Теорема 1. Сложность алгоритма 1 равна $O\left(Ng^{d^N}\right)$, где g и d — некоторые целые числа.

Несмотря на то, что сложность данного алгоритма высокая, он может быть использован для синтаксического анализа применительно к языку программирования, находящемуся в стадии разработки.

ЛИТЕРАТУРА

1. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
2. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.

УДК 510.52 DOI 10.17223/2226308X/13/33

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ПРЕДСТАВИМОСТИ НАТУРАЛЬНЫХ ЧИСЕЛ СУММОЙ ДВУХ КВАДРАТОВ

А. Н. Рыбалов

Изучается генерическая сложность проблемы представимости натуральных чисел суммой двух квадратов. Эта проблема, восходящая ещё к Ферма и Эйлеру, тесно связана с проблемами факторизации целых чисел и распознавания квадратичности вычетов по составным модулям, для решения которых не известно эффективных алгоритмов. Доказывается, что, при условии трудноразрешимости этой проблемы в худшем случае и P = BPP, для её решения не существует полиномиального сильно генерического алгоритма. Сильно генерический алгоритм решает проблему не на всём множестве входов, а на подмножестве, последовательность относительных плотностей которого при увеличении размера экспоненциально быстро сходится к 1.

Ключевые слова: *генерическая сложность, суммы квадратов, диофантовы уравнения.*

Введение

Проблема представимости натуральных чисел суммой двух квадратов состоит в том, чтобы по любому заданному натуральному числу N определить, разрешимо ли в натуральных числах диофантово уравнение $x^2 + y^2 = N$. Эта задача восходит ещё к Ферма, который в 1640 г. сформулировал (см. [1, 2]) следующее красивое утверждение: любое простое число вида $p = 4n + 1$ представимо в виде суммы квадратов двух натуральных чисел. Эта гипотеза впоследствие была доказана Эйлером и называется теперь теоремой Ферма — Эйлера [1, 2]. В дальнейшем был получен критерий Ферма — Эйлера разрешимости диофантова уравнения $x^2 + y^2 = N$ для любого натурального N. Однако этот критерий сводит проблему к задаче факторизации (разложения на множители) целых чисел, которая на текщий момент считается трудноразрешимой [3]. Таким образом, критерий Ферма — Эйлера не может быть проверен эффективно (за полиномиальное от размера входа время).

Генерический подход к алгоритмическим проблемам предложен в [4]. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют генерическое множество. Понятие «почти все» формализуется введением естественной меры на

множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов. Классическим примером такого алгоритма является симплекс-метод — он за полиномиальное время решает задачу линейного программирования для большинства входных данных, но имеет экспоненциальную сложность в худшем случае. Более того, может так оказаться, что проблема трудноразрешима или вообще неразрешима в классическом смысле, но легкоразрешима на генерическом множестве.

В данной работе изучается генерическая сложность проблемы представимости натуральных чисел суммой двух квадратов. Доказывается, что если проблема трудноразрешима в худшем случае и P = BPP, то для неё не существует полиномиального сильно генерического алгоритма. Класс BPP состоит из проблем, разрешимых за полиномиальное время на вероятностных машинах Тьюринга. Одной из важных гипотез в теории сложности вычислений является гипотеза о совпадении классов P и BPP. Из неё следует, что любой полиномиальный вероятностный алгоритм $\mathcal{A}$ можно эффективно дерандомизировать, то есть построить полиномиальный алгоритм $\mathcal{B}$, не использующий генератор случайных чисел и решающий ту же проблему, что и алгоритм $\mathcal{A}$. В работе [5] доказано, что равенство P = BPP следует из весьма правдоподобных гипотез о вычислительной сложности некоторых трудных проблем.

