J. Almeida, M. V. Volkov, S. V. Gol'dberg, Complexity of the identity checking problem for finite semigroups, *Zap. Nauchn. Sem. POMI*, 2008, Volume 358, 5–22

Записки научных
семинаров ПОМИ
Том 358, 2008 г.

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

СЛОЖНОСТЬ ЗАДАЧИ ПРОВЕРКИ ТОЖДЕСТВ В КОНЕЧНЫХ ПОЛУГРУППАХ

§1. Постановка задачи и обзор результатов

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.[1] В качестве примера упомянем следующую задачу VAR-MEMB: *для двух конечных алгебр $\mathcal{A}$ и $\mathcal{B}$ одинаковой сигнатуры определить, удовлетворяет ли алгебра $\mathcal{A}$ всем тождествам алгебры $\mathcal{B}$.* (Обозначение VAR-MEMB произведено от "variety membership", поскольку в терминах теории многообразий речь идет о распознавании принадлежности алгебры $\mathcal{A}$ многообразию, порожденному алгеброй $\mathcal{B}$.) Понятно значение задачи VAR-MEMB для современной универсальной алгебры, в которой, как хорошо известно, классификация алгебр с помощью тождеств занимает одно из центральных мест. В то же время указанная задача интересна и для компьютерных наук, см., например, обсуждение ее связи с формальной теорией спецификаций в [8, §1]. Алгоритмическая разрешимость задачи VAR-MEMB легко выводится из HSP-теоремы Тарского и отмечалась еще в пионерской работе Калицкого [16]. Исследование же вычислительной сложности этой задачи началось сравнительно недавно и принесло довольно неожиданные результаты. Верхнюю оценку привели Бергман и Слуцки [8], установившие, что задача VAR-MEMB принадлежит классу `2-EXPTIME` (класс задач, разрешимых за дважды экспоненциальное время). Эта оценка сперва представлялась сильно завышенной, но затем Секели [30] по-

[1] Сложность алгоритмов в настоящей работе понимается в смысле монографий [1, 23]; там же читатель сможет найти определения упоминаемых в работе классов сложности NP, co-NP, EXPSPACE и т.д.

Работа первого автора была частично поддержана Центром математики университета Порту, финансируемым Фондом науки и технологии через совместные программы Португалии и Европейского Союза POCTI и POSI. Второй и третий авторы получали поддержку РФФИ по гранту 05-01-00540 .

казал, что обсуждаемая задача NP-трудна, а Козик [20, 21] установил, что она является даже EXPSPACE-трудной. В конце концов, Козик [22] доказал 2-EXPTIME-полноту задачи VAR-MEMB, подтвердив тем самым, что оценка Бергмана и Слуцки в действительности точна.

Задача, рассматриваемая в настоящей работе, в определенном смысле еще более фундаментальна, чем задача VAR-MEMB. В последней спрашивается, удовлетворяет ли алгебра $\mathcal{A}$ каждому из (бесконечно многих) тождеств алгебры $\mathcal{B}$, в то время как здесь мы локализуем ситуацию, спрашивая, выполняется ли в фиксированной конечной алгебре $\mathcal{A}$ *одно* данное тождество. Соответствующую задачу будем называть *задачей проверки тождеств в алгебре* $\mathcal{A}$ и обозначать через CHECK-ID($\mathcal{A}$). Более формально, CHECK-ID($\mathcal{A}$) – это комбинаторная задача распознавания, входными данными которой служат всевозможные пары (p, q) термов в сигнатуре алгебры $\mathcal{A}$, а ответами – "ДА" или "НЕТ" в зависимости от того, выполнено или не выполнено тождество $p \approx q$ в этой алгебре. Ясно, что эта задача алгоритмически разрешима – если термы p и q в совокупности зависят от m переменных, можно просто поочередно подставлять вместо переменных всевозможные m-ки элементов алгебры $\mathcal{A}$ и проверять, приводят ли такие подстановки к равным значениям термов p и q. Заметим, однако, что, поскольку число m-ок, подлежащих перебору, равно $|\mathcal{A}|^m$, время работы такого прямолинейного алгоритма в худшем случае экспоненциально зависит от размера входных данных. С другой стороны, очевидно, что для любой конечной алгебры $\mathcal{A}$ задача CHECK-ID($\mathcal{A}$) принадлежит классу сложности co-NP: если для какой-то пары термов (p, q) тождество $p \approx q$ не выполняется в алгебре $\mathcal{A}$, то недетерминированный полиномиальный алгоритм может угадать m-ку элементов из $\mathcal{A}$, опровергающую данное тождество, а затем подтвердить свою догадку вычислением значений термов p и q на этой m-ке.

Исследовать вычислительную сложность задачи CHECK-ID($\mathcal{A}$) (равно как и задачи VAR-MEMB) предложил Сапир в хорошо известном обзоре [17], см. там проблемы 2.4 и 2.5. Как подмечено в [17, с. 402], если $\mathcal{A}$ – двухэлементная булева алгебра, то задача CHECK-ID($\mathcal{A}$) равносильна "отрицанию" классической задачи Выполнимость. Поскольку последняя NP-полна (см. [1, 23]), отсюда следует, что задача проверки тождеств в двухэлементной булевой алгебре будет co-NP-полной. Что можно сказать о сложности задачи CHECK-ID($\mathcal{A}$), 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 [17]. На сегодня полный ответ получен для ассоциативных колец: Хант и Стирнс [14] показали, что задача CHECK-ID($\mathcal{R}$) разрешима за полиномиальное время, если кольцо $\mathcal{R}$ нильпотентно, а Баррис и Лоуренс [9] установили, что эта задача co-NP-полна, если $\mathcal{R}$ – ненильпотентное кольцо. Для групп столь же законченного описания пока нет, но недавно были получены существенные продвижения в направлении к нему. Так, Баррис и Лоуренс [10] доказали полиномиальную разрешимость задачи CHECK-ID($\mathcal{G}$) для случаев, когда группа $\mathcal{G}$ нильпотентна или диэдральна; последний результат получен также Хорватом и Сабо в [13], где установлена полиномиальная разрешимость задачи проверки тождеств и для некоторых других типов метабелевых групп. С другой стороны, Хорват, Лоуренс, Мераи и Сабо [12] обнаружили, что если группа $\mathcal{G}$ неразрешима, то задача CHECK-ID($\mathcal{G}$) оказывается co-NP-полной. В классе полугрупп, не являющихся группами, до сих пор были найдены только отдельные примеры, в которых задача проверки тождеств co-NP-полна, см. [4, 15, 18, 19, 25–28]. Отметим, что примеры из [19, 25] демонстрируют, в частности, что класс полугрупп с полиномиальной проверкой тождеств незамкнут относительно взятия подполугрупп.

В §2 настоящей работы доказывается следующая редукционная теорема.

Теорема 1. *Пусть $\mathcal{S}$ – конечная полугруппа, а $\mathcal{G}$ – прямое произведение всех ее максимальных подгрупп. Существует полиномиальное сведéние задачи* CHECK-ID($\mathcal{G}$) *к задаче* CHECK-ID($\mathcal{S}$).

