

## Сложность задачи проверки тождеств в конечных полугруппах

Ж. Алмейда, М. В. Волков, С. В. Плещева

Многие базовые алгоритмические задачи алгебры, разрешимость которых давно известна и/или очевидна, приводят к интересным и зачастую весьма трудным проблемам, если задаться вопросом о *вычислительной сложности* соответствующих алгоритмов. Сложность алгоритмов в настоящей работе понимается в смысле монографий [1, 14]; там же можно найти определения упоминаемых в работе классов сложности P, NP и coNP.

Исследовать вычислительную сложность задачи проверки тождеств в конечных алгебрах предложил М. В. Сапир в хорошо известном обзоре 1995 года [10, проблема 2.4]. С тех пор в этой тематике наблюдаются значительные продвижения.

Под *задачей проверки тождеств* понимается следующая комбинаторная задача распознавания, имеющая в качестве параметра заданную конечную алгебру  $\mathcal{A}$ :

УСЛОВИЕ: задано тождество  $p \equiv q$ , где  $p$  и  $q$  – термы в сигнатуре алгебры  $\mathcal{A}$ ;

ВОПРОС: Выполнено ли тождество  $p \equiv q$  в алгебре  $\mathcal{A}$ ?

Задачу проверки тождеств для данной алгебры  $\mathcal{A}$  будем обозначать через ID-CHECK( $\mathcal{A}$ ).

Как подмечено в [10, с. 402], если  $\mathcal{A}$  – двухэлементная булева алгебра, то задача ID-CHECK( $\mathcal{A}$ ) равносильна “отрицанию” классической задачи Выполнимость. Поскольку задача Выполнимость NP-полна (см. [1, 14]), отсюда следует, что в этом случае задача ID-CHECK( $\mathcal{A}$ ) будет coNP-полной. Что можно сказать о сложности задачи ID-CHECK( $\mathcal{A}$ ), если исходная конечная алгебра  $\mathcal{A}$  обладает меньшими, чем булевы алгебры, “выразительными возможностями”, например, если  $\mathcal{A}$  – полугруппа, группа, кольцо? Этот вопрос также явно ставился в [10]. На сегодня полный ответ получен на него в случае ассоциативных колец: Хант и Стирнс [8, теорема 5.3] показали, что задача ID-CHECK( $\mathcal{R}$ ) разрешима за полиномиальное время, если кольцо  $\mathcal{R}$  нильпотентно, а Баррис и Лоуренс [5, теорема 1.7] установили, что эта задача coNP-полна, если  $\mathcal{R}$  – ненильпотентное кольцо. Для групп столь же законченного описания пока нет, но недавно были получены существенные продвижения в направлении к нему: Баррис и Лоуренс [6] доказали полиномиальную

разрешимость задачи  $\text{ID-CHECK}(\mathcal{G})$  для случаев, когда группа  $\mathcal{G}$  нильпотентна или диэдральна, а Хорват, Лоуренс, Мераи и Сабо [7] обнаружили, что если  $\mathcal{G}$  неразрешима (в смысле теории групп), то задача  $\text{ID-CHECK}(\mathcal{G})$  оказывается  $\text{coNP}$ -полной. В классе полугрупп, не являющихся группами, до сих пор были найдены только отдельные примеры, в которых задача проверки тождеств  $\text{coNP}$ -полна, см. [11, 12, 15, 9, 17, 18, 16, 2].

В настоящей работе мы доказываем следующий редукционный результат:

**ТЕОРЕМА 1.** *Пусть  $\mathcal{S}$  – конечная полугруппа, а  $\mathcal{G}$  – прямое произведение всех ее максимальных подгрупп. Тогда задача  $\text{ID-CHECK}(\mathcal{G})$  полиномиально сводится к задаче  $\text{ID-CHECK}(\mathcal{S})$ .*

Отсюда и из цитированного выше результата работы [7] о неразрешимых группах немедленно вытекает

**СЛЕДСТВИЕ 1.** *Если конечная полугруппа содержит неразрешимую подгруппу, то задача проверки тождеств в этой полугруппе  $\text{coNP}$ -полна.*

Обращение следствия 1 неверно – среди упомянутых выше полугрупп с  $\text{coNP}$ -полной задачей проверки тождеств имеются и такие, в которых все подгруппы тривиальны [12, 15, 9]. Однако, комбинируя следствие 1 с известными результатами, можно полностью классифицировать полугруппы некоторых важных типов по отношению к сложности проверки тождеств. Например, для полугрупп матриц над конечными полями исчерпывающий ответ дает

**СЛЕДСТВИЕ 2.** *Задача проверки тождеств в полугруппе всех  $n \times n$ -матриц над конечным полем  $\text{coNP}$ -полна при  $n > 1$  и решается за полиномиальное время при  $n = 1$ .*

Другую классическую серию конечных полугрупп составляют полугруппы всех преобразований  $n$ -элементного множества.

