Доклады Академии наук СССР
1974. Том 214, № 5

УДК 51.01+518.5

МАТЕМАТИКА

М. И. ДЕХТЯРЬ

О СЛОЖНОСТИ ОТНОСИТЕЛЬНЫХ ВЫЧИСЛЕНИЙ

(Представлено академиком А. Д. Александровым 18 VI 1973)

В теории алгоритмов важное место занимает изучение иерархий множеств натуральных чисел, связанных с эффективной сводимостью одного множества к другому. Ограничение сложности сводящих алгоритмов позволяет классифицировать в аналогичных терминах рекурсивные множества (р.м.), которые с точки зрения эффективной сводимости не различаются. При этом естественно возникают вопросы о зависимости сложности вычисления одних предикатов от выбора других предикатов в качестве оракулов. Эти вопросы изучались в работах ([1–3]). В частности, непосредственным следствием теоремы Б. А. Трахтенброта о неавтосводимых р.м. ([2]) является существование пары р.м. A и B, каждое из которых в качестве оракула не уменьшает сложности вычисления другого (это аналог известной теоремы Мучника — Фридберга о существовании пары несравнимых в смысле сводимости по Тьюрингу рекурсивно-перечислимых множеств).

В настоящей работе рассматриваются следующие вопросы:

1) Насколько может упроститься вычисление за счет привлечения оракула и как точно можно контролировать уменьшение сложности, выбирая тот или иной оракул?

2) Для всякого ли р.м. A существуют такие нетривиальные (например, сколь угодно сложные) р.м. B, что A и B не помогают вычислению друг друга?

Ниже уточняются понятия относительного вычисления, его сложности, помощи, оказываемой одним множеством вычислению другого. Теорема 1 отвечает на первый вопрос, теоремы 2 и 3 связаны со вторым.

Мы рассматриваем следующий вариант машин Тьюринга с оракулами. Каждая машина $\mathfrak{M}$ имеет четыре правосторонние ленты: входную, выходную, ленту для вопросов оракулу и рабочую. Первые три имеют двоичный алфавит (0, 1, Λ — пустой символ), рабочая лента имеет некоторый конечный алфавит, зависящий от машины. Головки на входной и выходной лентах не могут двигаться влево, причем головка на входе не может писать, а на выходе читать. Кроме обычных состояний $\mathfrak{M}$ имеет специальное вопросительное состояние $q_?$ и два выделенных состояния q_0, q_1. Работая с оракулом A (A — некоторое множество) и попав в вопросительное состояние $q_?$, $\mathfrak{M}$ переходит за один такт в одно из выделенных состояний q_0, q_1 в зависимости от того, принадлежит или не принадлежит число, записанное в этот момент на ленте, для вопросов множеству A. Обозначим через $\varphi_{\mathfrak{M}}^{(A)}$ функцию, вычисляемую машиной $\mathfrak{M}$ с оракулом A. Сложность вычисления этой функции будем характеризовать емкостной сигнализирующей $s_{\mathfrak{M}}^{(A)}(x)$ машины $\mathfrak{M}$ с оракулом A, равной максимальному числу ячеек, используемых на каждой из четырех лент $\mathfrak{M}$ при вычислении $\varphi_{\mathfrak{M}}^{(A)}(x)$, если $\varphi_{\mathfrak{M}}^{(A)}(x)$ определена, и не определенной в противном случае.

Пусть $\{\mathfrak{M}_i\}$ — гёделевская нумерация машин Тьюринга с оракулами. Для произвольного множества A и числа i через $\varphi_i^{(A)}$ обозначим функцию, вычисляемую $\mathfrak{M}_i$ с оракулом A, а через $s_i^{(A)}$ — емкостную сигнализирующую этой машины. Если $A=\phi$, то будем говорить, что соответствующие вычисления проводятся без оракула, и вместо $\varphi_i^{(\phi)}$, $s_i^{(\phi)}$ писать φ_i, s_i.

Через c_A обозначим характеристическую функцию множества A.