Отсюда и из цитированного выше результата работы [12] о неразрешимых группах немедленно вытекает такое следствие.

Следствие 1. *Если конечная полугруппа $\mathcal{S}$ содержит неразрешимую подгруппу, то задача* CHECK-ID($\mathcal{S}$) co-NP-*полна.*

Обращение следствия 1 неверно – среди упомянутых выше полугрупп с co-NP-полной задачей проверки тождеств имеются и такие, в которых все подгруппы тривиальны [15, 19, 25]. 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 следующее утверждение.

Следствие 2. *Задача проверки тождеств в полугруппе всех $n \times n$-матриц над конечным полем* co-NP*-полна при $n > 1$ и решается за полиномиальное время при $n = 1$.*

Этот же результат независимо и другим способом получили Сабо и Вертеши [29]. Их доказательство использует арифметическую технику теории конечных матричных групп (в частности, классическую теорему Жигмонди о примитивных простых делителях последовательности разностей степеней натуральных чисел с одинаковыми показателями). При нашем подходе важен только сам факт существования неразрешимых подгрупп в "достаточно больших" полугруппах матриц над конечным полем.

Другую классическую серию конечных полугрупп составляют полугруппы всех преобразований n-элементного множества. В §3 изучается сложность задачи проверки тождеств для этих полугрупп. При $n \geqslant 5$ здесь также можно использовать следствие 1, но случай $n \leqslant 4$ требует другого подхода. Нам удалось разобрать случай $n = 3$, что позволило получить следующий "почти полный" результат.

Теорема 2. *Задача проверки тождеств в полугруппе всех преобразований n-элементного множества* co-NP*-полна при $n = 3$ и $n \geqslant 5$ и решается за полиномиальное время при $n = 1, 2$.*

Вопрос о сложности проверки тождеств в полугруппе всех преобразований 4-элементного множества пока остается открытым. Отметим, что не исключено, что и в этом случае можно будет воспользоваться сведéнием из теоремы 1, так как, хотя группа всех перестановок 4-элементного множества и разрешима, она не попадает ни в один из известных классов групп с полиномиальной проверкой тождеств.

Теорема 1 получена авторами совместно, а теорема 2 принадлежит третьему автору. Часть результатов работы была анонсирована в [6].

§2. Доказательство теоремы 1

Теорема 1 возникла как одно из приложений развитой в [7] теории групповых множеств общего положения в свободной проконечной полугруппе. Чтобы сделать возможным понимание настоящей работы без обращения к [7], мы приведем здесь "финитный" вариант доказательства, в котором все проконечные объекты заменены их подходящими конечными приближениями. Читатель, знакомый с определением и основными свойствами свободной проконечной полугруппы,

легко проделает "предельный переход", позволяющий придать излагаемым ниже построениям естественную для них общность.

Введем несколько необходимых для дальнейшего понятий из теории полугрупп и напомним два элементарных факта, доказательства которых можно найти, например, в [24, глава 3], см. там предложение 1.4 и следствие 1.7. Пусть, как обычно, $\mathcal{S}^1$ есть наименьшая полугруппа с единицей, содержащая данную полугруппу $\mathcal{S}$ (т.е. $\mathcal{S}^1 = \mathcal{S}$, если в $\mathcal{S}$ есть единица, а в противном случае $\mathcal{S}^1 = \mathcal{S} \cup \{1\}$, где добавленный символ 1 ведет себя как единица по умножению). На каждой полугруппе $\mathcal{S}$ определены три естественных предпорядка $\leqslant_{\mathfrak{L}}$, $\leqslant_{\mathfrak{R}}$ и $\leqslant_{\mathfrak{J}}$ – отношения левой, правой и двусторонней делимости:

$$a \leqslant_{\mathfrak{L}} b \Leftrightarrow a = sb \quad \text{для некоторого} \quad s \in \mathcal{S}^1;$$
$$a \leqslant_{\mathfrak{R}} b \Leftrightarrow a = bs \quad \text{для некоторого} \quad s \in \mathcal{S}^1;$$
$$a \leqslant_{\mathfrak{J}} b \Leftrightarrow a = sbt \quad \text{для некоторых} \quad s, t \in \mathcal{S}^1.$$

Через $\mathfrak{L}$, $\mathfrak{R}$ и $\mathfrak{J}$ обозначаются отношения эквивалентности, соответствующие предпорядкам $\leqslant_{\mathfrak{L}}$, $\leqslant_{\mathfrak{R}}$ и $\leqslant_{\mathfrak{J}}$ (т.е. $a \,\mathfrak{L}\, b$ тогда и только тогда, когда $a \leqslant_{\mathfrak{L}} b \leqslant_{\mathfrak{L}} a$, и т.д.). Положим еще $\mathfrak{H} = \mathfrak{L} \cap \mathfrak{R}$.

Предложение 2.1. *Пусть $\mathcal{S}$ – конечная полугруппа, $s, t \in \mathcal{S}$.*

1) *Если $s \leqslant_{\mathfrak{L}} t$ и $s \,\mathfrak{J}\, t$, то $s \,\mathfrak{L}\, t$.*
2) *Если $s \leqslant_{\mathfrak{J}} s^2$, то $\mathfrak{H}$-класс элемента s является максимальной подгруппой полугруппы $\mathcal{S}$.*

Пусть $\Sigma = \{x_1, \ldots, x_m\}$ – конечный алфавит, Σ^+ – свободная полугруппа над Σ, т.е. множество слов, составленных из букв $x_1, \ldots, x_m$, с операцией приписывания. Будем говорить, что слово $u \in \Sigma^+$ является

- *фактором* слова $v \in \Sigma^+$, если $u \geqslant_{\mathfrak{J}} v$;
- *суффиксом* слова $v \in \Sigma^+$, если $u \geqslant_{\mathfrak{L}} v$;
- *префиксом* слова $v \in \Sigma^+$, если $u \geqslant_{\mathfrak{R}} v$.

Если слово $w \in \Sigma^+$ таково, что каждая буква $x_1, \ldots, x_m \in \Sigma$ является его фактором, то w называется *словом полного содержания*.

Любой эндоморфизм φ полугруппы Σ^+ однозначно определяется m словами $w_i = x_i\varphi$, $i = 1, \ldots, m$, которые мы будем называть *компонентами* этого эндоморфизма. Договоримся отождествлять эндоморфизм φ с вектором $[w_1, \ldots, w_m]$, составленным из его компонент. В соответствии с этим соглашением выражение вида $[w_1, \ldots, w_m]^k$ обозначает k-ю степень (итерацию) эндоморфизма $[w_1, \ldots, w_m]$.

Лемма 2.2. *Предположим, что слова $w_1, \dots, w_m$ над алфавитом $\Sigma = \{x_1, \dots, x_m\}$ удовлетворяют следующим трем условиям:*

(а) *каждое из слов $w_1, \dots, w_m$ является словом полного содержания;*

(б) *каждое из слов $w_1, \dots, w_m$ начинается с буквы x_1 и оканчивается на эту букву;*

(в) *слово x_1^2 является фактором слова w_1.*

Пусть $\mathcal{S}$ – произвольная конечная полугруппа и ℓ – максимальная длина $\leqslant_{\mathfrak{J}}$-цепи без $\mathfrak{J}$-эквивалентных элементов в $\mathcal{S}$. Тогда для любого гомоморфизма из Σ^+ в полугруппу $\mathcal{S}$ в последней найдется такая подгруппа, которая будет содержать значения всех компонент эндоморфизма $[w_1, \dots, w_m]^{2\ell}$ при этом гомоморфизме.

