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 СЛОЖНОСТИ ПРОБЛЕМЫ РАВЕНСТВА В ПОЛУГРУППАХ С УСЛОВИЕМ ОДНОРОДНОСТИ ОПРЕДЕЛЯЮЩИХ СООТНОШЕНИЙ

А.Н. РЫБАЛОВ

Abstract. In this paper we study the computational complexity of the word problem in semigroups with the condition of homogeneity of the defining relations. These are finitely defined semigroups, in which for each defining relation the lengths of the left and right parts are equal. The word problem for such semigroups is decidable, but known algorithms require exponential time and memory. We prove that this problem belongs to the class **PSPACE**, consisting of algorithmic problems that are solved by Turing machines using space (memory cells) bounded polynomially. This improves the upper bound on the space complexity known before. On the other hand, we prove that there exists a semigroup with the condition of homogeneity of defining relations, in which the equality problem is complete in the class **PSPACE** with respect to polynomial reducibility. It is assumed (although not proven) that the class **PSPACE** is wider than the class **NP** and, even more so, the class **P**. Thus, it is shown that there are semigroups with the condition of homogeneity of defining relations with the intractable problem of equality.

Keywords: computational complexity, semigroups, word problem.

Rybalov, A.N., On complexity of the word problem in semigroups with homogeneous relations.

Работа выполнена в рамках государственного задания ИМ СО РАН, проект FWNF-2022-0003.

Поступила 30 июня 2023 г., опубликована 1 сентября 2023 г.

1. Введение

Важнейшей алгоритмической проблемой в алгебре является проблема равенства для различных алгебраических систем: групп, полугрупп, колец, алгебр и т.д. Одним из выдающихся достижений алгебры XX века является построение А. А. Марковым [7], Э. Постом [9] конечно определенных полугрупп и П. С. Новиковым [8] конечно определенных групп с неразрешимой проблемой равенства. К ярким положительным результатам можно отнести результат А. И. Мальцева [6] о разрешимости проблемы равенства в любой конечно определенной коммутативной полугруппе.

В дальнейшем, фокус исследований проблемы равенства в полугруппах сдвинулся в сторону изучения ее вычислительной сложности для различных классов полугрупп с разрешимой проблемой равенства. Е. Кордоза показал [2], что проблема равенства в любой фиксированной конечно определенной коммутативной полугруппе разрешима за линейное время. С другой стороны, Е. Майр и А. Мейер доказали [5], что проблема равенства в многообразии всех коммутативных полугрупп (то есть, когда входом алгоритма является не только два слова, для которых проверяется равенство, но и само конечное представление полугруппы) является полной относительной полиномиальной сводимости в классе **EXPSPACE**. Класс **EXPSPACE** – это класс проблем, разрешимых с использованием экспоненциальной памяти. Доказано (см., например, [4]), что этот класс строго шире класса **P**.

В данной работе изучается вычислительная сложность проблемы равенства полугрупп с условием однородности определяющих соотношений. Это конечно определенные полугруппы, в которых для каждого определяющего соотношения длины левой и правой частей равны. Сам термин был предложен в известном обзоре С. И. Адяна и В. Г. Дурнева [1], где буквально в одном абзаце доказывается разрешимость проблемы равенства для таких полугрупп. Частным случаем таких полугрупп являются так называемые моноиды трассировки [3] или частично коммутативные моноиды, которые возникают в информатике при анализе распараллеливания программ. Известно [3], что проблема равенства в таких моноидах решается за линейное время. Однако в общем случае, известные алгоритмы для решения проблемы равенства в полугруппах с условием однородности определяющих соотношений (например, алгоритм из [1]), работают за экспоненциальное время (и пространство).

В данной статье доказывается, что проблема равенства в любой полугруппе с условием однородности определяющих соотношений лежит в классе **PSPACE**. Здесь класс **PSPACE** состоит из алгоритмических проблем распознавания, которые решаются машинами Тьюринга с использованием пространства (ячеек памяти), ограниченного полиномиально. Тем самым улучшается верхняя оценка на вычислительную сложность по пространству из [1]. С другой стороны, доказывается, что существует полугруппа с условием однородности определяющих соотношений, в которой проблема равенства полна в классе **PSPACE** относительно полиномиальной сводимости. Предполагается (хотя и не доказано), что класс **PSPACE** шире класса **NP** и тем более класса **P**. Таким образом, показано, что существуют полугруппы с условием однородности определяющих соотношений с трудноразрешимой проблемой равенства.

