# АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ ДЛЯ УРАВНЕНИЙ В СВОБОДНЫХ ГРУППАХ И ПОЛУГРУППАХ С ОГРАНИЧЕНИЯМИ НА РЕШЕНИЯ

**В. Г. Дурнев, А. И. Зеткина**

*Ярославский государственный университет им. П. Г. Демидова*

## Введение

Жозеф Альфред Серре. Курс высшей алгебры. Русский перевод. 1910.

“Алгебра – это, по сути, жонглирование уравнениями”

Другой вариант перевода

“Алгебра – это, по сути, анализ уравнений”

Современная точка зрения с начала XX века.

Алгебра – это наука об алгебраических операциях. Алгебра изучает алгебраические структуры или даже алгебраические системы.

Евклид (325 – 270 г.г. до н.э., III век до н.э.)

Диофант (предположительно III век н.э.) начал изучать уравнения с рациональными (положительными) ограничениями на решения, т.е. системы вида

$$F(x_1, \ldots, x_n) \;=\; G(x_1, \ldots, x_n) \;\&\; \mathop{\&}_{i=1}^{n} x_i \in \mathbb{Q}_+,$$

где $F(x_1, \ldots, x_n)$ и $G(x_1, \ldots, x_n)$ – многочлены с положительными рациональными коэффициентами, т.е. многочлены над множеством положительных рациональных чисел $\mathbb{Q}_+$. Диофанта интересовал вопрос о нахождении какого-нибудь рационального решения этого и нахождение (получение, описание) всех рациональных решений, отправляясь, как правило, от одного известного решения.

Вопрос, имеет ли решение эта система не обсуждался, в частности, из-за определенной простоты рассматривавшихся уравнений – они имели, как правило, степень 2 и лишь две неизвестные и одно решение обычно легко находилось..

Пьер Ферма (1601-1665 гг.) Во “Втором вызове математикам” (британским) (1657 г.) рассматривает уравнение с ограничением на решение

$$ax^2 + 1 = y^2 \,\&\, x, y \in \mathbb{N}$$

и предлагает доказать, что оно всегда имеет (натуральное) решение, если $a$ не является полным квадратом и найти какое-нибудь решение при нескольких указанных в “Вызове” значениях $a$, в частности, при $a = 149109433$.

Это уравнение теперь хорошо известно, с “легкой руки” оно называется уравнение Пелля и записывается в виде

$$x^2 - ay^2 = 1.$$

С тех пор изучение уравнений и их систем с различными ограничениями на решения – важная задача теории чисел, алгебры и теории алгоритмов.

Напомним, что 10-я проблема Д. Гильберта – это вопрос о существовании общего метода (алгоритма), позволяющего по произвольному уравнению с ограничениями на решения вида

$$F(x_1, \ldots, x_n) = 0 \,\&\, \mathop{\&}_{i=1}^{n} x_i \in \mathbb{Z},$$

где $F(x_1, \ldots, x_n)$ – многочлен над кольцом целых чисел $\mathbb{Z}$, определить, имеет ли оно решение.

Хорошо известно, что эта проблема решена отрицательно в работах М. Дэвиса, Дж. Робинсон, Х. Путнама и Ю.В. Матиясевича [1]. Отрицательно решается и равносильный предыдущему

вопросу вопрос о существовании алгоритма, позволяющего по произвольному уравнению с ограничениями на решения вида

$$F(x_1, \ldots, x_n) \;=\; 0 \;\&\; \mathop{\&}_{i=1}^{n} x_i \in \mathbb{N},$$

где $\mathbb{N}$ – множество натуральных чисел, определить, имеет ли оно решение.

Вопрос о существовании алгоритма, решающего проблему существования решения для уравнений с ограничениями на решения вида

$$F(x_1, \ldots, x_n) \;=\; 0 \;\&\; \mathop{\&}_{i=1}^{n} x_i \in \mathbb{Q},$$

где $\mathbb{Q}$ – поле рациональных чисел, в настоящее время открыт.

