МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ИЗОМОРФИЗМА КОНЕЧНЫХ ПОЛУГРУПП[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

Изучается генерическая сложность проблемы изоморфизма конечных полугрупп. В этой проблеме по любым двум полугруппам одинакового порядка, заданным таблицами умножения, требуется определить, являются ли они изоморфными. В. Н. Земляченко, Н. М. Корнеенко и Р. И. Тышкевич в 1982 г. доказали, что к этой проблеме полиномиально сводится проблема изоморфизма конечных графов — известная алгоритмическая проблема, которая активно изучается с 1970-х годов и для которой до сих пор неизвестно полиномиальных алгоритмов. 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, установленная Д. Клейтманом, Б. Ротшильдом и Дж. Спенсером, а также полиномиальный алгоритм Боллобаша, решающий проблему изоморфизма для почти всех сильно разреженных графов.

Ключевые слова: *генерическая сложность, конечные полугруппы, проблема изоморфизма.*

DOI 10.17223/20710410/51/6

ON GENERIC COMPLEXITY OF THE ISOMORPHISM PROBLEM FOR FINITE SEMIGROUPS

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: alexander.rybalov@gmail.com

Generic-case approach to algorithmic problems was suggested by A. Miasnikov, V. Kapovich, P. Schupp, and V. Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. In this paper, we study the generic complexity of the isomorphism problem for finite semigroups. In this problem, for any two semigroups of the same order, given by their multiplication tables, it is required to determine whether they are isomorphic. V. Zemlyachenko, N. Korneenko, and R. Tyshkevich in 1982 proved that the graph

[1]Исследование поддержано Программой фундаментальных научных исследований СО РАН I.1.1.4, проект № 0314-2019-0004.

isomorphism problem polynomially reduces to this problem. The graph isomorphism problem is a well-known algorithmic problem that has been actively studied since the 1970s, and for which polynomial algorithms are still unknown. So from a computational point of view the studied problem is no simpler than the graph isomorphism problem. We present a generic polynomial algorithm for the isomorphism problem of finite semigroups. It is based on the characterization of almost all finite semigroups as 3-nilpotent semigroups of a special form, established by D. Kleitman, B. Rothschild, and J. Spencer, as well as the Bollobas polynomial algorithm, which solves the isomorphism problem for almost all strongly sparse graphs.

Keywords: *generic complexity, finite semigroups, isomorphism problem.*

Введение

Понятие изоморфизма является одним из важнейших понятий в современной математике. Изоморфные объекты имеют одинаковые математические свойства и одинаковую математическую структуру, что позволяет абстрагироваться от конкретных представителей этих объектов, однако это также порождает проблему изоморфизма: по двум конкретным представлениям определить, являются ли они изоморфными. Наиболее известная алгоритмическая проблема такого рода — проблема изоморфизма конечных графов. Несмотря на то, что эта проблема находится в центре внимания специалистов с 1970-х годов, до сих пор для неё не найдено полиномиальных алгоритмов. 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 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, введённого в [2], алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое 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 [3] предложен первый полиномиальный генерический алгоритм для проблемы изоморфизма графов, который по каждому графу из пары пытается построить *каноническую разметку* вершин — каждой вершине сопоставляет некоторое натуральное число, её уникальный код. Если это удалось сделать для обоих графов, то алгоритм сравнивает полученные два набора канонических разметок: если они совпадают, то графы изоморфны. Более того, эти метки показывают, как задать сам изоморфизм — здесь он будет единственным. Алгоритм Бабаи — Эрдеша — Селкова [3] может не найти каноническую разметку для некоторых графов, но доля (вероятность) таких графов среди всех графов размера n ограничена $O(1/\sqrt[7]{n})$. В дальнейшем было предложено много эффективных алгоритмов для решения проблемы изоморфизма графов в раз-

личных моделях случайных графов. Б. Боллобаш в [4] предложил полиномиальный алгоритм, решающий эту проблему для почти всех сильно разреженных графов, в которых для графов с n вершинами вероятность $p(n)$ того, что две вершины соединены ребром, удовлетворяет условию $\dfrac{C_1 \ln n}{n} \leqslant p(n) \leqslant \dfrac{C_2}{n^{11/12}}$, где $C_1 > 1$, $0 < C_2 < 1$ — любые константы. Так же как и алгоритм Бабаи — Эрдеша — Селкова, алгоритм Боллобаша пытается сначала построить канонические разметки вершин обоих графов, по которым затем ищет изоморфизм (единственный) между графами, если он существует. Вероятность того, что каноническая разметка не будет найдена для одного графа, оценивается числом n^{-C}, где $C > 0$ — некоторая константа.

