S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 11, стр. 144–144 (2014) УДК 510.652
MSC 11U99

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ РАВЕНСТВА В НЕКОТОРЫХ КОНЕЧНО ОПРЕДЕЛЕННЫХ ПОЛУГРУППАХ

А.Н. РЫБАЛОВ

Abstract. Generic-case approach to algorithmic problems was suggested by Miasnikov, Kapovich, Schupp and 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 present a polynomial algorithm for the word problem in some finitely defined semigroups. This algorithm works for semigroups with one defining relation. Its justification relies on the theory of finite periodic Markov chains.

Keywords: generic complexity, word problem, semigroups, Markov chains.

1. Введение

Генерический подход был предложен в 2003 году И. Каповичем, А. Г. Мясниковым, В. Шпильрайном и П. Шуппом в работе [7]. В рамках этого подхода изучается поведение алгоритмов на множествах входов, асимптотическая плотность которых равна 1 (эти множества называются генерическими), и игнорируется поведение алгоритма на остальных входах, на которых алгоритм может работать медленно или вообще не останавливаться. Исследования вычислительной сложности для «почти всех» входов началось в 1970-80-х годах, после того как был выделен огромный пласт трудноразрешимых алгоритмических проблем – NP-полных проблем, для которых не удалось найти эффективных алгоритмов, работающих за полиномиальное время для всех входов. Оказалось, что если немного ослабить требование эффективности – рассматривать не все входы, а «почти все» или случайные входы, то иногда можно

Rybalov, A.N., On the generic complexity of the word problem in some finitely defined semigroups.

быстро решать задачу для таких типичных входов. Этот подход имеет практический смысл, когда алгоритм должен решать быстро задачу для случайных входных данных: если вероятность «наткнуться» на «плохой» вход пренебрежимо мала, то алгоритм будет быстро работать практически всегда. Ярким примером такого алгоритма является симплекс-метод: этот алгоритм имеет экспоненциальную сложность в худшем случае, но за полиномиальное время решает задачу линейного программирования для почти всех входных данных.

Важнейшей алгоритмической проблемой в алгебре является проблема равенства для различных алгебраических систем: групп, полугрупп, колец, алгебр и т.д. Одним из выдающихся достижений алгебры 20 века является построение конечно определенных полугрупп А. А. Марковым [10], Э. Постом [16] и групп П. С. Новиковым [15] с неразрешимой проблемой равенства. Позднее простые примеры полугрупп с неразрешимой проблемой равенства были найдены Г. С. Цейтиным [18], Г. С. Маканиным [9] и Ю. В. Матиясевичем [11]. И. Капович, А. Г. Мясников, В. Шпильрайн и П. Шупп [7] предложили генерический алгоритм для проблемы равенства в некоторых конечно определенных группах, в том числе в классических группах с неразрешимой проблемой равенства. Также этот алгоритм работает за полиномиальное время в конечно порожденных группах с одним определяющим соотношением, тогда как классический алгоритм Магнуса, решающий проблему равенства в таких группах не является полиномиальным. Для обоснования генеричности этого алгоритма были использованы результаты В. Восса [19], Л. Бартольди [2], Р. Григорчука [3] о случайных блужданиях по графам Кэлли конечно порожденных групп. В дальнейшем Д. Вон [20] предложил простой генерический алгоритм для проблемы равенства в конечно определенных полугруппах, в том числе и для классических полугрупп с неразрешимой проблемой равенства: полугруппа Цейтина, полугруппа Маканина. Однако он не работает для полугрупп с одним соотношением. Проблемой равенства для таких полугрупп много занимались С. И. Адян и его ученики [1]. Тем не менее, вопрос о разрешимости проблемы равенства для полугрупп с одним соотношением до сих пор открыт. В [17] был получен генерический алгоритм для проблемы равенства в некотором классе конечно определенных полугрупп, включающим полугруппы с одним определяющим соотношением.

В данной работе строится генерический полиномиальный алгоритм для проблемы равенства, работающий в более широком классе конечно определенных полугрупп, чем алгоритм из работы [17]. Для обоснования генеричности этого алгоритма будут использованы периодические конечные цепи Маркова.