Доказательство. Зафиксируем гомоморфизм из Σ^+ в $\mathcal{S}$ и будем обозначать образ слова $w \in \Sigma^+$ при этом гомоморфизме через $\overline{w}$. Для каждого $k = 1, 2, \dots$ положим

$$[w_1, \dots, w_m]^k = [w_{1,k}, \dots, w_{m,k}];$$

таким образом, слово $w_{i,k}$ есть i-я компонента k-й итерации эндоморфизма $\varphi = [w_1, \dots, w_m]$. Отметим, что

$$w_{i,k+1} = x_i\varphi^{k+1} = (x_i\varphi)\varphi^k = w_i(x_1, \dots, x_m)\varphi^k = \\ = w_i(x_1\varphi^k, \dots, x_m\varphi^k) = w_i(w_{1,k}, \dots, w_{m,k}). \quad (1)$$

В силу условия (а) равенства (1) позволяют заключить, что слово $w_{i,k}$ является фактором слова $w_{j,k+1}$ для всех $k = 1, 2, \dots$ и для всех $i, j = 1, \dots, m$. Поскольку отношения делимости сохраняются при гомоморфизмах, в полугруппе $\mathcal{S}$ выполняется цепочка неравенств

$$\overline{w}_{1,1} \geqslant_{\mathfrak{J}} \overline{w}_{1,2} \geqslant_{\mathfrak{J}} \cdots \geqslant_{\mathfrak{J}} \overline{w}_{1,2\ell+1}.$$

Благодаря выбору числа ℓ мы можем утверждать (опираясь на принцип Дирихле), что в этой цепочке найдутся три последовательных $\mathfrak{J}$-эквивалентных элемента. Пусть число $k < 2\ell$ таково, что $\overline{w}_{1,k}\,\mathfrak{J}\,\overline{w}_{1,k+1}\,\mathfrak{J}\,\overline{w}_{1,k+2}$. В силу условия (в) и равенств (1) слово $w_{1,k}^2$ является фактором слова $w_{1,k+1}$. Отсюда в полугруппе $\mathcal{S}$ имеем $\overline{w}_{1,k}^2 \geqslant_{\mathfrak{J}} \overline{w}_{1,k+1}\,\mathfrak{J}\,\overline{w}_{1,k}$. Применяя пункт 2) предложения 2.1, заключаем, что $\mathfrak{H}$-класс $\mathcal{H}$ элемента $\overline{w}_{1,k}$ является максимальной подгруппой полугруппы $\mathcal{S}$. Далее, в силу условия (б) и равенства (1) слово $w_{1,k}$ является как префиксом, так и суффиксом каждого из слов $w_{i,k+1}$, которые, в свою очередь, являются факторами слова $w_{1,k+2}$ в силу (а).

Следовательно, все элементы $\overline{w}_{i,k+1}$ лежат в одном и том же $\mathfrak{J}$-классе полугруппы $\mathcal{S}$. Более того, из пункта 1) предложения 2.1 и двойственного утверждения вытекает, что все они лежат в одном $\mathfrak{L}$-классе и в одном $\mathfrak{R}$-классе с элементом $\overline{w}_{1,k}$. Итак, все элементы $\overline{w}_{i,k+1}$ принадлежат подгруппе $\mathcal{H}$, но тогда той же подгруппе принадлежат и все элементы $\overline{w}_{i,n}$ для всех $n > k$. Поэтому подгруппа $\mathcal{H}$ содержит значения всех слов $w_{1,2\ell}, \ldots, w_{m,2\ell}$ при гомоморфизме $w \mapsto \overline{w}$. □

Свободную полугруппу Σ^+ можно считать подполугруппой в свободной группе $\mathcal{FG}(\Sigma)$ над Σ.

Лемма 2.3. *Предположим, что слова $w_1, \ldots, w_m \in \Sigma^+$ порождают свободную группу $\mathcal{FG}(\Sigma)$. Тогда для любой конечной группы $\mathcal{H}$ и любых m ее элементов $h_1, \ldots, h_m$ найдется такой гомоморфизм $\zeta : \Sigma^+ \to \mathcal{H}$, что $w_i\zeta = h_i$ для всех $i = 1, \ldots, m$.*

Доказательство. Поскольку слова $w_1, \ldots, w_m$ порождают $\mathcal{FG}(\Sigma)$, продолжение ψ эндоморфизма $[w_1, \ldots, w_m]$ на $\mathcal{FG}(\Sigma)$ будет сюръекцией. Хорошо известно (см. [3, предложение I.3.5]), что каждый сюръективный эндоморфизм конечнопорожденной свободной группы является ее автоморфизмом. Положим $g_i = x_i\psi^{-1}$, $i = 1, \ldots, m$. Тогда

$$w_i(g_1, \ldots, g_m) = w_i(x_1\psi^{-1}, \ldots, x_m\psi^{-1}) = \\ = w_i(x_1, \ldots, x_m)\psi^{-1} = x_i\psi\psi^{-1} = x_i \quad (2)$$

для всех $i = 1, \ldots, m$. Поскольку равенства (2) выполняются в свободной m-порожденной группе, они остаются справедливыми при интерпретации букв $x_1, \ldots, x_m$ любыми m элементами произвольной группы. Определим теперь гомоморфизм $\zeta : \Sigma^+ \to \mathcal{H}$, полагая

$$x_i\zeta = g_i(h_1, \ldots, h_m), \quad i = 1, \ldots, m.$$

Тогда в силу равенств (2) имеем

$$w_i(x_1, \ldots, x_m)\zeta = w_i(x_1\zeta, \ldots, x_m\zeta) = \\ = w_i\big(g_1(h_1, \ldots, h_m), \ldots, g_m(h_1, \ldots, h_m)\big) = h_i$$

для всех $i = 1, \ldots, m$. □

Для каждого натурального m рассмотрим следующий набор из m слов:

$$\begin{aligned} w_1 &= x_1^2 x_2 \cdots x_m x_1, \\ w_2 &= x_1 x_2^2 \cdots x_m x_1, \\ &\cdots\cdots\cdots\cdots \\ w_{m-1} &= x_1 x_2 \cdots x_{m-1}^2 x_m x_1, \\ w_m &= x_1 x_2 \cdots x_m x_1. \end{aligned} \tag{3}$$

Очевидно, что слова (3) удовлетворяют условиям (а)–(в) леммы 2.2. Нетрудно проверить, что они удовлетворяют и условию леммы 2.3. Действительно, в свободной группе $\mathcal{FG}(\Sigma)$ имеют место равенства

$$\begin{aligned} x_1 &= w_1 w_m^{-1}, \\ x_2 &= x_1^{-1} w_2 w_m^{-1} x_1, \\ x_3 &= (x_1 x_2)^{-1} w_3 w_m^{-1} x_1 x_2, \\ &\cdots\cdots\cdots\cdots \\ x_{m-1} &= (x_1 x_2 \cdots x_{m-2})^{-1} w_{m-1} w_m^{-1} x_1 x_2 \cdots x_{m-2}, \\ x_m &= (x_1 x_2 \cdots x_{m-1})^{-1} w_m x_1^{-1}, \end{aligned}$$

из которых видно, что слова (3) порождают $\mathcal{FG}(\Sigma)$. Мы готовы теперь доказать теорему 1.