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 [5], а также упомянутый полиномиальный алгоритм Боллобаша для почти всех сильно разреженных графов из [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

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

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. Конечные полугруппы

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 называются *изоморфными*, если существует биекция $\varphi : S_1 \to \to S_2$, 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.

Будем говорить, что конечная полугруппа S с основным множеством $\{1, 2, \ldots, n\}$ имеет вид $H(A, \psi, z)$, где $A \subset \{1, 2, \ldots, n\}$, $\psi : A \times A \to \bar{A}$ и $z \in \bar{A}$ (через $\bar{A}$ обозначено дополнение к A), если операция умножения в S определена следующим образом:

$$xy = \begin{cases} \psi(x, y), & \text{если } x, y \in A, \\ z & \text{иначе.} \end{cases}$$

Легко проверяется, что определённая таким образом операция умножения обладает свойством ассоциативности. Элемент z играет роль нуля. Любая полугруппа вида $H(A, \psi, z)$ является 3-нильпотентной. В [5] доказано, что почти все конечные полугруппы являются 3-нильпотентными, более того, имеют вид $H(A, \psi, z)$. Точнее, пусть $\mathcal{S}$ — множество всех конечных полугрупп, $\mathcal{NS}$ — 3-нильпотентные полугруппы вида $H(A, \psi, z)$. Тогда множество $\mathcal{NS}$ является генерическим в $\mathcal{S}$. Доказано также, что почти все полугруппы достаточно большого порядка n имеют вид $H(A, \psi, z)$, где $|A|$ принадлежит интервалу $I_n = (t_0 - 3, t_0 + 3)$, $t_0 = n - n/(2 \ln n)$. Таким образом, если $\mathcal{NS}_n$ — 3-нильпотентные полугруппы вида $H(A, \psi, z)$ порядка n, а $\mathcal{NS}(k)_n$ — полугруппы в $\mathcal{NS}_n$ вида $H(A, \psi, z)$, где $|A| = k$, то множество

$$\bigcup_{n=1}^{\infty} \bigcup_{k \in I_n} \mathcal{NS}(k)_n$$

является генерическим в $\mathcal{S}$.

Заметим, что представление конечной полугруппы в виде $H(A, \psi, z)$ может быть неоднозначным. Это происходит, если $A_1 \subset A_2$ и $\psi(a, b) = z$, когда $a \in A_2 \setminus A_1$ или $b \in A_2 \setminus A_1$. Будем называть представление полугруппы $S = H(A, \psi, z)$ *минимальным*, если не существует множества A', такого, что $S = H(A', \psi', z')$ и $|A'| < |A|$. Обозначим через $\mathcal{NS}'$ множество всех полугрупп из $\mathcal{NS}$ с минимальным представлением, а через $\mathcal{NS}'(k)_n$ — множество всех полугрупп из $\mathcal{NS}(k)_n$ с минимальным представлением. В [5] доказано, что $\mathcal{NS}'$ также является генерическим в $\mathcal{S}$; более того, для любого достаточно большого n и любого $k < n$ имеет место

$$|\mathcal{NS}(k)_n| = (1 + o(1))|\mathcal{NS}'(k)_n|.$$

Отсюда следует, что множество

$$\bigcup_{n=1}^{\infty} \bigcup_{k \in I_n} \mathcal{NS}'(k)_n$$

также является генерическим в $\mathcal{S}$ и

$$\lim_{n \to \infty,\ k \in I_n} \frac{|\mathcal{NS}(k)_n|}{|\mathcal{NS}'(k)_n|} = 1.$$

Лемма 1. Существует генерический полиномиальный алгоритм $\mathcal{A}$, который по произвольной полугруппе S, заданной таблицей умножения, получает её минимальное представление в виде $H(A, \psi, z)$ (если это возможно).