Вопрос о существовании алгоритма, решающего проблему существования решения для уравнений с ограничениями на решения вида

$$F(x_1, \ldots, x_n) \;=\; 0 \;\&\; \mathop{\&}_{i=1}^{n} x_i \in \mathbb{R},$$

где $\mathbb{R}$ – поле действительных чисел, достаточно давно положительно решен А. Тарским (1901 – 1983 гг.).

Более того А. Тарский разработал разрешающий алгоритм для элементарной теории поля действительных чисел, т.е. алгоритм, позволяющий по произвольной замкнутой формуле $\Phi$ в сигнатуре $\langle 0, 1, +, \cdot, \leq \rangle$ определить, истинна ли она на поле действительных чисел.

Ю.Л. Ершов и J. Ax and S. Kochen доказали разрешимость элементарной теории любого поля $\mathbb{Q}_p$ $p$-адических чисел. Напомним, что поле $\mathbb{R}$ действительных чисел и каждое поле $\mathbb{Q}_p$ $p$-адических чисел являются пополнением поля $\mathbb{Q}$ рациональных чисел относительно соответствующей нормы.

Напомним, что проблема разрешимости для уравнений с ограничениями на решения вида

$$F(x_1, \ldots, x_n) \,=\, 0 \,\&\, \mathop{\&}_{i=1}^{n} x_i \in \{\, 0,\, 1 \,\}$$

является $\mathbb{NP}$-полной.

Д. Гильберт (1862 – 1943 гг.):

Для произвольных многочленов $F_i(x_1, \ldots, x_n)(i \in I)$ с комплексными коэффициентами система

$$\mathop{\&}_{i \in I} F_i(x_1, \ldots, x_n) \,=\, 0 \,\mathop{\&}_{i=1}^{n} x_i \,\in\, \mathbb{C}$$

не имеет решения тогда и только тогда, когда многочлены $F_i(x_1, \ldots, x_n)(i \in I)$ порождают в кольце $\mathbb{C}[x_1, \ldots, x_n]$ единичный идеал, т.е. существуют такие многочлены $G_i(x_1, \ldots, x_n)(i \in I)$ с комплексными коэффициентами, для которых выполняется равенство

$$\sum_{i \in I} G_i(x_1, \ldots, x_n) F_i(x_1, \ldots, x_n) \,=\, 1.$$

## Уравнения в свободных группах, разрешенные относительно неизвестных, с ограничениями на решения

Обозначим через $F_m$ – свободную группу ранга $m$ со свободными образующими $a_1, \ldots, a_m$. При $m = 2$ вместо $a_1$ и $a_2$ будем писать $a$ и $b$ соответственно.

Уточним некоторые определения, относящиеся к системам уравнений в свободных группах.

*Системой уравнений* с неизвестными $x_1, \ldots, x_n$ в свободной группе $F_m$ называется выражение вида

$$\mathop{\&}_{i=1}^{k} w_i(x_1, \ldots, x_n, a_1, \ldots, a_m) = u_i(x_1, \ldots, x_n, a_1, \ldots, a_m), \tag{1}$$

где $w_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ и $u_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ – слова в алфавите

$$\{ x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}, a_1, a_1^{-1}, \ldots, a_m, a_m^{-1} \}.$$

Набор $\langle g_1, \ldots, g_n \rangle$ элементов группы $F_m$ называется *решением* системы (1), если при любом $i$ $(i = 1, \ldots, k)$ в группе $F_m$ выполняется равенство

$$w_i(g_1, \ldots, g_n, a_1, \ldots, a_m) = u_i(g_1, \ldots, g_n, a_1, \ldots, a_m).$$

Две системы уравнений с одними и теми же неизвестными называются *эквивалентными*, если множества их решений совпадают.

Используя уравнение

$$[x, a] = ([x, b]\, y^2)^2,$$

имеющее в свободной группе $F_m$ при любом $m \geq 2$ лишь тривиальное решение $x = 1$, $y = 1$, любую систему уравнений (1) можно заменить одним, ей равносильным, уравнением.