Если A и B — два множества, то через $M_A^{(B)}$ обозначим множество всех

общерекурсивных функций (о.р.ф.), которые являются верхними границами сложности вычислений A относительно B:

$$M_A^{(B)}=\{f \mid f\text{—о.р.ф.}\&\exists i\forall x\ [\varphi_i^{(B)}(x)=c_A(x)\&s_i^{(B)}(x)\leqslant f(x)]\}.$$

Множество всех нижних границ сложности вычислений A относительно B обозначим $\overline{M}_A^{(B)}$:

$$\overline{M}_A^{(B)}=\{f \mid f\text{—о.р.ф.}\&f\notin M_A^{(B)}\}.$$

Функции из $\overline{M}_A^{(B)}$ являются нижними границами сложности в следующем смысле: емкостная сигнализирующая всякого вычисления A с оракулом B в бесконечном числе точек превосходит любую о.р.ф. f из $\overline{M}_A^{(B)}$.

Пусть $M_A=M_A^{(\phi)}$, $\overline{M}_A=\overline{M}_A^{(\phi)}$.

Определение. Множество B помогает вычислению множества A, если существует функция f такая, что $f\in\overline{M}_A$ и $f\in\overline{M}_A^{(B)}$.

Для любого р.м. A существуют оракулы, которые не помогают вычислению A (например ϕ), и оракулы, использование которых позволяет вычислить A с минимальной емкостью (в качестве такого оракула можно взять само A). Следующий результат показывает, что существуют сколь угодно сложные р.м. A, размер помощи которым за счет выбора подходящего оракула можно контролировать достаточно точно.

Теорема 1. *Для произвольной о.р.ф. f существуют такое р.м. A, и константа c, что $\forall h\in M_A$, $\forall x^{\infty}\ [h(x)\geqslant f(x)]$ *, и для всякой емкостной сигнализирующей g, не превосходящей f, существует р.м. B такое, что:*

1) *существует вычисление A с оракулом B, сложность которого не превосходит g, т. е. $g\in\overline{M}_A^{(B)}$;*

2) *всякое вычисление A с оракулом B почти во всех точках сложнее $g(x)-c$:*

$$\forall j\ [(\varphi_j^{(B)}=c_A)\to\forall x^{\infty}\ (s_j^{(B)}(x)\geqslant g(x)-c)].$$

Замечание. Вычисление не всякого сложного множества можно улучшить с точностью, гарантируемой утверждениями 1) и 2) теоремы 1. Именно, существуют о.р.ф. f, емкостные сигнализирующие g, g_1 и р.м. A такие, что:

а) $\forall h\in M_A$, $\forall x^{\infty}\ [h(x)\geqslant f(x)]$;

б) $\forall x\ [f(x)>g(x)\geqslant g_1(x)]$;

в) $\overline{\lim\limits_{x\to\infty}}\dfrac{g_1(x)}{g(x)}=0$;

г) для любого р.м. B такого, что существует вычисление A с оракулом B сложности не больше g, найдется вычисление A с тем же оракулом сложности не больше g_1, т.е. $g\in M_A^{(B)}\leftrightarrow g_1\in M_A^{(B)}$.

Из в) и г) следует, что для таких A, f и g утверждение 2) теоремы 1 не выполняется ни при каком выборе константы c.

В ([3]) показано, что для всякого р.м. A и произвольной нижней границы сложности $\bar{f}\in\overline{M}_A$ найдутся сколь угодно сложные р.м. B**, которые сохраняют эту нижнюю границу, т. е. $f\in\overline{M}_A^{(B)}$. Теорема 2 описывает некоторый класс множеств сохраняющих произвольное фиксированное перечислимое множество $F=\{f_i\}$ нижних границ сложности р.м. A.

Определение. Пусть $\varepsilon(x)$ — произвольная всюду определенная функция. Множество B называется ε-редким, если $|B\cap[0,\ x]|\leqslant\varepsilon(x)$ для бесконечного числа точек x.

---

* $\overset{\infty}{\forall}x\mathfrak{A}(x)$ означает: «для всех x, за исключением, быть может, конечного числа, справедливо $\mathfrak{A}(x)$».

** Утверждение «существуют сколь угодно сложные р.м. B со свойством $\mathfrak{A}(B)$» означает, что для всякой о.р.ф. f найдется рядом р.м. B такое, что $\forall h\in M_B$, $\forall^{\infty}x\ [h(x)\geqslant f(x)]$ и $\mathfrak{A}(B)$.