Доказательство. Полиномиальный алгоритм $\mathcal{A}$ работает на полугруппе S следующим образом:

1) Ищет по таблице умножения нуль: такой элемент z, что $za = z$ и $az = z$ для любого $a \in S$.
2) Если нуля нет, выдаёт ответ «?».
3) Ищет все элементы $B = \{b_1, \ldots, b_m\}$, такие, что $ab_i = z$ и $b_i a = z$ для любого $a \in S$. Это гарантирует минимальность представления.
4) Полагает $A = S \setminus (B \cup \{z\})$ и проверяет, верно ли, что для любых $a_1, a_2 \in A$ имеет место $a_1 a_2 \in B$.
5) Если проверка на шаге 4 пройдена, выдаёт множество A, часть таблицы умножения для множества A как задание функции ψ и элемент z как нуль.
6) Если проверка на шаге 4 не пройдена, то выдаёт ответ «?».

Генеричность этого алгоритма следует из результатов Д. Клейтмана, Б. Ротшильда, Дж. Спенсера [5]. ■

Лемма 2. Пусть $S_1 = H(A_1, \psi_1, z_1)$ и $S_2 = H(A_2, \psi_2, z_2)$ — изоморфные полугруппы с минимальными представлениями и φ — изоморфизм между ними. Тогда

1) $\varphi(z_1) = z_2$;
2) ограничение φ на A_1 есть биекция τ между A_1 и A_2, откуда $|A_1| = |A_2|$;
3) ограничение φ на $S_1 \setminus (A_1 \cup \{z_1\})$ есть биекция π между $S_1 \setminus (A_1 \cup \{z_1\})$ и $S_2 \setminus (A_2 \cup \{z_2\})$;
4) биекция π может быть найдена за полиномиальное время по биекции τ.

Доказательство.

1) Для любого $s \in S_1$ имеет место $sz_1 = z_1$, откуда $\varphi(z_1) = \varphi(sz_1) = \varphi(s)\varphi(z_1)$. Так как $\varphi(s)$ при этом пробегает всю полугруппу S_2, элемент $\varphi(z_1)$ является нулем в S_2, то есть $\varphi(z_1) = z_2$.

2) Легко видеть, что для минимального представления $S = H(A, \psi, z)$ имеют место следующие утверждения:

а) $\forall a \in A\ \exists b \in A\ (ab \neq z$ или $ba \neq z)$;

б) $\forall b \notin A\ \forall c \in S\ (bc = cb = z)$.

Из этого следует, что $\varphi(a) \in A_2$ для любого $a \in A_1$, т. е. ограничение φ на A_1 есть биекция τ между A_1 и A_2.

3) Следует из п. 2.

4) Пусть известна биекция τ, являющаяся ограничением некоторого изоморфизма φ между S_1 и S_2 на множество A_1. Обозначим $B_1 = S_1 \setminus (A_1 \cup \{z_1\})$ и $B_2 = S_2 \setminus (A_2 \cup \{z_2\})$. Нужно найти биекцию π между B_1 и B_2, которая является ограничением φ на B_1.

Пусть $\mathrm{Img}(\psi_1) \subseteq S_1 \setminus A_1$ есть образ функции ψ_1. Тогда для любого $b \in B_1$, такого, что $b \in \mathrm{Img}(\psi_1)$, найдутся $a_1, a_2 \in A_1$, такие, что $a_1 a_2 = b$. Поэтому

$$\pi(b) = \varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) = \tau(a_1)\tau(a_2) \in B_2.$$

Таких возможных пар не более, чем квадратичное число от порядка полугрупп, поэтому такой поиск выполняется за полиномиальное время.