Доказательство теоремы 1. Итак, пусть $\mathcal{S}$ – конечная полугруппа, а $\mathcal{G}$ – прямое произведение всех ее максимальных подгрупп. Мы хотим указать полиномиальное сведéние задачи CHECK-ID($\mathcal{G}$) к задаче CHECK-ID($\mathcal{S}$). Для этого рассмотрим произвольные входные данные задачи CHECK-ID($\mathcal{G}$), т.е. произвольную пару слов $u, v \in \Sigma^+$, где $\Sigma = \{x_1, \ldots, x_m\}$ – некоторый алфавит. Возьмем соответствующий набор слов (3) и, как и в доказательстве леммы 2.2, для каждого $k = 1, 2, \ldots$ положим

$$[w_1, \ldots, w_m]^k = [w_{1,k}, \ldots, w_{m,k}].$$

Пусть ℓ – максимальная длина $\leqslant_{\mathfrak{J}}$-цепи без $\mathfrak{J}$-эквивалентных элементов в $\mathcal{S}$. Покажем, что тождество

$$u(x_1, \ldots, x_m) \doteq v(x_1, \ldots, x_m) \tag{4}$$

выполняется в группе $\mathcal{G}$ тогда и только тогда, когда тождество

$$u(w_{1,2\ell}, \ldots, w_{m,2\ell}) \backsimeq v(w_{1,2\ell}, \ldots, w_{m,2\ell}) \tag{5}$$

выполняется в полугруппе $\mathcal{S}$.

Предположим сначала, что тождество (4) выполнено в $\mathcal{G}$. Рассмотрим произвольный гомоморфизм $\zeta : \Sigma^+ \to \mathcal{S}$. Как отмечалось выше, слова (3) удовлетворяют условиям леммы 2.2, а потому значения слов $w_{1,2\ell}, \ldots, w_{m,2\ell}$ при рассматриваемом гомоморфизме принадлежат некоторой подгруппе $\mathcal{H}$ полугруппы $\mathcal{S}$. Поскольку $\mathcal{H}$ является подгруппой также и в группе $\mathcal{G}$, в $\mathcal{H}$ выполняется тождество (4), и следовательно, при подстановке в него вместо переменных $x_1, \ldots, x_m$ значений слов $w_{1,2\ell}, \ldots, w_{m,2\ell}$ получается верное равенство

$$u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta).$$

Однако

$$u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = u(w_{1,2\ell}, \ldots, w_{m,2\ell})\zeta,$$
$$v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(w_{1,2\ell}, \ldots, w_{m,2\ell})\zeta;$$

другими словам, на выражения

$$u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) \quad \text{и} \quad v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta)$$

можно смотреть и как на результат применения гомоморфизма ζ соответственно к словам $u(w_{1,2\ell}, \ldots, w_{m,2\ell})$ и $v(w_{1,2\ell}, \ldots, w_{m,2\ell})$. Поскольку значения этих слов при произвольном гомоморфизме из Σ^+ в $\mathcal{S}$ оказались равными, тождество (5) выполнено в полугруппе $\mathcal{S}$.

Теперь допустим, что тождество (5) выполнено в полугруппе $\mathcal{S}$, и покажем, что тождество (4) выполнено в ее произвольной подгруппе $\mathcal{H}$. Так как слова (3) порождают свободную группу $\mathcal{FG}(\Sigma)$, продолжение ψ эндоморфизма $[w_1, \ldots, w_m]$ на $\mathcal{FG}(\Sigma)$ будет сюръекцией. Но тогда сюръекцией будет и любая степень ψ, в частности, $\psi^{2\ell}$. Отсюда следует, что компоненты эндоморфизма $[w_1, \ldots, w_m]^{2\ell}$, т.е. слова $w_{1,2\ell}, \ldots, w_{m,2\ell}$ также порождают свободную группу $\mathcal{FG}(\Sigma)$. Поэтому к словам $w_{1,2\ell}, \ldots, w_{m,2\ell}$ применима лемма 2.3, согласно которой для любых элементов $h_1, \ldots, h_m \in \mathcal{H}$ существует такой гомоморфизм $\zeta : \Sigma^+ \to \mathcal{H}$, что $w_{i,2\ell}\zeta = h_i$ для всех $i = 1, \ldots, m$. Поскольку тождество (5) выполнено в полугруппе $\mathcal{S}$, оно выполнено и в ее подгруппе $\mathcal{H}$. Поэтому справедливы равенства

$$u(h_1, \ldots, h_m) = u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) =$$

$$= v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(h_1, \ldots, h_m),$$

которые показывают, что слова $u(x_1, \ldots, x_m)$ и $v(x_1, \ldots, x_m)$ принимают одинаковые значения при любой замене входящих в них букв элементами подгруппы $\mathcal{H}$. Это и означает, что тождество (4) выполнено в $\mathcal{H}$. Тождества переносятся на прямые произведения, поэтому (4) выполнено и в $\mathcal{G}$.

Отметим теперь, что длина каждого из слов (3) не превосходит $m+2$, а потому длина каждого из слов $w_{1,2\ell}, \ldots, w_{m,2\ell}$ не превосходит $(m+2)^{2\ell}$. При этом параметр ℓ определяется полугруппой $\mathcal{S}$ и, следовательно, не зависит от размера входных данных (u, v) (т.е. от суммы длин слов u и v), а параметр m не превосходит этого размера. Так как длина слова $u(w_{1,2\ell}, \ldots, w_{m,2\ell})$ (соответственно $v(w_{1,2\ell}, \ldots, w_{m,2\ell})$) не превосходит произведения максимума длин слов $w_{i,2\ell}$ на длину слова u (соответственно v), мы видим, что проверка произвольного тождества (4) в группе $\mathcal{G}$ сводится к проверке в полугруппе $\mathcal{S}$ некоторого тождества, размер которого ограничен полиномом от размера тождества (4). Теорема 1 доказана. □

Как уже отмечалось в §1, следствие 1 немедленно вытекает из сопоставления теоремы 1 с результатом работы [12] о co-NP-полноте задачи проверки тождеств в конечной неразрешимой группе.