1. Генерические алгоритмы

Пусть I — некоторое множество входов. Для подмножества $S \subseteq I$ определим *последовательность относительных плотностей*

$$\rho_n(S) = \frac{|S_n|}{|I_n|},\ n = 1, 2, 3, \ldots,$$

где I_n — множество входов размера n; $S_n = S \cap I_n$. Заметим, что $\rho_n(S)$ — это вероятность попасть в S при случайной и равновероятной генерации входов из I_n. В данной работе множеством входов для алгоритмов является множество натуральных чисел, записанных в двоичной форме. Под размером натурального числа понимается длина его двоичной записи.

Асимптотической плотностью множества S назовём верхний предел

$$\rho(S) = \overline{\lim_{n\to\infty}} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Следуя [4], назовём множество S *сильно пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 0, т. е. существуют константы σ, $0 < \sigma < 1$, и $C > 0$, такие, что $\rho_n(S) < C\sigma^n$ для любого n. Теперь S называется *сильно генерическим*, если его дополнение $I \setminus S$ сильно пренебрежимо.

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется (*сильно*) *генерическим*, если

1) $\mathcal{A}$ останавливается на всех входах из I;
2) множество $\{x \in I : \mathcal{A}(x) \neq ?\}$ является (сильно) генерическим.

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если $(\mathcal{A}(x) = y \in J) \Rightarrow$ $\Rightarrow (f(x) = y)$ для всех $x \in I$. Ситуация $\mathcal{A}(x) = ?$ означает, что $\mathcal{A}$ не может вычислить функцию f на аргументе x. Но условие 2 гарантирует, что $\mathcal{A}$ корректно вычисляет f на

почти всех входах (входах из генерического множества). Множество $S \subseteq I$ называется (*сильно*) *генерически разрешимым за полиномиальное время*, если существует (сильно) генерический полиномиальный алгоритм, вычисляющий его характеристическую функцию.

2. Проблема представимости натуральных чисел суммой двух квадратов

Проблема представимости натуральных чисел суммой двух квадратов состоит в следующем. Дано натуральное число N, записанное в двоичной системе. Нужно определить, разрешимо ли в натуральных числах диофантово уравнение $x^2 + y^2 = N$. Классический критерий Ферма — Эйлера [1, 2] связывает эту проблему с известной проблемой факторизации целых чисел.

Теорема 1 (Ферма, Эйлер). Пусть N — натуральное число. Диофантово уравнение $N = x^2 + y^2$ разрешимо в натуральных числах тогда и только тогда, когда каждый простой делитель N вида $4k + 3$ входит в разложение N в чётной степени.

Если бы проблема факторизации решалась эффективно, то этот критерий давал бы эффективный алгоритм для проблемы представимости натуральных чисел суммой двух квадратов. Однако до сих пор неизвестно эффективных алгоритмов для проблемы факторизации [3]. Кроме того, проблема представимости натуральных чисел суммой двух квадратов тесно связана с проблемой распознавания квадратичности вычетов по составным модулям, которая тоже считается трудноразрешимой [3].

3. Основные результаты

Теорема 2. Если существует сильно генерический полиномиальный алгоритм, решающий проблему представимости натуральных чисел суммой двух квадратов, то существует вероятностный полиномиальный алгоритм, разрешающий эту проблему на всём множестве входов.

Теорема 3. Если проблема представимости натуральных чисел суммой двух квадратов не лежит в классе P и P = BPP, то не существует сильно генерического полиномиального алгоритма для этой проблемы.

ЛИТЕРАТУРА

1. *Dickson L. E.* History of the Theory of Numbers. V. II. N.Y.: Dover Publications, 2005. 803 p.
2. *Сендеров В., Спивак А.* Суммы квадратов и целые гауссовы числа // Квант. 1999. № 3. С. 14–22.
3. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II // Proc. First Intern. Symp. Algorithmic Number Theory. N.Y., USA, May 6–9, 1994. P. 291–322.
4. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
5. *Impagliazzo R. and Wigderson A.* P = BPP unless E has subexponential circuits: Derandomizing the XOR Lemma. Proc. 29th STOC. El Paso: ACM, 1997. P. 220–229.