Остаётся заметить, что в качестве ограничения искомой биекции π между $B_1 \setminus \mathrm{Img}(\psi_1)$ и $B_2 \setminus \pi(\mathrm{Img}(\psi_1))$ можно выбрать произвольную биекцию между этими множествами. ■

3. Конечные полугруппы и графы

Граф G — это пара (V, E), где V — множество вершин; $E \subseteq V \times V$ — множество рёбер графа G. Таким образом, будем рассматривать ориентированные графы с петлями. Под размером графа $G = (V, E)$ будем понимать число вершин $|V|$. Два графа $G = (V_1, E_1)$ и $H = (V_2, E_2)$ называются *изоморфными*, если $|V_1| = |V_2|$, $|E_1| = |E_2|$ и существует взаимно однозначная функция $f : V_1 \to V_2$, такая, что $(u, v) \in E_1$ тогда и только тогда, когда $(f(u), f(v)) \in E_2$. *Проблема изоморфизма графов* состоит в следующем: заданы два графа G_1 и G_2 одинакового размера, требуется определить, являются ли они изоморфными.

Для любой полугруппы $S = H(A, \psi, z)$ определим граф $G(S)$ следующим образом. Вершины графа $G(S)$ — это множество A. Для вершин $a_1, a_2 \in A$ в графе $G(S)$ есть ребро (a_1, a_2) тогда и только тогда, когда $a_1 a_2 = z$.

Лемма 3. Пусть полугруппы $S_1 = H(A_1, \psi_1, z_1)$ и $S_2 = H(A_2, \psi_2, z_2)$ с минимальными представлениями изоморфны. Тогда изоморфны и графы $G(S_1)$ и $G(S_2)$.

Доказательство. Обозначим через φ изоморфизм между полугруппами S_1 и S_2. По лемме 2 $|A_1| = |A_2|$ и ограничение φ на A_1 является биекцией. Докажем, что ограничение φ на A_1 является изоморфизмом между графами $G(S_1)$ и $G(S_2)$. Действительно, так как $\varphi(z_1) = z_2$, то для любых $a_i, a_j \in A_1$ в графе $G(S_1)$ есть ребро $(a_i, a_j) \Leftrightarrow$ $\Leftrightarrow a_i a_j = z_1 \Leftrightarrow \varphi(a_i a_j) = z_2 \Leftrightarrow \varphi(a_i)\varphi(a_j) = z_2 \Leftrightarrow$ есть ребро $(\varphi(a_i), \varphi(a_j))$ в графе $G(S_2)$. ■

Пусть $\mathcal{G}$ — множество графов, для которых алгоритм Боллобаша не находит канонической разметки. Определим множество

$$\mathcal{R}(k)_n = \{S \in \mathcal{NS}(k)_n : G(S) \in \mathcal{G}\}.$$

Лемма 4. Существуют константы $C_1, C_2 > 0$, такие, что для любого достаточно большого n и любого $k \in (t_0 - 3, t_0 + 3)$, где $t_0 = n - \dfrac{n}{2 \ln n}$, имеет место

$$\rho_n(\mathcal{R}(k)_n) = \frac{|\mathcal{R}(k)_n|}{|\mathcal{NS}(k)_n|} < \frac{C_1}{n^{C_2}}.$$

Доказательство. Заметим, что

$$\mathcal{NS}(k)_n = \bigcup_{A \subset \{1,\ldots,n\},\, |A| = k} \mathcal{NS}(k, A)_n,$$

где $\mathcal{NS}(k, A)_n$ — множество всех полугрупп вида $H(A, \psi, z)$, A — k-элементное подмножество $\{1, \ldots, n\}$. Легко видеть, что $|\mathcal{NS}(k, A_1)_n| = |\mathcal{NS}(k, A_2)_n|$ для любых k-элементных подмножеств A_1 и A_2 множества $\{1, \ldots, n\}$. Число таких $\mathcal{NS}(k, A)_n$ равно C_n^k. Определим для любого k-элементного подмножества $A \subset \{1, \ldots, n\}$

$$\mathcal{R}(k, A)_n = \mathcal{R}(k)_n \cap \mathcal{NS}(k, A)_n.$$

Заметим, что

$$|\mathcal{R}(k, A_1)_n| = |\mathcal{R}(k, A_2)_n|$$

для всех k-элементных подмножеств A_1 и A_2 множества $\{1,\dots,n\}$, так как любая биекция между A_1 и A_2 задаёт биекцию между сравниваемыми множествами. Число таких множеств равно C_n^k. Поэтому для любого фиксированного подмножества A имеем $\rho_n(\mathcal{R}(k,A)_n) = \rho_n(\mathcal{R}(k)_n)$.

