Теорема 1. Для функции, заданной коммутативным образом уравнения (1), имеет место разложение в ряд Лорана

$$z(x) = \sum_{k_2+\ldots+k_n\geqslant 1} (-1)^k \frac{(2k_2+\ldots+nk_n)!}{((n-1)k_n+\ldots+k_2+1)!k_2!\ldots k_n!} \times$$
$$\times x_0^{(n-1)k_n+\ldots+k_2+1} x_1^{-nk_n-\ldots-2k_2-1} x_2^{k_2} \cdot \ldots \cdot x_n^{k_n}.$$

Поскольку в формуле решения степени переменной x_1 отрицательные, то решение исходного некоммутативного уравнения (1) в виде ФСР невозможно, таким образом, имеет место следующее

Следствие 1. Полиномиальная грамматика, порождённая уравнением (1), не имеет решения (не порождает полиномиального языка).

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.
3. *Егорушкин О. И., Колбасина И. В., Сафонов К. В.* О совместности систем символьных полиномиальных уравнений и их приложении // Прикладная дискретная математика. Приложение. 2016. №9. С. 119–121.
4. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166–172.
5. *Семёнов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Докл. АН СССР. 1973. №212. С. 50–52.
6. *Safonov K. V.* On power series of algebraic and rational functions in C^n // J. Math. Analysis Appl. 2000. V. 243. P. 261–277.

УДК 510.52 DOI 10.17223/2226308X/14/41

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ИЗОМОРФИЗМА КОНЕЧНЫХ ПОЛУГРУПП

А. Н. Рыбалов

Изучается генерическая сложность проблемы изоморфизма конечных полугрупп: по любым двум полугруппам одинакового порядка, заданным таблицами умножения, требуется определить, являются ли они изоморфными. К этой проблеме полиномиально сводится проблема изоморфизма конечных графов. Таким образом, проблема изоморфизма конечных полугрупп с вычислительной точки зрения не проще проблемы изоморфизма графов. Предлагается генерический полиномиальный алгоритм для проблемы изоморфизма конечных полугрупп. В его основе лежит характеризация почти всех конечных полугрупп как 3-нильпотентных полугрупп специального вида, а также полиномиальный алгоритм Боллобаша, решающий проблему изоморфизма для почти всех сильно разреженных графов.

Ключевые слова: *генерическая сложность, конечные полугруппы, изоморфизм.*

Введение

Понятие изоморфизма является одним из важнейших понятий в современной математике. Изоморфные объекты имеют одинаковые математические свойства, одинаковую математическую структуру. Это позволяет абстрагироваться от конкретных представителей этих объектов, однако это также порождает проблему изоморфизма: по двум конкретным представлениям определить, являются ли они изоморфными. Наиболее известной алгоритмической проблемой такого рода является проблема изоморфизма конечных графов. Несмотря на то, что эта проблема находится в центре внимания специалистов с 1970-х гг., до сих пор не найдено полиномиальных алгоритмов её решения. В то же время не доказана её NP-полнота. Таким образом, она может занимать промежуточное положение между проблемами из класса P и NP-полными проблемами. Проблема изоморфизма возникает для многих других конечных алгебраических объектов: групп, полугрупп, колец, полей, алгебр и т. д. Например, для конечных полей эта проблема решается тривиально: известно, что любые два конечных поля одинакового порядка изоморфны. Для конечных полугрупп ситуация гораздо сложнее. Простой алгоритм, который перебирает всевозможные биекции между полугруппами и проверяет, являются ли эти биекции изоморфизмами, работает за экспоненциальное время. Существуют ли полиномиальные алгоритмы для решения этой проблемы, неизвестно. В [1] доказано, что к этой проблеме полиномиально сводится проблема изоморфизма конечных графов. Таким образом, проблема изоморфизма конечных полугрупп с вычислительной точки зрения не проще проблемы изоморфизма конечных графов.

В рамках генерического подхода [2] 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.

В данной работе предлагается генерический полиномиальный алгоритм для проблемы изоморфизма конечных полугрупп. В его основе лежит характеризация почти всех конечных полугрупп как 3-нильпотентных полугрупп специального вида, установленная в [3], а также полиномиальный алгоритм Боллобаша, решающий проблему изоморфизма для почти всех сильно разреженных графов [4].

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.

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.

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

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

Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если

$$\forall x \in I \ (\mathcal{A}(x) = y \in J) \Rightarrow (f(x) = y).$$

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 *генерически разрешимым за полиномиальное время*, если существует генерический полиномиальный алгоритм, вычисляющий его характеристическую функцию.

2. Проблема изоморфизма конечных полугрупп

Для определённости будем рассматривать конечные полугруппы с элементами из множеств $\{1, 2, \ldots, n\}$, $n \in \mathbb{N}$. *Таблицей умножения* конечной полугруппы S порядка n называется таблица $n \times n$, в которой на месте (i, j) стоит результат произведения элементов i и j.

Полугруппы S_1 и S_2 *изоморфны*, если существует биекция $\varphi : S_1 \to S_2$, такая, что для любых элементов $a, b \in S_1$ имеет место $\varphi(ab) = \varphi(a)\varphi(b)$. Биекция φ называется *изоморфизмом*. *Проблема изоморфизма конечных полугрупп* состоит в следующем: даны две конечные полугруппы S_1 и S_2 одинакового порядка, заданные таблицами умножения; определить, являются ли они изоморфными.

Теорема 1. Проблема изоморфизма конечных полугрупп генерически разрешима за полиномиальное время.

ЛИТЕРАТУРА

1. *Земляченко В. Н., Корнеенко Н. М., Тышкевич Р. И.* Проблема изоморфизма графов // Записки научных семинаров ЛОМИ. 1982. Т. 118. С. 83–158.
2. *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.
3. *Kleitman D. J., Rothschild B. R., and Spencer J. H.* The number of semigroups of order n // Proc. Amer. Math. Soc. 1976. V. 55. No. 1. P. 227–232.
4. *Bollobas B.* Distinguishing of vertices of random graphs // Ann. Discr. Math. 1982. V. 13. P. 33–50.