Доказательство следствия 2. По классической теореме Жордана–Диксона (см., например, [2, §4.2]) группа обратимых $n \times n$-матриц над конечным полем $\mathcal{K}$ неразрешима за исключением двух случаев: $n = 2$, $|\mathcal{K}| = 2$ и $n = 2$, $|\mathcal{K}| = 3$. По следствию 1 мы заключаем, что задача проверки тождеств в полугруппе $n \times n$-матриц над $\mathcal{K}$ является co-NP-полной, если $n \geqslant 3$ или $|\mathcal{K}| \geqslant 4$. Два упомянутых выше исключительных случая разобраны соответственно в [27] и [28]. □

§3. Доказательство теоремы 2

Полугруппу всех преобразований n-элементного множества будем обозначать через $\mathcal{T}_n$. Поскольку мы записываем преобразования справа от аргумента, произведение двух преобразований в $\mathcal{T}_n$ – это результат их последовательного выполнения в том порядке, в котором они записаны. Отметим, что на сложность задачи проверки тождеств это соглашение не влияет, – полугруппа $\overleftarrow{\mathcal{T}_n}$ всех "левых" преобразований n-элементного множества антиизоморфна $\mathcal{T}_n$ и удовлетворяет некоторому тождеству тогда и только тогда, когда в $\mathcal{T}_n$ выполняется зеркальное отражение этого тождества.

Еще Галуа установил, что при $n \geqslant 5$ группа $\mathcal{S}_n$ всех перестановок n-элементного множества неразрешима, а потому, как уже отмечалось в §1, заключение теоремы 2 при $n \geqslant 5$ сразу же вытекает из следствия 1. Полугруппа $\mathcal{T}_1$ одноэлементна, а потому задача проверки тождеств в ней тривиальна: любое тождество выполняется в $\mathcal{T}_1$. Полугруппа $\mathcal{T}_2$ четырехэлементна, что позволяет применить результат Климы [19, предложение 4], согласно которому задача CHECK-ID($\mathcal{S}$) разрешима за полиномиальное время для любой не более чем пятиэлементной полугруппы $\mathcal{S}$ с единицей. Учитывая, что работа [19] пока не опубликована, для удобства читателя мы приведем здесь полиномиальный алгоритм для проверки тождеств в $\mathcal{T}_2$, не использующий ни упомянутый общий результат, ни результаты диссертации Тессона [31], на которые опирается Клима.

Пусть Σ – некоторый алфавит. Назовем *кратностью* буквы $x \in \Sigma$ в слове $w \in \Sigma^+$ число различных вхождений x в w в качестве фактора, т.е. число различных представлений вида $w = uxv$, где u, v – возможно пустые слова. Через $\operatorname{suff}_x(w)$ обозначим максимальный суффикс слова w, не содержащий вхождения буквы x. Заметим, что $\operatorname{suff}_x(w) = w$, если x не входит в w.

Предложение 3.1. *Тождество $u \eqsim v$ справедливо в полугруппе $\mathcal{T}_2$ тогда и только тогда, когда для любых двух букв x и y кратности y в словах $\operatorname{suff}_x(u)$ и $\operatorname{suff}_x(v)$ имеют одинаковую четность и одновременно равны 0 или отличны от 0.*

Доказательство. *Необходимость.* Будем считать, что преобразования из $\mathcal{T}_2$ действуют на множестве $\{1, 2\}$, и договоримся обозначать через $\binom{12}{ij}$ преобразование, отображающее 1 в i, а 2 – в j, где $i, j \in \{1, 2\}$. Единичную перестановку $\binom{12}{12}$ будем обозначать через ε.

Рассмотрим сначала случай, когда буква x не входит в слова u и v. Допустим, что кратности буквы y в словах $\operatorname{suff}_x(u) = u$ и $\operatorname{suff}_x(v) = v$ имеют разную четность. Тогда при подстановке $y \mapsto \binom{12}{21}$, $z \mapsto \varepsilon$ при всех $z \neq y$ значение слова с нечетной кратностью y равно $\binom{12}{21}$, в то время как значение слова с четной кратностью y есть ε. Значит, такое тождество $u \eqsim v$ неверно в $\mathcal{T}_2$. Допустим теперь, что кратность буквы y в одном из рассматриваемых слов, скажем, в u, отлична от 0, а в другое слово y не входит. Тогда при подстановке $y \mapsto \binom{12}{11}$, $z \mapsto \varepsilon$ при всех $z \neq y$ значение слова u равно $\binom{12}{11}$, в то время как значение слова v есть ε. Значит, и в этом случае тождество $u \eqsim v$ ложно в $\mathcal{T}_2$.

Пусть теперь x входит в одно из слов u или v. По доказанному, x

входит и в другое слово. Допустим, что кратности буквы y в словах $\mathrm{suff}_x(u)$ и $\mathrm{suff}_x(v)$ имеют разную четность. Рассмотрим подстановку $x \mapsto \binom{12}{11}$, $y \mapsto \binom{12}{21}$, $z \mapsto \varepsilon$ при всех $z \neq x, y$. Легко видеть, что при такой подстановке значение слова с нечетной кратностью y в максимальном суффиксе, не содержащем вхождения x, равно $\binom{12}{22}$, в то время как значение другого слова равно $\binom{12}{11}$. Снова видим, что тождество $u \doteq v$ опровергается в $\mathcal{T}_2$. Наконец, допустим, что буква y входит только в одно из слов $\mathrm{suff}_x(u)$ или $\mathrm{suff}_x(v)$, скажем, в первое. Рассмотрим подстановку $x \mapsto \binom{12}{11}$, $y \mapsto \binom{12}{22}$, $z \mapsto \varepsilon$ при всех $z \neq x, y$. Значение слова u при этой подстановке равно $\binom{12}{22}$, а значение слова v равно $\binom{12}{11}$. Следовательно, и в этом случае тождество $u \doteq v$ не выполнено в $\mathcal{T}_2$.

Достаточность. Пусть Σ – множество всех букв, входящих в слова u и v. Рассмотрим произвольный гомоморфизм $\zeta : \Sigma^+ \to \mathcal{T}_2$. Если образ ζ содержится в группе $\mathcal{S}_2$, то уже то условие, что кратности каждой буквы в словах u и v имеют одинаковую четность, обеспечивает равенство $u\zeta = v\zeta$. В противном случае, пусть x – "самая правая" в u буква с тем свойством, что $x\zeta \notin \mathcal{S}_2$, т.е. $y\zeta \in \mathcal{S}_2$ для любой буквы y, входящей в $\mathrm{suff}_x(u)$. Тогда равенство $u\zeta = v\zeta$ вытекает из условия, что в $\mathrm{suff}_x(u)$ и $\mathrm{suff}_x(v)$ входят одни и те же буквы и притом с кратностями одинаковой четности. □

Ясно, что условие предложения 3.1 можно проверить за полиномиальное (в действительности даже за линейное) время от суммы длин слов u и v. Отметим, что необходимость этого условия по существу установлена Эдмундсом [11, лемма 4.5]. (Моноид M_{31}, рассматриваемый Эдмундсом в указанной лемме, есть не что иное как полугруппа $\overleftarrow{\mathcal{T}_2}$ с присоединенным нулем; этот моноид и $\overleftarrow{\mathcal{T}_2}$ удовлетворяют одним и тем же тождествам.) Более ранняя характеризация тождеств полугруппы $\overleftarrow{\mathcal{T}_2}$, данная Симельгор [5], использует рекурсию по подмножествам алфавита и без дополнительного анализа еще не приводит к полиномиальному алгоритму для задачи CHECK-ID($\overleftarrow{\mathcal{T}_2}$).