Зафиксируем k-элементное подмножество $A \subset \{1,\dots,n\}$ и отметим, что $\rho_n(\mathcal{R}(k,A)_n)$ есть вероятность того, что для случайно и равновероятно выбранной из $\mathcal{NS}(k,A)_n$ полугруппы S алгоритм Боллобаша не выдаёт каноническую разметку для графа $G(S)$. Докажем, что вероятность быть соединёнными ребром для вершин случайного графа $G(S)$ не зависит от этих вершин, и оценим эту вероятность.

Полугруппа S имеет вид $H(A,\psi,z)$, где ψ — случайно и равновероятно выбранная функция из $A\times A$ в $\bar{A}$; z — случайно и равновероятно выбранный элемент из $\bar{A}$. Пусть $A=\{a_1,\dots,a_k\}$ и $S\setminus A=\{b_1,b_2,\dots,b_{n-k}\}$. Вершинами графа $G(S)$ является множество A. Вершины a_i и a_j соединены ребром, если $\psi(a_i,a_j)=z$. Так как функция ψ выбирается случайно и равновероятно, вероятность этого для любых i,j равна $p=1/(n-k)$. Так как

$$n-\frac{n}{1{,}99\ln n}<n-\frac{n}{2\ln n}-3<k<n-\frac{n}{2\ln n}+3<n-\frac{n}{2{,}01\ln n},$$

то

$$\frac{1{,}99\ln n}{n}<p<\frac{2{,}01\ln n}{n}.$$

Учитывая, что функция $f(x)=\ln x/x$ при $x>e$ убывает и что для достаточно больших n имеет место $n<1{,}01\,k$, получаем

$$\frac{1{,}99\ln(1{,}01\,k)}{1{,}01\,k}<\frac{1{,}99\ln n}{n}<p<\frac{2{,}01\ln n}{n}<\frac{2{,}01\ln k}{k}<\frac{0{,}5}{k^{11/12}}.$$

Отсюда

$$\frac{1{,}97\ln k}{k}<p<\frac{0{,}5}{k^{11/12}}.$$

Поэтому вероятность того, что алгоритм Боллобаша не выдаёт каноническую разметку для графа $G(S)$, для достаточно больших k оценивается, согласно [4], величиной $1/k^C$ с некоторой универсальной константой $C>0$. Следовательно,

$$\rho_n(\mathcal{R}(k)_n)=\rho_n(\mathcal{R}(k,A)_n)<\frac{1}{k^C}<\frac{C_1}{n^C}.$$

Последнее неравенство верно в силу того, что $0{,}99\,n<k$ при достаточно больших n. ■

4. Основной результат

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

Доказательство. Пусть S_1 и S_2 — две полугруппы порядка n, заданные таблицами умножения. Полиномиальный генерический алгоритм $\mathcal{B}$, решающий проблему изоморфизма, работает на входе (S_1,S_2) следующим образом:

1) Запустить полиномиальный генерический алгоритм $\mathcal{A}$ из леммы 1 на S_1 и S_2.
2) Если $\mathcal{A}(S_1)=?$ или $\mathcal{A}(S_2)=?$, то выдать ответ «?».
3) Теперь имеются минимальные представления полугрупп $S_1=H(A_1,\psi_1,z_1)$ и $S_2=H(A_2,\psi_2,z_2)$.