2. Генерические алгоритмы

Пусть I – некоторое множество входов. Для подмножества $S \subseteq I$ определим последовательность

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

где I_n – множество входов размера n, а $S_n = S \cap I_n$ – множество входов из S размера n. Заметим, что $\rho_n(S)$ это вероятность попасть в S при случайной и равновероятной генерации входов из I_n. *Асимптотической плотностью* S назовем предел (если он существует)

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

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 называется *генерическим*, если множество $\{x \in I : \mathcal{A}(x) \downarrow\}$ генерическое. Генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если

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

Генерический алгоритм $\mathcal{A}$ работает за полиномиальное время, если существует полином $p(n)$ такой, что

$$\forall x \in I \ \mathcal{A}(x) \downarrow \Rightarrow t_{\mathcal{A}}(x) < p(size(x)).$$

Еще такие алгоритмы мы будем называть полиномиальными генерическими.

С практической точки зрения, когда требуется построить алгоритм, решающий конкретную алгоритмическую проблему для почти всех входов, удобнее рассматривать алгоритмы следующего типа. Каждый такой алгоритм останавливается на всех входах, на входах из некоторого генерического множества выдает правильный ответ, а на пренебрежимом множестве остальных входов выдает специальный ответ «?» – «Не знаю». Определение такой эффективной генерической вычислимости можно найти в обзоре [5] и в гораздо более ранней работе [12].

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

(1) $\mathcal{A}$ останавливается на всех входах из I,
(2) множество $\{x \in I : \mathcal{A}(x) =?\}$ пренебрежимо.

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

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

Множество $S \subseteq I$ и соответствующая проблема распознавания (S, I) *(эффективно) генерически разрешимы*, если существует (эффективно) генерический алгоритм, вычисляющий характеристическую функцию S.

Легко видеть, что из эффективной генерической разрешимости следует генерическая разрешимость. Действительно, любой эффективный генерический алгоритм можно легко переделать в генерический заменив выдачу ответа «?» на бесконечное зацикливание. В обратную сторону это неверно – см., например, теорему 2.22 и следствие 2.24 в [6]. Однако для полиномиальной (экспоненциальной) сложности верно и обратное: из полиномиальной (экспоненциальной) генерической разрешимости следует полиномиальная (экспоненциальная) эффективная разрешимость. Действительно, если имеется полиномиальная оценка $p(n)$ на время работы генерического алгоритма в случае, когда он останавливается, то можно завести счетчик T числа шагов, и, в случае, если $T > p(n)$, можно обрывать вычисление и выдавать ответ «?», – в этом случае генерический алгоритм уже не остановится. Таким образом получается эффективно генерический полиномиальный алгоритм, решающий ту же проблему.

С учетом вышесказанного, в дальнейшем, при доказательстве существования генерического алгоритма, будут строиться эффективно генерические алгоритмы. Из существования эффективного (полиномиального) генерического алгоритма будет следовать существование (полиномиального) генерического алгоритма.

3. Полугруппы и цепи Маркова

При изложении нужных нам сведений и результатов теории цепей Маркова будем придерживаться классической монографии Феллера [4].

Пусть S – конечно определенный коммутативный моноид с сокращениями и с множеством порождающих $A = \{a_1, \ldots, a_m\}$. Свойство сокращения означает, что для любых $x, y, z \in S$ из равенства $xy = xz$ следует $y = z$. Более того, допустим, что моноид S конечный и $\{s_1, \ldots, s_r\}$ – все его элементы.

Определим цепь Маркова $MC(S)$ следующим образом. Состояния цепи $MC(S)$ есть все элементы моноида $\{s_1, \ldots, s_r\}$, причем $s_1 = 1$. Матрица $P = ||p_{ij}||$ цепи $MC(S)$ – это квадратная $r \times r$ матрица, ее элементы определяются так:

$$p_{ij} = \begin{cases} \frac{1}{m}, \text{ если } s_i a = s_j \text{ для некоторого порождающего } a \in A, \\ 0, \text{ иначе.} \end{cases}$$

Элемент p_{ij} задает вероятность перехода из состояния s_i в состояние s_j. Цепь $MC(S)$, начиная с состояния s_1 на нулевом шаге, каждом последующем шаге переходит из текущего состояния s_i в последующее состояние s_j с вероятностью p_{ij}. Это можно представлять как случайное блуждание по графу Кэли моноида S с началом в 1, когда в каждый момент времени, находясь в вершине s_i равновероятно из всех выходящих ребер (соответствующих всем порождающим из A) выбирается ребро, по которому происходит переход в следующую вершину. В дальнейшем мы будем отождествлять цепь Маркова $MC(S)$ и описанное случайное блуждание по графу Кэли моноида S.