2. Предварительные сведения

Пусть $S = \langle a_1, \ldots, a_n \mid u_1 = v_1, \ldots, u_m = v_m \rangle$ – конечно определенная полугруппа с множеством порождающих $A = \{a_1, \ldots, a_n\}$ и множеством определяющих соотношений $R = \{u_1 = v_1, \ldots, u_m = v_m\}$. Полугруппа S называется *полугруппой с условием однородности определяющих соотношений*, если $|u_i| = |v_i|$ для каждого $i = 1, \ldots, m$.

Пусть M – машина Тьюринга, $s_M(x)$ – число ячеек ленты, используемое в работе M на x. Проблема распознавания (множество) A принадлежит *классу* **PSPACE**, если существует машина Тьюринга M, распознающая A, и полином $p(n)$ такие, что $s_M(x) < p(|x|)$.

Проблема распознавания (множество) A **PSPACE**-*полна*, если

(1) $A \in$ **PSPACE**,
(2) любая проблема B из **PSPACE** полиномиально сводится к A, то есть существует функция f, вычислимая за полиномиальное время, такая, что
$$\forall x \; x \in B \Leftrightarrow f(x) \in B.$$

Известно (см., например, [4]), что **PSPACE**-полные проблемы существуют.

Проблема A принадлежит *классу* **NPSPACE**, если существует недетерминированная машина Тьюринга M и полином $p(n)$ такие, что $x \in A \Leftrightarrow \exists$ вычислительный путь τ M на x такой, что $M_\tau(x) = 1$ и $s_M(\tau, x) < p(|x|)$. Строгое определение недетерминированной машины Тьюринга можно найти в [4]. В программе таких машин могут быть пары правил с одинаковыми левыми частями (внутренним состоянием и символом, обозреваемым в данный момент кареткой). Предполагается, что при работе такой машины в определенный момент может быть выбрано и то и другое правило. Таким образом, на одном входе могут возникнуть несколько вычислительных путей, и, в итоге, несколько результатов работы машины.

В теории сложности вычислений хорошо известна теорема Сэвича [10], которая утверждает, что **PSPACE** = **NPSPACE**. Это означает, что для любой проблемы, распознаваемой недерминированным алгоритмом с полиномиально ограниченной памятью, можно построить детерминированный алгоритм также с полиномиально ограниченной памятью, который также решает эту проблему. Теорема Сэвича контрастирует с ситуацией с аналогичными классами для временной сложности **P** и **NP** – большинство исследователей считает, что эти классы различаются.

3. Основные результаты

В доказательстве следующей теоремы мы будем использовать модель машин Тьюринга с несколькими рабочими лентами. Эта модель полиномиально эквивалентна обычной модели с одной лентой (см. [4]), и является более удобной для описания конкретных алгоритмов.

Теорема 1. *Проблема равенства в любой полугруппе с условием однородности определяющих соотношений принадлежит классу* **PSPACE**.

Доказательство. Пусть $S = \langle a_1, \ldots, a_n \mid u_1 = v_1, \ldots, u_m = v_m \rangle$ – конечно определенная полугруппа с условием однородности определяющих соотношений. Докажем, что проблема равенства в S принадлежит классу **NPSPACE**. Из этого, по теореме Сэвича, будет следовать ее принадлежность классу **PSPACE**.

Опишем работу следующего недетерминированного алгоритма $\mathcal{A}$ с полиномиально ограниченной памятью. Заметим сначала очевидный факт: при замене в слове w согласно определяющим соотношениям S может получиться слово w' для которого $|w| = |w'|$. Пусть на входе имеются два слова (w_1, w_2) над алфавитом A. Алгоритм $\mathcal{A}$ работает на входе (w_1, w_2) следующим образом.

(1) Вначале на первой ленте записано слово $w' = w_1$, на второй – слово w_2.
(2) Если длины w_1 и w_2 не равны, выдает ответ «НЕТ». Иначе переходит на следующий шаг.
(3) Недетерминированно выбирает в слове w' подслово, совпадающее с левой или правой частью какого-то соотношения полугруппы S, и заменяет его согласно этому соотношению. Получается новое слово w'. Заметим, что длина нового слова осталась той же самой, тем самым алгоритм не использовал новую память для вычислений.
(4) Если $w' = w_2$, то останавливается и выдает ответ «ДА».
(5) Иначе возвращается на шаг 3.