Оставшаяся часть параграфа посвящена случаю $n = 3$. Отметим, что к полугруппе $\mathcal{T}_3$ нельзя применить сведéние из теоремы 1, так как все подгруппы в $\mathcal{T}_3$ изоморфно вкладываются в $\mathcal{S}_3$, а последняя подгруппа диэдральна, и стало быть, задача CHECK-ID($\mathcal{S}_3$) полиномиально разрешима [10]. Тем не менее, мы покажем, что сама задача CHECK-ID($\mathcal{T}_3$) является co-NP-полной; доказательство использует технику, предложенную в [27].

Через $\mathcal{T}_3(m)$ будем обозначать множество всех таких преобразований из $\mathcal{T}_3$, образ которых состоит из m элементов. Тогда полугруппа $\mathcal{T}_3$ разбивается на множества $\mathcal{T}_3(3) = \mathcal{S}_3$, $\mathcal{T}_3(2)$ и $\mathcal{T}_3(1)$. Будем считать, что все рассматриваемые преобразования действуют на множестве $\{1,2,3\}$, и сопоставим каждому преобразованию $\varphi \in \mathcal{T}_3(2)$ его ядро $\ker\varphi$, т.е. такое разбиение множества $\{1,2,3\}$ на два класса, что числа $i,j \in \{1,2,3\}$ находятся в одном классе тогда и только тогда, когда $i\varphi = j\varphi$, и его образ $\operatorname{Im}\varphi$, т.е. двухэлементное подмножество $\{1\varphi, 2\varphi, 3\varphi\}$ множества $\{1,2,3\}$. Если ξ – разбиение множества $\{1,2,3\}$ на два класса, а A – двухэлементное подмножество в $\{1,2,3\}$, будем писать $A \in \xi$, если A совпадает с одним из ξ-классов. Вполне очевидна следующая лемма.

Лемма 3.2. *Если $\varphi, \psi \in \mathcal{T}_3(2)$, то $\varphi\psi \in \mathcal{T}_3(1)$ тогда и только тогда, когда $\operatorname{Im}\varphi \in \ker\psi$.*

Отметим, что перестановки $\pi \in \mathcal{S}_3$ естественным образом действуют как на множестве всех двухэлементных подмножеств в $\{1,2,3\}$, так и на множестве всех разбиений множества $\{1,2,3\}$ на два класса. При этом очевидна следующая лемма.

Лемма 3.3. *Если $\varphi \in \mathcal{T}_3(2)$, $\pi \in \mathcal{S}_3$, то $\pi\varphi, \varphi\pi \in \mathcal{T}_3(2)$, причем:*

- $\ker(\pi\varphi) = (\ker\varphi)\,\pi^{-1}$, $\operatorname{Im}(\pi\varphi) = \operatorname{Im}\varphi$;
- $\ker(\varphi\pi) = \ker\varphi$, $\operatorname{Im}(\varphi\pi) = (\operatorname{Im}\varphi)\,\pi$.

Используя индукцию, из лемм 3.2 и 3.3 нетрудно извлечь следующий результат.

Лемма 3.4. *Пусть $\varphi_1, \ldots, \varphi_n \in \mathcal{T}_3(2)$, $\pi_1, \ldots, \pi_{n+1} \in \mathcal{S}_3$. Произведение $\psi = \pi_1\varphi_1\pi_2\varphi_2\cdots\pi_n\varphi_n\pi_{n+1}$ лежит в $\mathcal{T}_3(1)$ тогда и только тогда, когда найдется индекс $k \in \{1,\ldots,n-1\}$, такой, что $(\operatorname{Im}\varphi_k)\,\pi_{k+1} \in \ker\varphi_{k+1}$. При этом, если $\psi \in \mathcal{T}_3(2)$, то $\ker\psi = (\ker\varphi_1)\,\pi_1^{-1}$, $\operatorname{Im}\psi = (\operatorname{Im}\varphi_n)\,\pi_{n+1}$.*

Для дальнейшего анализа полезно и такое следствие лемм 3.2 и 3.3.

Лемма 3.5. *Для любого цикла $\pi \in \{(123),(132)\}$ и любого преобразования $\varphi \in \mathcal{T}_3(2)$ произведение $\varphi\pi\varphi\pi^2\varphi^2$ принадлежит $\mathcal{T}_3(1)$.*

Доказательство. Двухэлементные множества $\operatorname{Im}\varphi$, $\operatorname{Im}(\varphi\pi)$ и $\operatorname{Im}(\varphi\pi^2)$ попарно различны, и потому одно из них есть класс разбиения $\ker\varphi$. □

Зафиксируем еще следующее элементарное соображение.

Лемма 3.6. *Для любого преобразования $\varphi \in \mathcal{T}_3(2)$ выполнено равенство $\varphi^2 = \varphi^4$, а если $\varphi^2 \in \mathcal{T}_3(2)$, то выполнено даже равенство $\varphi = \varphi^3$.*

Доказательство. Пусть сначала $\varphi^2 \in \mathcal{T}_3(2)$. Тогда $\operatorname{Im}\varphi = \operatorname{Im}(\varphi^2)$, т.е. φ действует на двухэлементном множестве $\operatorname{Im}\varphi$ как перестановка. Отсюда φ^2 действует на $\operatorname{Im}\varphi$ как единичная перестановка, а это значит, что $\varphi = \varphi^3$.

Если же $\varphi^2 \in \mathcal{T}_3(1)$, то $\varphi^2 = \varphi^4$, поскольку любое константное преобразование идемпотентно. □

Предложение 3.7. *Задача* CHECK-ID($\mathcal{T}_3$) co-NP-*полна.*

Доказательство. Рассмотрим задачу 6-РАСКРАСКА, входными данными которой служат всевозможные простые (т.е. без петель и кратных ребер) графы Γ, а ответами – "ДА" или "НЕТ" в зависимости от того, можно ли раскрасить вершины графа Γ в шесть цветов так, чтобы цвета любых двух смежных вершины различались. Легко видеть, что задача 6-РАСКРАСКА принадлежит классу сложности NP и что к ней полиномиально сводится (с помощью известной конструкции композиции графов, см., например, [1, §6.2]) классическая NP-полная задача 3-РАСКРАСКА. Поэтому задача 6-РАСКРАСКА также является NP-полной.

Зафиксируем теперь произвольный простой граф $\Gamma = (V, E)$ без изолированных вершин. Мы построим по нему некоторое тождество $p \doteq q$, размер которого (т.е. сумма длин слов p и q) ограничен полиномом от числа вершин Γ, и покажем, что граф Γ имеет 6-раскраску тогда и только тогда, когда тождество $p \doteq q$ ложно в полугруппе $\mathcal{T}_3$. Поскольку добавление или удаление изолированных вершин не влияет на хроматическое число графа, мы получим полиномиальное сведéние задачи 6-РАСКРАСКА к отрицанию задачи CHECK-ID($\mathcal{T}_3$). Отсюда и будет следовать, что задача CHECK-ID($\mathcal{T}_3$) co-NP-полна.