4) Если $|A_1| \neq |A_2|$, то выдать ответ «НЕТ». Корректность этого ответа следует из леммы 2.
5) Пусть $k = |A_1|$. Если $k \notin \left\{n - \dfrac{n}{2\ln n} - 3, \ldots, n - \dfrac{n}{2\ln n} + 3\right\}$, то выдать ответ «?».
6) Построить графы $G(S_1)$ и $G(S_2)$.
7) Запустить алгоритм Боллобаша для проверки изоморфизма графов $G(S_1)$ и $G(S_2)$.
8) Если проверка закончилась неудачей, выдать ответ «?».
9) Если алгоритм Боллобаша выдал «НЕТ», выдать «НЕТ». Корректность ответа в данном случае следует из леммы 3.
10) Если алгоритм Боллобаша выдал «ДА» и выдал изоморфизм φ между графами $G(S_1)$ и $G(S_2)$, то проверить, является ли изоморфизмом между полугруппами S_1 и S_2 отображение φ', определённое следующим образом:

$$\varphi'(a) = \begin{cases} \varphi(a), & \text{если } a \in A_1, \\ z_2, & \text{если } a = z_1, \\ \pi(a), & \text{если } a \in S_1 \setminus (A_1 \cup \{z_1\}). \end{cases}$$

Здесь π — биекция между $S_1 \setminus (A_1 \cup \{z_1\})$ и $S_2 \setminus (A_2 \cup \{z_2\})$, построенная по ограничению φ на A_1 из п. 4 леммы 2. Если является, то выдать ответ «ДА», иначе — «НЕТ». Корректность ответа также следует из леммы 3.

Докажем генеричность алгоритма $\mathcal{B}$. Алгоритм может выдать ответ «?» на шагах 2, 5 и 8. Пренебрежимость множества входов, на которых алгоритм выдаёт ответ «?» на шагах 2 и 5, следует из леммы 1 и результатов Клейтмана — Ротшильда — Спенсера. На шаге 8 алгоритм выдаёт ответ «?», если алгоритм Боллобаша не смог найти каноническую разметку для графа $G(S_1)$ или $G(S_2)$. Напомним, что через $\mathcal{G}$ обозначается множество графов, для которых алгоритм Боллобаша не выдаёт каноническую разметку. Нужно доказать, что

$$\lim_{n\to\infty,\ k\in I_n} \frac{|\mathcal{R}'(k)_n|}{|\mathcal{NS}'(k)_n|} = 0,$$

где $I_n = \left\{n - \dfrac{n}{2\ln n} - 3, \ldots, n - \dfrac{n}{2\ln n} + 3\right\}$ и $\mathcal{R}'(k)_n = \{S \in \mathcal{NS}'(k)_n : G(S) \in \mathcal{G}\}$. Так как $\mathcal{R}'(k)_n \subset \mathcal{R}(k)_n$ и, согласно [5], имеет место

$$\lim_{n\to\infty,\ k\in I_n} \frac{|\mathcal{NS}(k)_n|}{|\mathcal{NS}'(k)_n|} = 1,$$

то достаточно доказать, что

$$\lim_{n\to\infty,\ k\in I_n} \frac{|\mathcal{R}(k)_n|}{|\mathcal{NS}(k)_n|} = 0.$$

Это следует из леммы 4, по которой для всех $k \in I_n$ выполняется неравенство

$$\frac{|\mathcal{R}(k)_n|}{|\mathcal{NS}(k)_n|} < \frac{C_1}{n_2^C}.$$

Теорема 1 доказана. ■

Автор выражает благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

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. *Babai L., Erdos P, and Selkow S.* Random graph isomorphism // SIAM J. Computing. 1980. V. 9. No. 3. P. 628–635.
4. *Bollobas B.* Distinguishing of vertices of random graphs // Ann. Discrete Math. 1982. V. 13. P. 33–50.
5. *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.

REFERENCES

1. *Zemlyachenko V. N., Korneenko N. M., and Tyshkevich R. I.* The graph isomorphism problem [Problema izomorfizma grafov]. Zapiski Nauchnyh Seminarov LOMI, 1982, vol. 118, pp. 83–158. (in Russian)
2. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
3. *Babai L., Erdos P, and Selkow S.* Random graph isomorphism. SIAM J. Computing, 1980, vol. 9, no. 3, pp. 628–635.
4. *Bollobas B.* Distinguishing of vertices of random graphs. Ann. Discrete Math., 1982, vol. 13, pp. 33–50.
5. *Kleitman D. J., Rothschild B. R., and Spencer J. H.* The number of semigroups of order n. Proc. Amer. Math. Soc., 1976, vol. 55, no. 1, pp. 227–232.