Легко видеть, что, $w_1 = w_2$ в полугруппе S, то есть слово w_2 можно получить из w_1 применением замен согласно определяющим соотношениям S, тогда и только тогда, когда существует вычислительный путь алгоритма $\mathcal{A}$ на (w_1, w_2), на котором он выдает ответ «ДА». Полиномиальное ограничение на память при работе алгоритма $\mathcal{A}$ следует из замечания к шагу 3. □

В доказательстве следующей теоремы мы будем использовать стандартную модель машин Тьюринга с одной рабочей лентой. У таких машин будут два конечных состояния: q_a – принимающее и q_r – отвергающее.

Теорема 2. *Существует полугруппа с условием однородности определяющих соотношений, для которой проблема равенства является* **PSPACE***-полной.*

Доказательство. Пусть $C \subseteq A^*$ – некоторое **PSPACE**-полное подмножество строк над алфавитом $A = \{a_1, \ldots, a_k\}$. Пусть M – машина Тьюринга, распознающая множество C с рабочим алфавитом $A \cup \{a_0\}$, где a_0 будет обозначать пустой символ. Обозначим через $p(n)$ полином, ограничивающий функцию пространства $s_M(x)$ машины M. Наконец пусть $Q = \{q_1, q_2, \ldots, q_m, q_a, q_r\}$ – множество состояний машины M, среди которых отдельно выделены два конечных состояния: q_a – принимающее и q_r – отвергающее состояния. Программа машины M состоит из правил вида

$$(q_i, a) \to (q_j, b, shift),$$

где $q_i \in Q \setminus \{q_a, q_r\}$, $q_j \in Q$, $a, b \in A \cup \{a_0\}$ и $shift \in \{R, L\}$ – сдвиг каретки. По одному правилу для каждой возможной комбинации (q_i, a).

Будем строить полугруппу S с условием однородности определяющих соотношений, определяющие соотношения которой будут соответствовать правилам программы машины M, а цепочка преобразований согласно этим соотношениям некоторого начального слова будет моделировать работу машины M на входном слове $w \in A^*$ до ее остановки с условием ограничения $p(|w|)$ на используемое пространство.

Порождающими полугруппы S будет множество $X = A \cup \{a_0\} \cup Q$. Теперь каждому правилу программы машины M вида

$$(q_i, a) \to (q_j, b, R)$$

сопоставим определяющее соотношение $q_i a = b q_j$, а каждому правилу вида

$$(q_i, a) \to (q_j, b, L)$$

сопоставим определяющие соотношения $cq_i a = q_j cb$ для всех $c \in A \cup \{a_0\}$. Добавим еще соотношения $q_a c = q_a a_0$ и $q_a c = c q_a$ для всех символов $c \in A \cup \{a_0\}$. Легко заметить, что правые и левые части всех этих соотношений имеют одинаковые длины, то есть полугруппа S получается с условием однородности определяющих соотношений.

Покажем теперь, что машина M работает на слове $w \in A^*$, останавливается и принимает слово w (то есть попадает в состояние q_a), используя при этом пространство, ограниченное $p(|w|)$, тогда и только тогда, когда в полугруппе S равны слова $w_1 = a_0^{p(|w|)} q_1 w a_0^{p(|w|)}$ и $w_2 = q_a a_0^{2p(|w|)+|w|}$. Заметим, что $|w_1| = |w_2| = 2p(|w|) + |w| + 1$.

Действительно, пусть машина M принимает вход w. Тогда, нетрудно видеть, что каждой конфигурации машины M (то есть содержимому ленты, положению каретки и состоянию машины M), которая получается применением некоторого правила программы, соответствует слово, которое получается применением соответствующего определяющего соотношения. В частности, начальной конфигурации машины соответствует слово $w_1 = a_0^{p(|w|)} q_1 w a_0^{p(|w|)}$. При этом те пустые ячейки ленты, которые пока не задействованы в вычислении, но, потенциально могут использоваться в будущем, в словах-элементах полугруппы S уже заранее «зарезервированы» в начале и в конце слова в символах a_0. Причем, условие, что количество ячеек ленты, используемое в работе, ограничено $p(|w|)$, гарантирует, что этих зарезервированных символов a_0 хватит для корректного моделирования работы машины.