Для уравнений в свободных группах традиционно рассматриваются две основные задачи: проблема существования решения и проблема описания множества всех решений.

Исследование разрешимости уравнений в свободных группах было начато в конце 50-х годов в связи с проблемой разрешимости элементарных теорий свободных групп, поставленной А. Тарским [1]Этому вопросу посвящены, в частности, работы [2-5].

В 1982 году Г.С. Маканин [6] получил полное решение проблемы распознавания разрешимости уравнений в свободной группе. Он доказал, что если данное уравнение с длиной записи $d$ имеет решение в свободной группе, то длина каждой компоненты минимального (по максимальной длине компоненты) решения не превосходит числа $\Phi(d)$, где $\Phi(x)$ – некоторая рекурсивная функция. Это дает переборный алгоритм для распознавания разрешимости произвольного уравнения в свободной группе.

В связи с уже упоминавшейся выше проблемой А. Тарского о разрешимости элементарной теории произвольной свободной группы представляет интерес исследование алгоритмической природы фрагментов этой теории. Основные на сегодняшний день результаты в этой области получены Г.С. Маканиным. Вскоре после опубликования работы [6] ему удалось на том же пути доказать разрешимость экзистенциональной (универсальной) и позитивной теорий любой свободной группы [7]. При доказательстве разрешимости позитивной теории свободной группы Г.С. Маканин использовал результат Ю.И. Мерзлякова [8] об устранимости кванторов общности в позитивных формулах, относящихся к свободным группам.

А.А. Разборов [9] дал описание множества решений произвольной совместной системы уравнений в свободной группе.

**Где “проходит граница” между “Алгоритмически разрешимые проблемы” и “Алгоритмически неразрешимые проблемы”?**

**Где “проходит граница” между “Разрешимые (решаемые) проблемы” и “Неразрешимые (нерешаемые) проблемы”?**

**Где “проходит граница” между “Возможное” и “Невозможное”?**

**Какие дополнительные условия “превращают” “Алгоритмически разрешимую проблему” в “Алгоритмически неразрешимую проблему”?**

**“Интерполяция” между двумя “Мирами”: “Разрешимые (решаемые) проблемы” и “Неразрешимые (нерешаемые) проблемы”**

**“Интерполяция” между двумя “Мирами”: “Возможное” и “Невозможное”**

После построения Г.С. Маканиным [6] разрешающего алгоритма для систем уравнений в свободной группе $F_m$, особый интерес стал представлять вопрос о существовании аналогичных алгоритмов для уравнений в свободных группах с различными "не слишком сложными" ограничениями на решения.

Вопрос о разрешимости позитивной теории свободной группы был сведен Ю.И. Мерзляковым [8] к следующей проблеме:

*существует ли алгоритм, позволяющий для произвольного уравнения*

$$w\,(\,x_1,\,\ldots\,,\,x_n,\,a_1,\,\ldots\,,\,a_m\,)\,=\,1$$

*в свободной группе счетного ранга определить, имеет ли оно такое решение* $g_1$, ..., $g_n$, *что*

$$g_1\,\in\,F_{m_1},\;g_2\,\in\,F_{m_2},\,\ldots\,,\,g_t\,\in\,F_{m_t}\,,$$

*где* $m_1\,\leq\,m_2\,\leq\,\ldots\,\leq\,m_t$, $F_{m_i}$ *- свободная группа с образующими* $a_1,\ldots,a_{m_i}$.

Г.С. Маканиным [7] построил искомый алгоритм, и тем самым доказал разрешимость позитивной теории свободной группы.

