Доклады Академии наук СССР
1970. Том 192, № 6

УДК 51.01+518.5 *МАТЕМАТИКА*

Б. А. ТРАХТЕНБРОТ

ОБ АВТОСВОДИМОСТИ

(Представлено академиком П. С. Новиковым 15 XII 1969)

1°. Введение. В данной работе определяется и изучается понятие автосводимости (неавтосводимости), которое, как нам кажется, естественным образом уточняет интуитивное представление о взаимной зависимости (о взаимной независимости) индивидуальных задач, составляющих некоторую массовую проблему. Рассмотрим, например, проблему распознавания выводимости в некоторой формальной теории T, построенной обычным образом средствами логики предикатов. Быть может эта проблема алгоритмически неразрешима; существует, однако, эффективная процедура (в нашей терминологии — автосведение), дающая правильный ответ на каждый вопрос «выводима ли формула $\mathfrak{A}$?», если только считаются известными ответы для других формул, отличных от $\mathfrak{A}$. Например, достаточно привлечь информацию о выводимости или невыводимости $\neg\neg\mathfrak{A}$. Допустим теперь, что для нашей теории T выводимость эффективно распознаваема, а следовательно, нужные ответы можно находить при помощи прямых вычислений (без автосведения). Могло, однако, оказаться, что при этом невозможно обойтись без сложных вычислений (обычно так оно и есть); указанная же выше процедура автосведения является очень простой.

Конечно, априори могут существовать алгоритмически неразрешимые проблемы, для которых невозможно автосведение (неавтосводимые проблемы), а также алгоритмически разрешимые проблемы, для которых невозможно автосведение существенно более простое, чем безусловные разрешающие алгоритмы.

Такие ситуации можно интерпретировать как проявление независимости индивидуальных задач массовой проблемы друг от друга.

В дальнейшем под массовой проблемой мы понимаем, как это принято в теории алгоритмов, проблему вхождения в некоторое множество G натуральных чисел, и основное внимание мы уделяем рекурсивно перечислимым (р.п.) множествам или их дополнениям. В п. 2° приведены определения, связанные с автосводимостью, а также с формализацией понятия случайной последовательности (коллектива Мизеса), принадлежащей А. Н. Колмогорову (2) и Д. В. Лавлэнду (3); отсюда видно, что неавтосводимость является свойством более слабым (и, значит, и более общим), чем случайность. В п. 3° выясняется, какие автосводимые и неавтосводимые множества существуют в классе р.п. множеств. В п. 4° для рекурсивных множеств сравнивается сложность вычисления со сложностью автосведения. Результаты, близкие к теореме 2 этого пункта, но имеющие более частный характер, содержатся в работе Дж. Ходжаева (7). Наконец, в п. 5° кратко обсуждается связь автосводимости с понятиями внутрисводимости * и равномерной внутрисводимости (4).

2°. Пусть G — произвольное множество натуральных чисел, Γ — его характеристическая функция (предикат), или, что то же самое, соответствующая последовательность из единиц и нулей:

$$\Gamma(1), \Gamma(2), \ldots, \Gamma(n), \ldots \tag{1}$$

* В РЖМат 7А72, 1969 г. термин «introreducible» переведен как самосводимый; мы же предпочитаем более точный перевод внутрисводимый. (Самосводимый можно было бы использовать как синоним для автосводимый.)

В терминах машин с оракулом ((1), стр. 130) можно формализовать понятие стратегии (допустимой системы) угадывания и стратегии (допустимой системы) выбора следующим образом.

Стратегией угадывания называется машина $\mathfrak{M}$ с оракулом, удовлетворяющая условию: каковы бы ни были оракул G и натуральное число n, будучи запущенной на аргументе n, машина $\mathfrak{M}$ никогда не обращается к оракулу с вопросом «$n \in G$?» (хотя и может задавать любые вопросы «$\nu \in G$?» при $\nu \neq n$).

Стратегией выбора называется машина $\mathfrak{M}$ с оракулом, которая, будучи запущенной на пустой ленте, записывает на ней (в некотором стандартном коде) зависящую от оракула последовательность (конечную или бесконечную) неповторяющихся натуральных чисел

$$i_1, i_2, \ldots, i_k, \ldots \tag{2}$$

с соблюдением условия: каковы бы ни были оракул G и натуральное k, вплоть до завершения записи числа i_k машина не обращается к оракулу с вопросом «$i_k \in G$?».

