$$B = \Big\{ x \in \omega : (\exists y)\big[|y| \le r(|x|) \text{ и } \langle x, y\rangle \in W\big] \Big\}.$$

Пусть

$$L_B = \Big\{ \langle x, z\rangle : (\exists y)\big[|y| \le r(|x|) \text{ и } z \le y \text{ и } \langle x, y\rangle \in W\big] \Big\}.$$

Очевидно, $L_B \in \mathbf{NP}$, следовательно, L_B распознается некоторой машиной Тьюринга с оракулом $\mathfrak{N}^{(A)}$, работающей не больше $s(|x|)$ шагов для некоторого полинома s на любом входе x.

Пусть дано x — натуральное число. Введем обозначение

$$y_{\max} = \max\{z \in \omega : \langle x, z\rangle \in L_B\},$$

если множество в скобках не пусто. В противном случае $y_{\max}$ не существует. Тогда

$$x \in B \iff [y_{\max} \text{ существует}].$$

Кроме того очевидно, что если $y_{\max}$ существует, то $\langle x, y_{\max}\rangle \in W$.

Так как $\mathfrak{N}^{(A)}$ работает полиномиальное время, то она задает оракулу вопросы, длина которых не превосходит $s(|x| + |z|)$. Но поскольку из $\langle x, z\rangle \in L_B$ следует, что $|z| \leq r(|x|)$, то можно считать, что длина вопросов не превосходит $s(r(|x|))$.

Для каждого оракула C определим множество

$$Z^{(C)}(x) = \left\{z \in \left[0, 2^{r(|x|)}\right] : \mathfrak{N}^{(C)} \text{ принимает } \langle x, z\rangle\right\}$$

и число $y^{(C)}$, получаемое в результате двоичного поиска максимального в $Z^{(C)}(x)$ элемента. Заметим, что поскольку $Z^{(C)}(x)$ может не являться начальным сегментом $\left[0, 2^{r(|x|)}\right]$, то и $y^{(C)}$ не всегда будет максимальным элементом $Z^{(C)}(x)$. Однако, $Z^{(A)}(x)$ — начальный сегмент $\left[0, 2^{r(|x|)}\right]$, следовательно, $y_{\max} = y^{(A)}$, если $y_{\max}$ существует.

Так как

$$M^p\left(A \cap \left[0, 2^{s(r(|x|))}\right]\right) \leq k \lg\lg\left(2^{s(r(|x|))}\right) = k \lg s(r(|x|)) = \lg s(r(|x|))^k,$$

то существует не больше чем

$$2^{M^p\left(A \cap \left[0, 2^{s(r(|x|))}\right]\right)} \leq s(r(|x|))^k$$

машин Тьюринга, среди которых мы должны искать машину, распознающую начальный сегмент A. Пусть C_j — множество распознаваемое машиной $\mathfrak{M}_j, j \in \left[0, s(r(|x|))^k\right]$ за время $p(s(r(|x|)))$. Для каждого $j \in \left[0, s(r(|x|))^k\right]$ найдем $y^{(C_j)}$, что также можно сделать за полиномиальное время. Поскольку

$$A^{\left(2^{s(r(|x|))}\right)} \in \left\{C_j^{\left(2^{s(r(|x|))}\right)} : j \in \left[0, s(r(|x|))^k\right]\right\},$$

то

$$y_{\max} \in \left\{y^{(C_j)} : j \in \left[0, s(r(|x|))^k\right]\right\},$$

если $y_{\max}$ существует. Если хотя бы для одного $j \in \left[0, s(r(|x|))^k\right]$ имеет место $\left\langle x, y^{(C_j)}\right\rangle \in W$, то, очевидно, $x \in B$ (по определению W). Если же для всех $j \in \left[0, s(r(|x|))^k\right]$ имеет место $\left\langle x, y^{(C_j)}\right\rangle \notin W$, то $y_{\max}$ не определен, и, следовательно, $x \notin B$. □

Из этой теоремы сразу получается следствие.

Следствие 2. *Пусть $A \subseteq \left\{2^{2^n} - 1 : n \in \omega\right\}$. Тогда A не является* **NP***-трудной по Тьюрингу проблемой, если* $\mathbf{P} \neq \mathbf{NP}$.

Доказательство. Предположим, что существует **NP**-трудное по Тьюрингу множество A указанного вида. Пусть

$$a_n = \begin{cases} 1, & \text{если } 2^{2^n} - 1 \in A, \\ 0, & \text{иначе.} \end{cases}$$

Очевидно, что в слове $x_n = a_0 a_1 \dots a_{\lg\lg n}$ заключена вся информация о начальном отрезке A длины n, и $A^{(n)}$ легко распознается за полиномиальное время при известном x_n. Следовательно,

$$M^P\left(A^{(n)}\right) \le \lg\lg n + \text{const}$$

почти для всех n. Поскольку константа не существенна, то по теореме из **NP**-трудности A следует, что $\mathbf{P} = \mathbf{NP}$. Противоречие. □

Данное следствие является непосредственным усилением теоремы 6 из [2] и отвечает на один из открытых вопросов из [2].

Список литературы

[1] Агафонов В.Н. Сложность алгоритмов и вычислений. Ч.2. — Новосибирск: НГУ, 1975. — 146 с.

[2] Дехтярь М.И. О сводимости к «редким» множествам и плотности **NP**-полных задач. // Автоматы, алгорифмы, языки. Межвузовский тематический сборник — Калинин: КГУ, 1982. — С.42–52.

[3] Buhrman H., Torenvliet L. On the structure of complete sets // 9th Structural complexity theory. Int.conf. (Amsterdam, Holland, 1994) — Amsterdam, 1994. — P.118–133.

[4] Cook S.A. The complexity of theorem proving procedures // Proc. of the 3rd Ann. ACM Symp. on theory of computing. Int.conf. (Ohio, USA, 1971) — New-York, 1971. — P.151–158.

[5] Dekhtyar' M.I. Complexity spectra of recursive sets and approximability of initial segments of complete problems. // Elektronische Informationsverarbeitung Kybernetik. — 1979. Vol.15, №1. — P.11–32.

[6] Homer S., Longpré L. On reductions of **NP** sets to sparse sets // 6th Structural complexity theory. Int.conf. (Chicago, USA, 1991) — Chicago, 1991. — P.79–88.

[7] Complexity theory. Retrospective II. / Hemachandra L. A., Selman A. L. — New-York: Springer-Verlag, 1997. — 339 p.

[8] Kadin J. $\mathbf{P}^{\mathbf{NP}[\log n]}$ and sparse Turing complete sets of **NP** // Journal of Computer and System Sciences. — 1989. Vol.39, № 3. — P.282–298.

[9] Li M., Vitányi P. An Introduction to Kolmogorov Complexity and its Application. — New-York: Springer, 2008. — 729 p.