Пусть теперь M – бесконечный коммутативный конечно определенный моноид с сокращениями и с множеством порождающих $A = \{a_1, \ldots, a_m\}$. Для фиксированного натурального q добавим к определяющим соотношениям моноида M соотношения $\{a_1^q = 1, \ldots, a_m^q = 1\}$. Обозначим полученный новый моноид через $M(q)$. Легко видеть, что для любого q моноид $M(q)$ конечен. У каждого порождающего a_i есть обратный a_i^{q-1}, так что фактически $M(q)$ является группой.

Лемма 1. *Пусть $M(a_1, \ldots, a_m)$ – бесконечный конечно определенный коммутативный моноид с сокращениями. Тогда число элементов $M(q)$ растет с ростом q.*

Доказательство. Известно [8], что моноид M вкладывается в конечно определенную абелеву группу A с таким же множеством порождающих $a_1, \ldots, a_m$. Обозначим через $A(q)$ группу A с добавленными к ее определяющим соотношениям соотношениями $a_1^q = 1, \ldots, a_m^q = 1$. Легко видеть, что $A(q)$ изоморфна $M(q)$.

По теореме о классификации конечнопорожденных абелевых групп [13], A изоморфна прямому произведению простых циклических групп и бесконечных циклических групп, то есть

$$A \cong \langle b_1 \rangle \oplus \ldots \oplus \langle b_k \rangle \oplus \langle c_1 \rangle \oplus \ldots \oplus \langle c_l \rangle,$$

где $b_1, \ldots, b_k$ – элементы бесконечного порядка, а элементы $c_1, \ldots, c_l$ имеют конечные порядки $r_1, \ldots, r_l$. Причем, так как A бесконечна, то $k > 0$. Кроме того, все элементы $b_1, \ldots, b_k$ независимы, то есть любую ненулевую степень b_i нельзя выразить через остальные и $c_1, \ldots, c_l$.

Теперь покажем, что $b_1^s \neq 1$ в $M(q)$ при $0 < s < q$. Из этого будет следовать утверждение леммы. Действительно, пусть $b_1^s \neq 1$ в $M(q)$ при $0 < s < q$. Тогда

$$b_1^s = a_1^{qt_1} \dots a_m^{qt_m} c_1^{r_1 u_1} \dots c_l^{r_l u_l}$$

в группе A. Теперь перепишем a_i через $b_1, \dots, b_k$ и $c_1, \dots, c_l$. Получим выражение

$$b_1^s = b_1^{qz_1} \dots b_k^{qz_k} c_1^{y_1} \dots c_l^{y_l}$$

или

$$b_1^{s-qz_1} = b_2^{qz_2} \dots b_k^{qz_k} c_1^{y_1} \dots c_l^{y_l}$$

для некоторых целых $z_1, \dots, z_k, y_1, \dots, y_l$. Таким образом, получаем, что ненулевая степень b_1 выражается через $b_2, \dots, b_k$ и $c_1, \dots, c_l$. Противоречие. □

Матрица называется *стохастической*, если ее элементы неотрицательны и сумма элементов в каждой строке равна 1. Легко видеть, что матрица P цепи Маркова $MC(S)$ (как и любой другой конечной цепи) является стохастической. Матрица называется *дважды стохастической*, если ее элементы неотрицательны и сумма элементов в каждой строке и в каждом столбце равна 1. Легко проверяется, что произведение двух дважды стохастических матриц является опять дважды стохастической матрицей.

Лемма 2. *Матрица P цепи $MC(M(q))$ является дважды стохастической.*

Доказательство. Фактически нужно доказать, что в любую вершину s графа Кэли моноида $MC(q)$ входят ровно m ребер, помеченных порождающими $a_1, \dots, a_m$. Действительно, для каждого порождающего a_i одно ребро, помеченное a_i, входит в вершину s из вершины, соответствующей элементу sa_i^{q-1}. Допустим, что два ребра, помеченные a_i, входят в s из двух разных вершин s_l и s_t. Это означает, что $s = s_l a_i = s_t a_i$, откуда, так как моноид $M(q)$ есть моноид с сокращениями, следует, что $s_l = s_t$. Противоречие. □

Цепь Маркова называется *неприводимой*, если для любых двух ее различных состояний s_i и s_j состояние s_j достижимо из s_i и наоборот, s_i достижимо из s_j. Достижимость означает, что имеется ненулевая вероятность получить одно состояние из другого за конечное число шагов. Заметим, что цепь $MC(M(q))$ является неприводимой. Это легко следует из того, что в графе Кэли моноида $M(q)$ любые две вершины связаны ориентированным путем.