При этом о последовательности из нулей и единиц

$$\Gamma(i_1), \Gamma(i_2), \ldots, \Gamma(i_k), \ldots \tag{3}$$

говорят, что она выделена из последовательности (1) посредством стратегии выбора $\mathfrak{M}$.

Множество G называется автосводимым, если оно обладает автосведением, т. е. стратегией угадывания, которая, будучи снабжена оракулом G, вычисляет для каждого n значение $\Gamma(n)$; в противном случае G неавтосводимо.

Как известно, в соответствии с концепцией Мизеса последовательность (1) объявляется коллективом, как случайной последовательностью, если выполнены условия: 1) в ней существует предел относительной частоты единиц; 2) этот предел сохраняется для каждой бесконечной последовательности (3), выделяемой из (1) посредством стратегии выбора *.

В дальнейшем при употреблении указанной выше терминологии мы не будем различать между собой множество G, последовательность (1), предикат Γ или соответствующую проблему вхождения (например, случайное множество G, автосводимая последовательность $\Gamma(1), \Gamma(2), \ldots$ и т. п.).

Следующее утверждение почти очевидно:

Если последовательность (1) автосводима, то существует стратегия выбора, выделяющая из нее бесконечную последовательность (3), сплошь лежащую в G или в его дополнении. Следовательно, всякое случайное множество неавтосводимо.

3°. Свойство автосводимости рекурсивно инвариантно. Однако оно не инвариантно относительно m-эквивалентности. Для любого множества G существует m-эквивалентное ему множество G', которое автосводимо (и вдобавок процесс автосведения очень прост). Именно, G' можно определить условием:

$$\forall n [2n \in G' \equiv 2n + 1 \in G' \equiv n \in G]. \tag{4}$$

С другой стороны, любое утверждение о существовании случайных множеств автоматически является также теоремой существования неавтосводимых множеств. Так, например, в (3) устанавливается, что в классе Клини — Мостовского $\Sigma_2 \cap \Pi_2$ существуют случайные (а значит и неавтосводимые) множества. Однако, поскольку случайное множество не может быть рекурсивно перечислимым и даже не может быть получено из р.п. множеств посредством булевых операций, то это нам не дает никакой информации

* Напомним, что первоначальная формализация концепции Мизеса принадлежит Черчу; она основана на определении стратегии выбора, отличном от употребляемого нами определения Колмогорова — Лавлэнда и выделяющем более узкий класс стратегий.

относительно р.п. множеств (или, что то же самое, относительно множеств с р.п. дополнением). На самом же деле посредством двух подходящих диагональных конструкций можно обнаружить существование неавтосводимых р.п. множеств двух взаимно исключающих друг друга типов.

Теорема 1. (А). *Существует неавтосводимое множество G с р.п. дополнением, которое не иммунно (т. е. G содержит бесконечное р.п. множество).*

(В). *Существует неавтосводимое множество G с р.п. дополнением, удовлетворяющее условию: никакая стратегия выбора не может выделить из G бесконечного р.п. подмножества.* (*)

Заметим, что условие (*) сильнее чем обычная иммунность.

Нерешенные задачи. (I). Существует ли для каждого нерекурсивного множества (и, в частности, для каждого нерекурсивного р.п. множества) такое m-эквивалентное (таблично-эквивалентное, тьюрингово-эквивалентное, . . .) множество, которое неавтосводимо?

(II). Описать «естественные» массовые проблемы, которые неавтосводимы. (Во введении уже отмечались автосводимость распознавания логической выводимости; это относится и к проблеме тождества теории групп и т. п.)

4°. Мы будем оценивать сложность вычислений и автосведений посредством емкостных сигнализирующих ([5]). Напомним некоторые определения, относящиеся к обычным машинам Тьюринга, а также к машинам Тьюринга с оракулом. Емкостная сигнализирующая $s_{\mathfrak{M}}(n)$ указывает для обычной машины $\mathfrak{M}$ число ячеек, используемых $\mathfrak{M}$, коль скоро она запущена на аргументе n, заданном в унарной записи (n-палочек). Аналогичный смысл имеет $s_{\mathfrak{M}\Gamma}(n)$ для машины, снабженной оракулом Γ. Всюду определенная функция $h(n)$ называется емкостной, если она совпадает с $s_{\mathfrak{M}}(n)$ для некоторой обычной машины $\mathfrak{M}$.