Будем строить наше тождество над алфавитом $\Sigma = V \cup E \cup \{x\}$, где x – некоторая "новая" буква, не входящая в множества V и E. Каждому ребру $e_i \in E$ мы сопоставим слово $w_i = e_i v_j v_k^5 e_i^5 v_k v_j^5$, где вершины v_j, $v_k \in V$ суть концы ребра e_i. Зафиксируем некоторый порядок перечисления ребер и пар различных ребер графа Γ и рассмотрим произведения

$$P = \prod_{e_i \in E} (x w_i^4)^6, \quad Q = \prod_{e_i \in E} (x w_i^6)^6, \quad H = \prod_{e_i, e_j \in E} (w_i w_j w_i w_j^2 w_i^2)^6,$$

в которых сомножители, соответствующие ребрам и парам ребер, перечисляются в выбранном порядке. Положим $p = PP^2PxH$, $q = PQ^2PxH$. Тогда тождество $p \doteq q$ и будет искомым.

Легко подсчитать, что сумма длин так построенных слов p и q ограничена квадратичным полиномом от числа ребер графа Γ, а следовательно, полиномом четвертой степени от числа его вершин. Остается проверить, что тождество $p \doteq q$ ложно в полугруппе $\mathcal{T}_3$ тогда и только тогда, когда граф Γ имеет 6-раскраску.

Допустим сначала, что вершины графа Γ можно раскрасить в 6 цветов. Тогда существует такое отображение $\zeta : V \to \mathcal{S}_3$, что $v_j\zeta \neq v_k\zeta$ для любых двух смежных вершин $v_j, v_k \in V$. Учитывая, что в группе $\mathcal{S}_3$ выполнено тождество $x^6 \doteq 1$, и продолжая ζ на множество V^+ всех слов над алфавитом V, можно переписать предыдущее неравенство в виде $\left(v_jv_k^5\right)\zeta \neq \varepsilon$, где через ε обозначена единичная перестановка $\binom{123}{123}$. Поскольку $\mathcal{S}_3$ – группа без центра, существует перестановка $\pi_{jk} \in \mathcal{S}_3$, которая не коммутирует с перестановкой $\left(v_jv_k^5\right)\zeta$. Продолжим теперь отображение ζ на множество $(V \cup E)^+$, полагая $e_i\zeta = \pi_{jk}$, где j и k определяются из условия, что вершины v_j и v_k суть концы ребра e_i. Итак, $\left(e_iv_jv_k^5\right)\zeta \neq \left(v_jv_k^5e_j\right)\zeta$, откуда, снова используя тождество $x^6 \doteq 1$, мы заключаем, что $w_i\zeta = \left(e_iv_jv_k^5e_i^5v_kv_j^5\right)\zeta \neq \varepsilon$. Очевидно, что $w_i\zeta$ – четная перестановка, т.е. $w_i\zeta$ есть один из циклов (123) или (132). В частности, $w_i^4\zeta = w_i\zeta$.

Наконец, продолжим ζ до гомоморфизма $\Sigma^+ \to \mathcal{T}_3$, полагая $x\zeta = \varphi$, где $\varphi = \binom{123}{233}$. Заметим, что $\operatorname{Im}\varphi = \{2,3\} \in \ker\varphi = 1 \mid 23$, но если π – любой из циклов (123) или (132), то $\operatorname{Im}(\varphi\pi) \notin \ker\varphi$. Поэтому из леммы 3.4 вытекает, что $(PP^2Px)\zeta \in \mathcal{T}_3(2)$, а поскольку $H\zeta = \varepsilon$, мы заключаем, что и $p\zeta \in \mathcal{T}_3(2)$. С другой стороны, ясно, что $(xw_i^6)^6\zeta = \varphi^2 = \binom{123}{333}$ для любого i, откуда $q\zeta \in \mathcal{T}_3(1)$. Итак, $p\zeta \neq q\zeta$, и тождество $p \doteq q$ не выполняется в полугруппе $\mathcal{T}_3$.

Обратно, предположим, что тождество $p \doteq q$ ложно в $\mathcal{T}_3$, т.е. $p\zeta \neq q\zeta$ при некотором гомоморфизме $\zeta : \Sigma^+ \to \mathcal{T}_3$. Сначала мы покажем, что при таком гомоморфизме образ буквы x должен быть некоторым преобразованием из $\mathcal{T}_3(2)$, квадрат которого лежит в $\mathcal{T}_3(1)$, а образ каждого слова w_i должен быть неединичной перестановкой из $\mathcal{S}_3$. Для этого мы исключим все другие априори возможные случаи расположения элементов $x\zeta$ и $w_i\zeta$ внутри полугруппы $\mathcal{T}_3$.

Прежде всего, заметим, что у слов p и q есть общий суффикс PxH. Если его образ при гомоморфизме ζ принадлежит $\mathcal{T}_3(1)$, т.е. является

константным преобразованием, то $p\zeta = (PxH)\zeta = q\zeta$, что противоречит выбору тождества $p \eqsim q$ и гомоморфизма ζ. Отсюда, в частности, $x\zeta \notin \mathcal{T}_3(1)$ и $w_i\zeta \notin \mathcal{T}_3(1)$ для всех i. Кроме того, если $x^2\zeta \in \mathcal{T}_3(1)$, то $w_i\zeta \neq \varepsilon$ для всех i. Действительно, в противном случае образ входящего в общий суффикс PxH фактора xw_i^4x является константным преобразованием.

Теперь допустим, что $w_i\zeta \in \mathcal{T}_3(2)$ для некоторого i. Если найдется такой индекс j, что $w_j\zeta \in \mathcal{S}_3\backslash\{\varepsilon\}$, то с учетом того, что перестановка $w_j\zeta$ четная, можно применить лемму 3.5 к образу фактора $w_iw_jw_iw_j^2w_i^2$ слова H, и образ общего суффикса PxH снова оказывается константным преобразованием, противоречие. Если же $w_i\zeta \in \mathcal{T}_3(2) \cup \{\varepsilon\}$ для всех i, то по лемме 3.6 имеем $w_i^2\zeta = w_i^4\zeta = w_i^6\zeta$, откуда $P\zeta = Q\zeta$ и $p\zeta = q\zeta$, противоречие.