Обозначим через $p_n(s_i)$ – вероятность попасть в состояние s_i из начального состояния s_1 за n шагов. *Периодом* состояния s_i цепи Маркова называется число

$$t = \text{НОД}(t_1, t_2, t_3, \dots, t_k, \dots),$$

где для любого k имеет место

(1) $p_{t_k}(s_i) > 0$,
(2) $p_l(s_i) = 0$ для любого l такого, что $t_k < l < t_{k+1}$.

То есть через t_1 шагов мы можем впервые с ненулевой вероятностью попасть в состояние s_i, через t_2 – во второй раз, через t_k – в k-й раз и так далее. Для состояния s_i цепи $MC(M(q))$ это означает, что в графе Кэли моноида $M(q)$ существуют ориентированные пути из вершины s_1 в вершину s_i длин $t_1, t_2, \dots, t_k, \dots$ и для любого k не существуют путей длины l, где $t_k < l < t_{k+1}$. Цепь Маркова называется *непериодической*, если для каждого ее состояния период равен 1, иначе цепь называется *периодической*.

Одним из фундаментальных результатов теории цепей Маркова является следующий: любая конечная неприводимая непериодическая цепь является эргодической. Это означает, что для любого ее состояния s_i существует предельная вероятность, то есть существует предел

$$p(s_i) = \lim_{n\to\infty} p_n(s_i).$$

Для цепи $MC(M(q))$ вероятность $p_n(s_i)$ есть вероятность того, что случайно записанное слово длины n в алфавите A равно элементу s_i в моноиде $M(q)$.

В случае же периодической цепи все состояния имеют одинаковый период t, а множество состояний разбивается на классы (подцепи) $C_0, \ldots, C_{t-1}$ и свойство эргодичности имеет место для каждого класса $C_k, k = 0, \ldots, t-1$: для любого $s_i \in C_k$ имеет место

(1) существует предел $p(s_i) = \lim_{n\to\infty} p_{tn+k}(s_i)$,
(2) $p_n(s_i) = 0$, если $n \neq k(\mod t)$.

Эти подцепи $C_0, \ldots, C_{t-1}$ получаются следующим образом. Полагаем $s_1 \in C_0$. Далее в C_0 добавляются все состояния, достижимые из s_1 ровно за t шагов. Потом добавляются все состояния, достижимые ровно за t шагов из добавленных на предыдущем шаге и так до тех пор, пока есть еще не добавленные. Получается цепь C_0. Теперь цепь C_1 состоит из всех состояний, достижимых из всех состояний цепи C_0 ровно за 1 шаг, цепь C_2 – ровно за 2 шага, и так далее. Последняя цепь C_{t-1} содержит состояния, достижимые из C_0 ровно за $t-1$ шагов.

Если матрица исходной цепи есть P, то матрицы подцепей $C_0, \ldots, C_{t-1}$ равны P^t. Отметим также, что если матрица P дважды стохастическая, то и P^t тоже дважды стохастическая. Для цепи с дважды стохастической матрицей предельные вероятности одинаковы (см. [4], стр. 386):

(1) $p(s_i) = \frac{1}{r}$, где r – число состояний непериодической цепи,
(2) $p(s_i) = \frac{1}{|C_k|}$, если $s_i \in C_k$ для периодической цепи, состоящей из подцепей $C_0, \ldots, C_{t-1}$.

Лемма 3. *Пусть M – бесконечный коммутативный конечно определенный моноид с сокращениями и с множеством порождающих $A = \{a_1, \ldots, a_m\}$. Тогда множество*

$$eq(M) = \{(w_1, w_2) \in A^* \times A^* \ : \ w_1 = w_2 \text{ в моноиде } M\}$$

пренебрежимо.

Доказательство. Имеем

$$\rho_n\big(eq(M)\big) = \frac{|eq(M)_n|}{|\{(w_1, w_2) : w_1, w_2 \in A^*, |w_1| + |w_2| = n\}|} =$$

$$= \frac{|eq(M)_n|}{\sum_{k=0}^{n} m^k m^{n-k}} = \frac{\sum_{k=0}^{n} |eq(M)_{n,k}|}{n \cdot m^n} = \frac{1}{n} \sum_{k=0}^{n} \frac{|eq(M)_{n,k}|}{m^n}, \tag{1}$$

где

$$eq(M)_{n,k} = \{(w_1, w_2) \in A^* \times A^* : |w_1| = k, |w_2| = n-k\}.$$

Зафиксируем число q и рассмотрим моноид $M(q)$, определенный как выше добавлением к определяющим соотношениям моноида M соотношений $\{a_1^q =$

$1, \ldots, a_m^q = 1\}$. Легко видеть, что $eq(M) \subseteq eq(M(q))$, а потому выполняется оценка $\rho_n(eq(M)) \leq \rho_n(eq(M(q)))$.

