Мальцевские чтения
Новосибирск (2006)
Тезисы докладов

Пример полугруппы с генерически неразрешимой проблемой равенства слов

А. Н. Рыбалов

Классическая теория алгоритмов изучает алгоритмические проблемы *в худшем случае*, рассматривая поведение алгоритмов на всем множестве входов. В Computer Science исследуется также сложность алгоритмов *в среднем*, при этом алгоритм может хорошо (полиномиально) работать на большинстве входных данных и плохо (экспоненциально) на очень редких входах. Генерический подход к алгоритмическим проблемам был впервые предложен в работе [3]. В рамках этого подхода изучается поведение алгоритмов на множестве "почти всех" входов (это множество называется генерическим), игнорируя поведение алгоритма на остальных входах, на которых алгоритм может работать медленно, либо вообще не останавливаться. Такой подход имеет приложения в криптографии, где требуется чтобы алгоритмические проблемы были трудными для "почти всех" входов. В отличие от сложности в среднем, генерический подход применим и для алгоритмически неразрешимых проблем. Например, в работах [1,3] было доказано, что многие классические алгоритмически неразрешимые проблемы алгебры разрешимы в генерическом случае. А в работе [2] было установлено, что проблема остановки для машин Тьюринга с лентой, бесконечной в одну сторону, также генерически разрешима.

Пусть множество A есть множество всех входов для некоторой алгоритмической проблемы, а S – некоторое подмножество A. Множество входов S называется *генерическим*, если

$$\mu(S) = \lim_{n\to\infty} \frac{|S \cap A_n|}{|A_n|} = 1,$$

где A_n — множество всех входов проблемы размера n. Понятие генерического множества формализует интуитивное понятие множества "почти всех" входов в том смысле, что при увеличении размера входа вероятность того, что случайно сгенерированный вход попадет в генерическое множество, стремится к 1. Если входы проблемы являются наборами из A^n, то множество $S = S_1 \times \ldots \times S_n$ называется генерическим, если

$$\mu(S) = \mu(S_1) \ldots \mu(S_n) = 1.$$

Алгоритмическая проблема $\mathcal{A} \subseteq A^n$ генерически разрешима, если существует множество $S \subseteq A^n$ такое, что

1. S генерическое,

2. S разрешимое,
3. $\mathcal{A} \cap S$ разрешимое.

Генерический алгоритм, решающий проблему $\mathcal{A}$, работает следующим образом. Сначала определяет, принадлежит ли вход генерическому множеству. Если да, то проверяет принадлежность входа $\mathcal{A}$ (это возможно согласно п.3). Если нет, то отвечает "НЕ ЗНАЮ". Такой алгоритм правильно решает $\mathcal{A}$ на почти всех входах.

Целью данного доклада является построение полугруппы с генерически неразрешимой проблемой равенства слов. Выберем полугруппу

$$\mathfrak{S} = \langle a_1, \ldots, a_n | R \rangle$$

с алгоритмически неразрешимой проблемой равенства слов. Рассмотрим полугруппу

$$sm(\mathfrak{S}) = \langle a_1, \ldots, a_n, x | R, x = xa_1, \ldots, x = xa_n, x = xx \rangle.$$

Под размером строки над конечным алфавитом понимается ее длина, определение генерического множества дается относительно этого размера.

Теорема. Проблема равенства слов в полугруппе $sm(\mathfrak{S})$ генерически неразрешима.

Список литературы

[1] A.V. Borovik, A.G. Myasnikov, V.N. Remeslennikov. Multiplicative measures on free groups. Internat. J. Algebra Comput., 13 (2003), No. 6, 705–731.

[2] J.D.Hamkins, A.Miasnikov. The halting problem is decidable on a set of asymptotic probability one. To appear in Theoretical Computer Science. Eprint available from http://arxiv.org/abs/math/0504351.

[3] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain. Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 264 (2003), No. 2, 665–694.

E-mail: rybalov@omskreg.ru