Теорема 2. *Для любых р.м. A и перечислимого множества о.р.ф. $F=\{f_i\}$ таких, что $f_i\in\overline{M}_A$ для каждого i, существует о.р.ф. $\varepsilon(x)$ со следующими свойствами*:

1) $\varepsilon(x)$ — *неубывающая, неограниченная функция;*

2) *всякое ε-редкое множество B сохраняет нижние границы сложности A из F, т. е. $f_i\in\overline{M}_A^{(B)}$ для каждого i.*

Для любой о.р.ф. $\varepsilon(x)$, удовлетворяющей утверждению 1) теоремы 2, класс ε-редких множеств достаточно широк. В частности, существуют сколь угодно сложные ε-редкие рекурсивные множества ([4]). Среди них имеются и такие, вычислению которых A не помогает.

Теорема 3. *Для любых р.м. A и перечислимого множества о.р.ф. $F=\{f_i\}$ таких, что $f_i\in\overline{M}_A$ для каждого i, существует сколь угодно сложное р.м. B такое, что*:

1) *B сохраняет нижние границы сложности A из F, т. е. $f_i\in\overline{M}_A^{(B)}$ для каждого i;*

2) *A не помогает вычислению B.*

Замечание. Множество $\overline{M}_A$ всех нижних границ сложности любого р.м. A неперечислимо. Поэтому теоремы 2 и 3 нельзя непосредственно использовать для построения р.м. B такого, что A и B не помогают вычислению друг друга.

Если же рассматривать рекурсивно-перечислимые множества, то теорема 2 позволяет обнаружить среди них оракулы, не помогающие вычислению рекурсивных множеств.

Следствие. а) *Для произвольных р.м. A, о.р.ф. f и гиперпростого множества B, если $f\in\overline{M}_A$, то $f\in\overline{M}_A^{(B)}$.* б) *Во всякой рекурсивно-перечислимой нерекурсивной T-степени содержится рекурсивно-перечислимое множество, не помогающее вычислению никакого рекурсивного множества.*

Для табличных (tt-) степеней утверждение, аналогичное следствию б), неверно. Справедливо простое

Предложение. *Для каждого tt-полного множества B существует такая о.р.ф. f, что для любого р.м. A, если $f\in\overline{M}_A$, то B помогает A (т. е. B помогает всем достаточно сложным рекурсивным множествам).*

Из следствия а) и этого предложения получается, в частности, теорема Поста о табличной неполноте гиперпростых множеств.

Отметим, что все приведенные результаты могут быть распространены на произвольные меры сложности относительных вычислений ([3]) с помощью стандартной техники мажорирования. Например, теорема 3 примет следующий вид:

Теорема 3′ *Для произвольной меры сложности относительных вычислений $\{\Phi_i^{(\ )}\}$ существует о.р.ф. $g^{(2)}$ такая, что для любых р.м. A и перечислимого множества о.р.ф. $F=\{f_i\}$, для которых $g^{(2)}(x, f_i(x))\in\overline{M}'_A$ для каждого i, существует сколь угодно сложное р.м. B такое, что*:

1) *$f_i\in\overline{M}_A^{\prime(B)}$ для каждого i;*

2) *A не помогает B.*

(*Здесь* $M_A^{\prime(B)}=\{f\mid f-\text{о.р.ф.}\&\exists i[(\varphi_i^{(B)}=c_A)\&\forall_x^{\infty}(\Phi_i^{(B)}(x)\leqslant f(x))]\}$.)

В заключение автор благодарит Б. А. Трахтенброта и М. К. Валиева за полезное обсуждение работы.

Институт математики
Сибирского отделения Академии наук СССР
Новосибирск

Поступило
12 VI 1973

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Дж. Ходжаев, Вопросы кибернетики и вычислительной математики, Ташкент, **33**, 38 (1969). [2] Б. А. Трахтенброт, ДАН, **192**, № 6, 1224 (1970). [3] N. A. Lynch, Relativisation of the Theory of Computational Complexity, Proj. MAC Techn. Rep., 99 (1972). [4] Б. А. Трахтенброт, Алгебра и логика, Семинар, **4**, 5, 79 (1965).