Пусть $\{s_1, \ldots, s_r\}$ – все различные элементы моноида. Рассмотрим конечную цепь Маркова $MC(M(q))$, построенную по моноиду $M(q)$. Ее состояниями являются элементы моноида $\{s_1, \ldots, s_r\}$. Заметим теперь, что

$$\frac{|eq(M)_{n,k}|}{m^n} = \sum_{i=1}^{r} p_k(s_i) p_{n-k}(s_i), \tag{2}$$

где $p_t(s_i)$ есть вероятность того, что после t шагов, цепь $MC(M(q))$ будет находится в состоянии s_i.

Рассмотрим теперь два возможных случая.

Случай 1. Не существует непустого слова $w \in A^*$ такого, что $w = 1$ в моноиде M. Зафиксируем натуральное число $q > 1$. Тогда конечная неприводимая цепь Маркова $MC(M(q))$ является периодической с периодом q. Поэтому множество состояний $MC(M(q))$ разбивается на t классов $C_0, \ldots, C_{q-1}$ так, что для любого $s \in C_l$ имеет место $p_t(s) = 0$, если $t \neq l(\mod q)$. Таким образом, с учетом (2), выражение (1) для моноида $MC(q)$ переписывается в виде

$$\rho_n\big(eq(M(q))\big) = \frac{1}{n}\sum_{k=0}^{n} \frac{|eq(M)_{n,k}|}{m^n} = \frac{1}{n}\sum_{k=0}^{n}\Big(\sum_{i=1}^{r} p_k(s_i) p_{n-k}(s_i)\Big) =$$

$$\frac{1}{n}\sum_{k=0,\ldots,n;k=n-k(\mod q)}\Big(\sum_{i=1}^{r} p_k(s_i) p_{n-k}(s_i)\Big) \leq \frac{1}{n}\sum_{k=0,\ldots,n;k=n-k(\mod q)} 1,$$

так как имеет место оценка

$$\sum_{i=1}^{r} p_k(s_i) p_{n-k}(s_i) = \frac{|eq(M)_{n,k}|}{m^n} \leq 1.$$

Теперь

$$\frac{1}{n}\sum_{k=0,\ldots,n;k=n-k(\mod q)} 1 = \frac{n}{q},$$

если $n = 2e(\mod q)$ для некоторого натурального e, и

$$\frac{1}{n}\sum_{k=0,\ldots,n;k=n-k(\mod q)} 1 = 0,$$

иначе. В любом случае получаем, что $\rho_n\big(eq(M(q))\big) \leq \frac{1}{q}$. При увеличении числа q величина $\rho_n\big(eq(M(q))\big)$, а, значит и $\rho_n\big(eq(M)\big)$ стремится к 0.

Случай 2. Существует непустое слово $w \in A^*$ такое, что $w = 1$ в моноиде M. Выберем такое слово наименьшей длины f. Зафиксируем натуральное число $q > f$. Тогда конечная неприводимая цепь Маркова $MC(M(q))$ является периодической с периодом $g \leq f$. Это следует из того, что M – моноид сокращениями, и в любое состояние s_i можно вернуться по пути, соответствующему слову w длины f. Таким образом, если $t_1 < t_2 < \ldots < t_k < \ldots$ – число шагов, для которых $p_{t_k}(s_i) > 0$, то $t_{k+1} - t_k \leq f$. Поэтому период s_i, он же период всей цепи

$$g = \text{НОД}(t_1, t_2, t_3, \ldots, t_k, \ldots) \leq f.$$

Множество состояний $MC(M(q))$ разбивается на g подцепей $C_0, \ldots, C_{g-1}$ так, что для любого $s \in C_l$ имеет место

(1) $p_t(s) = 0$, если $t \neq l(\mod g)$,
(2) $\lim_{t\to\infty} p_{tg+l}(s) = p(s) = \frac{1}{|C_l|}$.