После того, как машина M попадает в конечное состояние q_a и принимает вход w, в слове-элементе полугруппы S, соответствующем этой конфигурации, появляется буква q_a. С помощью соответствующих определяющих соотношений для q_a слово можно преобразовать в $w_2 = q_a a_0^{2p(|w|)+|w|}$.

Рассуждения, показывающие, что если из слова $w_1 = a_0^{p(|w|)} q_1 w a_0^{p(|w|)}$ с помощью определяющих соотношений полугруппы S можно получить слово $w_2 = q_a a_0^{2p(|w|)+|w|}$, то машина M принимает вход w, полностью аналогичны рассуждениям из леммы 2.2. из [1].

Теперь покажем, что проблема равенства в полугруппе S является **PSPACE**-полной. То, что проблема равенства принадлежит классу **PSPACE**, следует из теоремы 1. Пусть теперь имеется любое множество B из **PSPACE**. Так как множество C, которое мы моделировали, является **PSPACE**-полным, то существует полиномиально вычислимая функция f такая, что $x \in B \Leftrightarrow f(x) \in C$. Теперь положим

$$g(x) = (a_0^{p(|f(x)|)} q_1 f(x) a_0^{p(|f(x)|)}, q_a a_0^{2p(|f(x)|)+|f(x)|}).$$

С учетом всего вышедоказанного понятно, что g – полиномиально вычислимая функция, которая сводит проблему B к проблеме равенства в полугруппе S. То есть, $x \in B$ тогда и только тогда, когда $g(x)$ есть пара равных слов в S. $\square$

References

[1] S. I. Adjan, V. G. Durnev. *Algorithmic problems for groups and semigroups*, Uspehi Math. Nauk, **55:2** (2000), 3–94.
https://www.mathnet.ru/links/dfff7cc9b43ec12ecd94fa7503d2cca1/rm267.pdf

[2] E. W. Cardoza. *Computational complexity of the word problem for commutative semigroups*, MAC technical memorandum, **67** (1975), MIT.
https://dspace.mit.edu/handle/1721.1/148895

[3] V. Diekert, Y. Métivier. *Partial Commutation and Traces*, in Rozenberg, G.; Salomaa, A. (eds.), Handbook of Formal Languages Vol. 3; Beyond Words, Springer-Verlag, Berlin, (1997), 457–534.
https://link.springer.com/chapter/10.1007/978-3-642-59126-6_8

[4] M. Garey, D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company, (1979). 340p.
https://bohr.wlu.ca/hfan/cp412/references/ChapterOne.pdf

[5] E. Mayr, A. Meyer. *The complexity of the word problems for commutative semigroups and polynomial ideals*, Advances in Mathematics, **46(3)** (1982), 305–329.
https://core.ac.uk/download/pdf/82035833.pdf

[6] A. I. Malcev. *On homomorphisms of finite groups*, Uch. zapiski Ivanovskogo ped. Instituta, **18** (1958), 49–60.

[7] A. A. Markov. *Impossibility of some algorithms in the theory of associative systems*, Doklady AN SSSR, **55(7)** (1947), 587–590.

[8] P. S. Novikov. *On algorithmical undecidability of the word problem in group theory*, Trudy MIAN SSSR, **44** (1955) 3–143.
https://www.mathnet.ru/links/26f6eee299f78947dcc78c29b7f9f702/tm1180.pdf

[9] E. L. Post. *Recursive unsolvability of a problem of Thue*, Journal of Symbolic Logic, **12:1** (1947), 1–11.
https://www.wolframscience.com/prizes/tm23/images/Post2.pdf

[10] W. J. Savitch. *Relationships between nondeterministic and deterministic tape complexities*, Journal of Computer and System Sciences, **4:2** (1970), 177–192.
https://www.sciencedirect.com/science/article/pii/S002200007080006X

Alexander Nikolaevich Rybalov
Sobolev Institute of Mathematics,
prospekt Koptyuga 4,
Novosibirsk, 630090, Russia.
Pevtsova 13,
Omsk, 644099, Russia.
Email address: alexander.rybalov@gmail.com