При  $n \geq 5$  здесь также можно использовать следствие 1, но случай  $n \leq 4$  требует другого подхода. Нам удалось частично разобрать этот случай, что позволило получить следующий “почти полный” результат:

**ТЕОРЕМА 2.** *Задача проверки тождеств в полугруппе всех преобразований  $n$ -элементного множества  $\text{coNP}$ -полна при  $n = 3$  и  $n \geq 5$  и решается за полиномиальное время при  $n = 1, 2$ .*

Вопрос о сложности проверки тождеств в полугруппе всех преобразований 4-элементного множества пока остается открытым.

Теорема 1 получена авторами совместно, а теорема 2 принадлежит третьему автору. Часть результатов работы была анонсирована в [3].

### Список литературы

- [1] М. Гэри, Д. Джонсон, Вычислительные машины и труднорешаемые задачи, М.: Мир, 1982.
- [2] С. В. Плещева, В. Вертеши, Сложность задачи проверки тождеств в 0-простой полугруппе, Изв. Урал. гос. ун-та, № 43, Компьютерные науки и информационные технологии, Вып. 1 (2006), С. 72–102.
- [3] J. Almeida, S. V. Plescheva, M. V. Volkov, An application of group generic implicit operators to the complexity of identity checking in finite semigroups, Междунар. алгебраич. конф., посвященная столетию со дня рождения П. Г. Конторовича и 70-летию Л. Н. Шеврина, Тез. докл., Екатеринбург: Изд-во Урал. ун-та, 2005, 16–17.

- [4] *C. Bergman, G. Slutzki*, Complexity of some problems concerning varieties and quasi-varieties of algebras, *SIAM J. Comput.*, 30, №2 (2000), 359–382.
- [5] *S. Burris, J. Lawrence*, The equivalence problem for finite rings, *J. Symbolic Comput.*, 15, №1 (1993), 67–71.
- [6] *S. Burris, J. Lawrence*, Results on the equivalence problem for finite groups, *Algebra Universalis*, 52, №4 (2005), 495–500.
- [7] *G. Horváth, J. Lawrence, L. Mérai, Cs. Szabó*, The complexity of the equivalence problem for nonsolvable groups, в печати.
- [8] *H. B. Hunt III, R. E. Stearns*, The complexity of equivalence for commutative rings, *J. Symbolic Comput.*, 10, №5 (1990), 411–436.
- [9] *M. Jackson, R. McKenzie*, Interpreting graph colorability in finite semigroups, *Int. J. Algebra and Computation*, 16, №1 (2006), 119–140.
- [10] *O. G. Kharlampovich, M. V. Sapir*, Algorithmic problems in varieties, *Int. J. Algebra and Computation*, 5, №4-5 (1995), 379–602.
- [11] *A. Kisielewicz*, Complexity of semigroup identity checking, *Int. J. Algebra and Computation*, 14, №4 (2004), 455–464.
- [12] *O. Klima*, Complexity issues of checking identities in finite monoids, в печати.
- [13] *M. Kozik*, On some complexity problems in finite algebras, PhD Dissertation, Vanderbilt University, Nashville, 2004.
- [14] *C. H. Papadimitriou*, Computational Complexity, Reading–Menlo Park–N.Y.: Addison-Wesley Publishing Company, 1994.
- [15] *S. Seif*, The Perkins semigroup has co-NP-complete term-equivalence problem, *Int. J. Algebra and Computation*, 15, №2 (2005), 317–326.
- [16] *S. Seif, Cs. Szabó*, Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields, *Semigroup Forum*, 72, №2 (2006), 207–222.
- [17] *Cs. Szabó, V. Vértési*, The complexity of the word-problem for finite matrix rings, *Proc. Amer. Math. Soc.*, 132, №12 (2004), 3689–3695.
- [18] *Cs. Szabó, V. Vértési*, The complexity of checking identities for finite matrix rings, *Algebra Universalis*, 51, №4 (2004), 439–445.

*E-mail:* Svetlana.Plescheva@usu.ru