Последнее равенство выполняется в виду того, что матрица вероятностей переходов для каждой подцепи C_l является дважды стохастической по лемме 2. Кроме того, заметим, что размеры классов $C_0, \ldots, C_{g-1}$ растут с ростом числа q, так как, по лемме 1, растет число элементов моноида $M(q)$ – оно же число состояний цепи $MC(M(q))$. Это следует из процедуры построения подцепей $C_0, \ldots, C_{g-1}$, описанной выше. Теперь оценим выражение (1) для моноида $M(q)$:

$$\rho_n\Big(eq(M(q))\Big) = \frac{1}{n}\sum_{k=0}^{n}\frac{|eq(M)_{n,k}|}{m^n} \leq \frac{2\sqrt{n}}{n} + \frac{1}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\frac{|eq(M)_{n,k}|}{m^n}. \tag{3}$$

Пусть число n достаточно большое, чтобы для каждого l и каждого $s \in C_l$ выполнялось неравенство

$$p_{tg+l}(s) < \frac{2}{|C_l|}$$

при $tg + l > \sqrt{n}$. Оценим сумму из (3)

$$\frac{1}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\frac{|eq(M)_{n,k}|}{m^n} = \frac{1}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\Big(\sum_{i=1}^{r}p_k(s_i)p_{n-k}(s_i)\Big) <$$

$$< \frac{1}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\Big(\sum_{i=0}^{g-1}\big(\sum_{s\in C_i}\frac{4}{|C_i|^2}\big)\Big) < \frac{1}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\Big(\sum_{i=0}^{g-1}\frac{4|C_i|}{|C_i|^2}\Big) =$$

$$= \frac{4}{n}\sum_{k=[\sqrt{n}]}^{n-[\sqrt{n}]}\Big(\sum_{i=0}^{g-1}\frac{1}{|C_i|}\Big) < \frac{4(n-2\sqrt{n}g)}{nC} < \frac{4g}{C},$$

где $C = \min\{|C_0|, \ldots, |C_{g-1}|\}$. Так как число C растет с ростом q, то $\rho_n(eq(M))$ стремится к 0. □

4. Проблема равенства в полугруппах

Напомним определение проблемы равенства для конечно определенной полугруппы $\mathfrak{S} = \langle A|R\rangle$ с множеством порождающих A и множеством определяющих соотношений R. Для произвольной заданной пары слов $(w_1, w_2) \in A^* \times A^*$ нужно определить, равны ли элементы, представляемые словами w_1, w_2 в полугруппе $\mathfrak{S}$. Под размером входа (w_1, w_2) понимается сумма их длин $|w_1|+|w_2|$.

Определим по полугруппе $\mathfrak{S}$ коммутативный моноид $\mathfrak{S}'$ с сокращениями, добавив к определяющим соотношениям R полугруппы $\mathfrak{S}$ соотношения коммутативности для всех порождающих $a_ia_j = a_ja_i$, $1 \leq i, j \leq m$, а также единицу. Также допускаем, что в $\mathfrak{S}'$ выполняется свойство сокращения.

Теорема 1. *Если для полугруппы $\mathfrak{S}$ моноид $\mathfrak{S}'$ бесконечен, то проблема равенства в $\mathfrak{S}$ генерически полиномиально разрешима.*

Доказательство. Пусть моноид $\mathfrak{S}'$ бесконечен. Эффективно генерический полиномиальный алгоритм для проблемы равенства в полугруппе S работает на паре слов $(w_1, w_2) \in A^* \times A^*$ следующим образом. Слова w_1 и w_2 рассматриваются как входы для проблемы равенства в моноиде $\mathfrak{S}'$. Известно [8], что

коммутативный моноид с сокращениями $\mathfrak{S}'$ вкладывается в абелеву группу с тем же множеством порождающих, что и $\mathfrak{S}'$. Методом Гаусса решаем за полиномиальное время, равны ли слова w_1 и w_2 в $\mathfrak{S}'$. Если они не равны в $\mathfrak{S}'$, то тем более они не равны и в $\mathfrak{S}$. В этом случае выдаем ответ «НЕТ». Иначе, выдаем ответ «?».

Пренебрежимость множества, на котором этот алгоритм выдает ответ «?», следует из леммы 3. □

В качестве следствия данного утверждения построим несколько более удобный алгоритм.

Пусть $\mathfrak{S} = \langle A \mid R\rangle$ – конечно определенная полугруппа с порождающими $A = \{a_1, \ldots, a_m\}$ и соотношениями $R = \{u_1 = v_1, \ldots, u_k = v_k\}$, где $u_i, v_i, i = 1, \ldots, k$ – некоторые слова в алфавите A.