Теорема 2. *Для любой емкостной функции h существует предикат Γ, удовлетворяющий условиям:*

1) (верхняя оценка вычисления). *Существует машина $\mathfrak{N}$, вычисляющая Γ и такая, что $\forall n[s_{\mathfrak{N}}(n) = h(n)]$.*

2 (нижняя оценка автосведения). *Пусть стратегия угадывания $\mathfrak{M}$ вычисляет Γ; тогда существует константа c такая, что*

$$\forall n\,[s_{\mathfrak{M}\Gamma}(n) \geqslant ch(n)].$$

Иначе говоря, существуют эффективные массовые проблемы любой сложности h, которые не допускают автосведений существенно более простых, чем безусловные их вычисления.

Ранее уже было замечено (см. введение и множества G', определяемые условием (4)), что существуют массовые проблемы с очень простым автосведением. Однако это имело место в связи с тривиальной взаимной зависимостью индивидуальных задач (например, выводимость $\mathfrak{A}$, выводимость $\neg\neg\mathfrak{A}$, $2n \in G' \equiv 2n+1 \in G'$).

Следующая теорема, усиливающая результат из ([6]), обнаруживает нетривиальную ситуацию взаимной зависимости, исключающую «трюки» вышеуказанного типа.

Теорема 3. *Для каждой строго монотонной емкостной функции h существует предикат Γ, удовлетворяющий условиям:*

(I) (верхняя оценка вычисления). *Существует машина $\mathfrak{N}$, вычисляющая Γ и такая, что $\forall n[s_{\mathfrak{N}}(n) = h(n)]$.*

(II) (нижняя оценка вычисления). *Для любой машины $\mathfrak{M}$, вычисляющей Γ, существует константа c такая, что*

$$\forall n\,[s_{\mathfrak{M}}(n) \geqslant ch(n)].$$

(III) (верхняя оценка автосведения). *Существуют стратегия угадывания Ω, вычисляющая Γ, и константа d такие, что*

$$\forall n[s_{\Omega\Gamma}(n) \leqslant h(n)] \quad \exists^{\infty} n[s_{\Omega\Gamma}(n) \leqslant dn].$$

Остается невыясненным вопрос: сохраняет ли силу теорема 3, если утверждение $\exists^\infty n[s_{\Omega\Gamma}(n) \leqslant dn]$ заменить более сильным утверждением $\forall n[s_{\Omega\Gamma}(n) \leqslant dn]$?

5°. Напомним следующие определения (см. ([4])).

Множество M называется внутрисводимым (introreducible), если оно сводимо к любому своему бесконечному подмножеству.

Множество M равномерно внутрисводимо, если существует такой алгоритм сведения (такая машина с оракулом), который сводит M к любому своему бесконечному подмножеству.

Обозначим через $\mathfrak{R}_{\mathrm{aut}}$, $\mathfrak{R}_{\mathrm{intr}}$, $\mathfrak{R}_{\mathrm{unif}}$ соответственно классы автосводимых, внутрисводимых и равномерно внутрисводимых множеств. Лахлан ([4]) доказал, что

$$\mathfrak{R}_{\mathrm{intr}} \supset \mathfrak{R}_{\mathrm{unif}}.$$

Нетрудно показать, что

$$\mathfrak{R}_{\mathrm{aut}} \supset \mathfrak{R}_{\mathrm{unif}}, \qquad \mathfrak{R}_{\mathrm{intr}} \not\supset \mathfrak{R}_{\mathrm{aut}}.$$

Остается невыясненным вопрос: $\mathfrak{R}_{\mathrm{aut}} \supset \mathfrak{R}_{\mathrm{intr}}$?

Институт математики
Сибирского отделения Академии наук СССР
Новосибирск

Поступило
11 XII 1969

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] H. Rogers jr., Theory of Recursive Functions and Effective Computubility, 1967. [2] A. N. Kolmogorov, Indian J. Statistics, Ser. A, 25, № 4, 369 (1963). [3] D. W. Loveland, Trans. Am. Math. Soc., 125, № 3, 497 (1966). [4] C. G. Jockusch, J. Symb. Logic, 33, № 4, 521 (1968); РЖМат., 7А72 (1969). [5] Б. А. Трахтенброт, Сложность алгоритмов и вычислений, Новосибирск, 1967. [6] Б. А. Трахтенброт, Алгебра и логика, семинар, 4, в. 5, 79 (1965). [7] Дж. Хождаев, Всесоюзн. конф. по проблемам теоретической кибернетики, Тезисы докл., Новосибирск, 1969, стр. 111.