Мы доказали, что $w_i\zeta \in \mathcal{S}_3$ для всех i. Если допустить, что и $x\zeta \in \mathcal{S}_3$, то в силу выполненного в $\mathcal{S}_3$ тождества $x^6 \eqsim 1$ и строения слов P, Q и H справедливы равенства $P\zeta = Q\zeta = H\zeta = \varepsilon$. Но тогда $p\zeta = q\zeta = x\zeta$, противоречие. Предположим, что $x^2\zeta \in \mathcal{T}_3(2)$. В этом случае $H\zeta = \varepsilon$ и $w_i^6\zeta = \varepsilon$. Отсюда, обозначая $x\zeta$ через φ, $P\zeta$ через ψ и учитывая лемму 3.6, получаем

$$q\zeta = (PQ^2PxH)\zeta = \psi(\varphi^6\cdots\varphi^6)^2\psi\varphi = \psi\varphi^2\psi\varphi. \tag{6}$$

Теперь заметим, что слово P начинается с буквы x, откуда $\psi = \varphi\chi$ для некоторого χ и $\varphi^2\psi = \varphi^3\chi = \varphi\chi = \psi$ по лемме 3.6. С учетом этого равенство (6) означает, что $q\zeta = \psi^2\varphi$. С другой стороны, в тех же обозначениях имеем $p\zeta = (PP^2Px)\zeta = \psi^4\varphi$. Ясно, что преобразование ψ принадлежит либо $\mathcal{T}_3(2)$, либо $\mathcal{T}_3(1)$. Отсюда $\psi^2 = \psi^4$, поскольку в первом случае применима лемма 3.6, а во втором – преобразование ψ константное, а значит, идемпотентное. Итак, $p\zeta = \psi^4\varphi = \psi^2\varphi = q\zeta$, противоречие.

Таким образом, мы установили, что возможна только следующая конфигурация: $x\zeta \in \mathcal{T}_3(2)$, $x^2\zeta \in \mathcal{T}_3(1)$ и $w_i\zeta \in \mathcal{S}_3\backslash\{\varepsilon\}$ для каждого i. Напомним, что $w_i = e_iv_jv_k^5e_i^5v_kv_j^5$, где вершины v_j, $v_k \in V$ суть концы ребра e_i. В силу выполненного в $\mathcal{S}_3$ тождества $x^6 \eqsim 1$ неравенство $w_i\zeta \neq \varepsilon$ возможно только, если $v_j\zeta \neq v_k\zeta$. Следовательно, гомоморфизм ζ сопоставляет любой паре смежных вершин графа Γ пару различных элементов группы $\mathcal{S}_3$ и тем самым задает 6-раскраску графа Γ.

Предложение 3.7 доказано, а вместе с ним доказана и теорема 2. $\square$

Литература

1. М. Гэри, Д. Джонсон, *Вычислительные машины и труднорешаемые задачи.* Мир, М., 1982.
2. М. И. Каргаполов, Ю. И. Мерзляков. *Основы теории групп.* Наука, М., 1972.
3. Р. Линдон, П. Шупп, *Комбинаторная теория групп.* Мир, М., 1980.
4. С. В. Плещева, В. Вертеши, *Сложность задачи проверки тождеств в 0-простой полугруппе.* — Изв. Урал. гос. ун-та, No. 43, Компьютерные науки информационные технологии, Вып. 1 (2006), 72–102.
5. Е. П. Симельгор, *Тождества в конечной симметрической полугруппе.* — Современ. алгебра **1** (1974), 174–188.
6. 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), сс. 16–17.
7. J. Almeida, M. V. Volkov, *Subword complexity of profinite words and subgroups of free profinite semigroups.* — Int. J. Algebra and Computation **16**, No. 2 (2006), 221–258.
8. C. Bergman, G. Slutzki, *Complexity of some problems concerning varieties and quasi-varieties of algebras.* — SIAM J. Comput. **30**, No. 2 (2000), 359–382.
9. S. Burris, J. Lawrence, *The equivalence problem for finite rings.* — J. Symbolic Computation **15**, No. 1 (1993), 67–71.
10. S. Burris, J. Lawrence, *Results on the equivalence problem for finite groups.* — Algebra Universalis **52**, No. 4 (2005), 495–500.
11. C. C. Edmunds, *On certain finitely based varieties of semigroups.* — Semigroup Forum **15**, No. 1 (1977), 21–39.
12. G. Horváth, J. Lawrence, L. Mérai, Cs. Szabó, *The complexity of the equivalence problem for nonsolvable groups.* — Bull. London Math. Soc **39**, No. 3 (2007), 433–438.
13. G. Horváth, Cs. Szabó, *The complexity of checking identities over finite groups.* — Int. J. Algebra and Computation **16**, No. 5 (2006), 931–939.
14. H. B. Hunt III, R. E. Stearns, *The complexity of equivalence for commutative rings.* — J. Symbolic Computation **10**, No. 5 (1990), 411–436.
15. M. Jackson, R. McKenzie, *Interpreting graph colorability in finite semigroups.* — Int. J. Algebra and Computation **16**, No. 1 (2006), 119–140.
16. J. Kalicki, *On comparison of finite algebras.* — Proc. Amer. Math. Soc. **3**, No. 1 (1952), 36–40.
17. O. G. Kharlampovich, M. V. Sapir, *Algorithmic problems in varieties.* — Int. J. Algebra and Computation **5**, Nos. 4–5 (1995), 379–602.
18. A. Kisielewicz, *Complexity of semigroup identity checking.* — Int. J. Algebra and Computation **14**, No. 4 (2004), 455–464.
19. O. Klíma, *Complexity issues of checking identities in finite monoids.* — Semigroup Forum (в печати).
20. M. Kozik, *On Some Complexity Problems in Finite Algebras.* PhD Dissertation, Vanderbilt University, Nashville, 2004.

21. M. Kozik, *Computationally and algebraically complex finite algebra membership problems.* — Int. J. Algebra and Computation **17**, No. 8 (2007), 1635-Ц1666.
22. M. Kozik, *Varietal membership problem is* 2-EXPTIME *complete* (в печати).
23. C. H. Papadimitriou, *Computational Complexity.* Reading–Menlo Park–N. Y.: Addison-Wesley Publishing Company, 1994.
24. J.-E. Pin, *Varieties of Formal Languages.* Oxford: North Oxford Academic and N. Y.: Plenum, 1986.
25. S. Seif, *The Perkins semigroup has* co-NP*-complete term-equivalence problem.* — Int. J. Algebra and Computation **15**, No. 2 (2005), 317–326.
26. S. Seif, Cs. Szabó, *Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields.* — Semigroup Forum **72**, No. 2 (2006), 207–222.
27. Cs. Szabó, V. Vértesi, *The complexity of the word-problem for finite matrix rings.* — Proc. Amer. Math. Soc. **132**, No. 12 (2004), 3689–3695.
28. Cs. Szabó, V. Vértesi, *The complexity of checking identities for finite matrix rings.* — Algebra Universalis **51**, No. 4 (2004), 439–445.
29. Cs. Szabó, V. Vértesi, *The identity checking problem in finite rings* (в печати).
30. Z. Székely, *Computational complexity of the finite algebra membership problem for varieties.* — Int. J. Algebra and Computation **12**, No. 6 (2002), 811–823.
31. P. Tesson, *Computational Complexity Questions Related to Finite Monoids and Semigroups.* PhD Thesis, McGill University, Montréal, 2003.

Almeida J., Volkov M. V., Goldberg S. V. Complexity of the identity checking problem for finite semigroups.

We prove that the identity checking problem in a finite semigroup S is co-NP-complete whenever S has a nonsolvable subgroup or S is the semigroup of all transformations on a 3-element set.

Департамент чистой математики,
Факультет естественных наук,
Университет Порту, Португалия

Поступило 4 июня 2007 г.

Уральский государственный университет,
Екатеринбург, Россия

E-mail: Mikhail.Volkov@usu.ru