Для каждой буквы a_i в алфавите A и для каждой пары слов $(w_1, w_2) \in A^* \times A^*$ определим $d_i(w_1, w_2)$ как число вхождений буквы a_i в слово w_1 минус число вхождений буквы a_i в слово w_2. Далее определим для произвольной пары $(w_1, w_2) \in A^* \times A^*$ следующий вектор

$$d(w_1, w_2) = \big(d_1(w_1, w_2), \ldots, d_m(w_1, w_2)\big).$$

Для полугруппы $\mathfrak{S}$ обозначим через $V_{\mathfrak{S}}$ подпространство векторного пространства $\mathbb{Q}^m$, порожденное векторами $d(v_i, u_i), i = 1, \ldots, k$ для всех соотношений $u_i = v_i, i = 1, \ldots, k$.

Следствие 1. *Пусть $\mathfrak{S} = \langle A \mid R\rangle$ – конечно определенная полугруппа такая, что подпространство $V_{\mathfrak{S}}$ имеет размерность меньше $m = |A|$. Тогда проблема равенства в $\mathfrak{S}$ генерически разрешима за полиномиальное время.*

Доказательство. Чтобы воспользоваться теоремой 1, нужно доказать, что моноид $\mathfrak{S}'$ бесконечен. Допустим, что $\mathfrak{S}'$ конечен. Так как он вкладывается в абелеву группу $\mathfrak{G}$ с множеством порождающих A и соотношений R, то $\mathfrak{G}$ тоже конечна. Но это противоречит тому, что фактор-пространство $\mathbb{Q}^m/V_{\mathfrak{S}}$ бесконечно. □

Применим данный алгоритм к некоторым классическим полугруппам.

Следствие 2. *Проблема равенства в полугруппе Цейтина* [18]

$$\mathfrak{T} = \langle a, b, c, d, e \mid ac = ca,\ ad = da,\ bc = cb,\ bd = db,$$
$$ce = eca,\ de = edb,\ cca = ccae\rangle$$

генерически разрешима за полиномиальное время.

Доказательство. Вычислим вектора d для соотношений полугруппы $\mathfrak{T}$:

$$\begin{aligned} d(ac, ca) &= (0,0,0,0,0),\\ d(ad, da) &= (0,0,0,0,0),\\ d(bc, cb) &= (0,0,0,0,0),\\ d(bd, db) &= (0,0,0,0,0),\\ d(ce, eca) &= (-1,0,0,0,0),\\ d(de, edb) &= (0,-1,0,0,0),\\ d(cca, ccae) &= (0,0,0,0,-1). \end{aligned}$$

Легко видеть, что подпространство $V_{\mathfrak{T}}$ имеет размерность $3 < 5$. Поэтому по следствию 1, проблема равенства в полугруппе $\mathfrak{T}$ генерически разрешима за полиномиальное время. □

Следствие 3. *Пусть* $\mathfrak{S} = \langle A \mid u_1 = v_1, \ldots, u_k = v_k \rangle$ *– полугруппа такая, что число соотношений* k *меньше числа порождающих* $|A|$*. Проблема равенства в* $\mathfrak{S}$ *генерически разрешима за полиномиальное время.*

Доказательство. Так как $|A| > k$, то подпространство $V_{\mathfrak{S}}$ порождено k векторами $d(u, v)$ и имеет размерность $\leq k < |A|$. По следствию 1, проблема равенства в полугруппе $\mathfrak{S}$ генерически разрешима за полиномиальное время. □

Вопрос о разрешимости проблемы равенства для полугрупп с одним определяющим соотношением до сих пор открыт, несмотря на впечатляющий прогресс для многих частных классов таких полугрупп [1].

Следствие 4. *Проблема равенства в полугруппе* $\mathfrak{S} = \langle A \mid u = v \rangle$ *с одним определяющим соотношением генерически разрешима за полиномиальное время.*

Доказательство. Если $|A| = 1$, то полугруппа $\mathfrak{S}$ циклическая и, очевидно, имеет разрешимую проблему равенства. В случае $|A| > 1$ утверждение следует из следствия 3. □

В работе [14] была построена конечно определенная полугруппа с генерически неразрешимой проблемой равенства. Пусть $\mathfrak{S} = \langle A \mid R \rangle$ – полугруппа с проблемой равенства, неразрешимой в классическом смысле. Пусть $A = \{a_1, \ldots, a_m\}$ и $x \notin A$. В полугруппе

$$\mathfrak{S}_x = \langle A, x | R, x = xa_1, \ldots, x = xa_m, x = xx \rangle$$

проблема равенства не является генерически разрешимой. Теорема 1 неприменима к полугруппе $\mathfrak{S}_x$, так как при добавлении соотношения коммутативности для всех пар порождающих и свойства сокращения полугруппа $\mathfrak{S}_x^*$ будет тривиальной. Также легко видеть, что утверждение 1 не работает для полугруппы $\mathfrak{S}_x$. Соответствующие вектора даже для не всех соотношений дают полный базис:

$$\begin{aligned} d(x, xa_1) &= (-1, 0, \ldots, 0, 0), \\ d(x, xa_2) &= (0, -1, \ldots, 0, 0), \\ &\ldots \\ d(x, xa_m) &= (0, 0, \ldots, -1, 0), \\ d(x, xx) &= (0, 0, \ldots, 0, -1). \end{aligned}$$

References

[1] S. I. Adjan, V. G. Durnev. Algorithmic problems for groups and semigroups, Russian Math. Surveys, **55:2** (2000), 207–296.

[2] L. Bartholdi. *Counting paths in graphs*, Enseign. Math., **45:2** (1999), 83–131.

[3] R. Grigorchuk. *Symmetrical random walks on discrete groups*, Multicomponent random systems, Adv. Probab. Related Topics, **6** (1980), 285–325.

[4] W. Feller. *An Introduction to Probability Theory and Its Applications, Vol. 1*, Wiley and Sons, (1966) 528 p.

[5] D. Hirschfeldt. *Some Questions in Computable Mathematics*, Computability and Complexity, (2017), 22–55.

[6] C. Jockusch, P. Schupp. *Generic computability, Turing degrees, and asymptotic density*, Journal of the London Mathematical Society, **85:2** (2012), 472–490.

[7] I. Kapovich, A. Myasnikov, P. Schupp, V. Shpilrain. *Generic-case complexity and decision problems in group theory*, Journal of Algebra, **264** (2003), 665–694.

[8] A. H. Clifford. G. B. Preston. *The Algebraic Theory of Semigroups*, American Mathematical Society, (1961) 224 p.

[9] G. S. Makanin. *On the word problem in finitely defined semigroups*, Doklady AN SSSR, **171:2** (1966), 285–287. (in Russian)
[10] A. A. Markov. *Impossibility of some algorithms in the theory of associative systems*, Doklady AN SSSR, **55:7** (1947), 587–590. (in Russian)
[11] Yu. V. Matiyasevich. *Simple examples of undecidable canonical calculi*, Trudy MIAN SSSR, **93** (1967), 50–88. (in Russian)
[12] A. Meyer. *An open problem on creative sets*, Recursive Function Theory Newsletter, **4** (1973), 15–16.
[13] O. V. Melnikov, V. N. Remeslennikov, V. A. Romankov. *Groups. Universal algebra, ed L. A. Skornakov. Vol 1*, M.: Nauka, (1990) 66–290. (in Russian)
[14] A. G. Myasnikov, A. N. Rybalov. *Generic complexity of undecidable problems*, Journal of Symbolic Logic, **73:2** (2008), 656–673.
[15] P. S. Novikov. *On the algorithmic undecidability of the word problem in group theory*, Trudy MIAN SSSR, **44** (1955), 3–143. (in Russian)
[16] E. L. Post. *Recursive unsolvability of a problem of Thue*, Journal of Symbolic Logic, **12:1** (1947), 1–11.
[17] A. Rybalov. *A generic algorithm for the word problem in semigroups and groups*, Journal of Physics: Conference Series, **1546** (2020), 1–10.
[18] G. S. Tseitin. *Associative calculus with unsolvable equivalence problem*, Trudy MIAN SSSR, **52** (1958), 172–189. (in Russian)
[19] W. Woess. *Cogrowth of groups and simple random walks*, Archive of Mathematics, **41** (1983), 363–370.
[20] D. Won. *Word problems on balanced semigroups and balanced groups*, City University of New York, ProQuest Dissertations Publishing, **3296964** (2008), 79 p.

Alexander Nikolaevich Rybalov
Sobolev Institute of Mathematics,
prospekt Koptyuga 4,
Novosibirsk, 630090, Russia.
Email address: alexander.rybalov@gmail.com