Хорошо известно, что вопрос о точности матричного представления Гасснер [10,11] группы крашеных кос эквивалентен вопросу об отсутствии нетривиального решения в свободной группе $F_m$ уравнения

$$x_1 a_1 x_1^{-1} \cdot x_2 a_2 x_2^{-1} \cdots x_m a_m x_m^{-1} = a_1 \cdot a_2 \cdots a_m,$$

удовлетворяющего условию

$$x_1 \in F_m^{(2)}, \ldots, x_n \in F_m^{(2)},$$

где $F_m^{(2)}$ – второй коммутант свободной группы $F_m$. Напомним, что для произвольной группы $G$ через $G^{(2)}$ обозначается ее второй коммутант, т.е. $G^{(2)} = [G^{(1)}, G^{(1)}]$, где $G^{(1)} = [G, G]$ – коммутант группы $G$. Кроме того при произвольном $t$ $G^{(t+1)} = [G^{(t)}, G^{(t)}]$ и $G^{(0)} = G$.

Обобщая эти ситуации Г.С. Маканин поставил в “Коуровской тетради” [12] следующую проблему для уравнений в свободных группах

9.25. *Указать алгоритм, который по уравнению*

$$w\,(\,x_1,\ldots,x_n,a_1,\ldots,a_m\,)\;=\;1$$

*в свободной группе* $F_m$ *и списку конечно порожденных подгрупп* $H_1,\ldots,H_n$ *группы* $F_m$ *позволял бы узнать, существует ли решение этого уравнения с условием*

$$x_1\;\in\;H_1,\ldots,x_n\;\in\;H_n.$$

Первые положительные результаты в направлении решения этой проблемы были получены А.Ш. Малхасяном [13].

В. Диекерт [14] показал, что проблема определения по произвольному уравнению

$$w\,(\,x_1,\ldots,x_n,a_1,\ldots,a_m\,)\;=\;1$$

в свободной группе $F_m$ и списку *регулярных подмножеств* (языков) $H_1,\ldots,H_n$ группы $F_m$ узнать, существует ли решение этого уравнения с условием

$$x_1\;\in\;H_1,\ldots,x_n\;\in\;H_n$$

разрешима и принадлежит классу $PSPACE$. Так как конечно порожденные подгруппы являются регулярными подмножествами, то тем самым решается и проблема Г.С. Маканина.

Представляет интерес дальнейшее исследование различных обобщений проблемы Г.С. Маканина для свободных групп, получающихся путем ослабления ограничений, налагаемых на подгруппы $H_1, \ldots, H_n$.

Одна из причин, по которым в формулировке задачи 9.25 речь идет именно о *конечно порожденных подгруппах*, заключается в том, что *для конечно порожденных подгрупп свободной группы разрешима проблема вхождения.*

В то же время проблема вхождения разрешима и для многих бесконечно порожденных подгрупп свободной группы, причем, например, для первого $F_m^{(1)}$ и второго $F_m^{(2)}$ коммутантов свободной группы $F_m$ проблема вхождения решается чрезвычайно просто, значительно проще, чем для некоторых конечно порожденных подгрупп. Поэтому представляется достаточно естественным следующее обобщение задачи 9.25.

9.25а. *Существует ли алгоритм, который по уравнению*

$$w\,(\,x_1,\,\ldots\,,\,x_n\,a_1,\,\ldots\,,\,a_m\,)\;=\;1$$

*в свободной группе $F_m$ и списку подгрупп $H_1, \ldots, H_n$ с разрешимыми проблемами вхождения позволял бы узнать, существует ли решение этого уравнения с условием $x_1 \in H_1, \ldots, x_n \in H_n$ ?.*

В работе [15] был получен следующий результат.

Теорема **1.** *В свободной группе $F_2$ со свободными образующими $a$ и $b$ можно построить такое уравнение*

$$w(x, x_1, \ldots, x_n, a, b) = 1$$

*с неизвестными $x_1, x_2, \ldots, x_n$, константами $a$ и $b$ и параметром $x$, что не существует алгоритма, позволяющего для произвольного натурального числа $k$ определить, существует ли решение уравнения*

$$w(a^k, x_1, \ldots, x_n, a, b) = 1,$$

*удовлетворяющее условию*

$$x_1 \in [F_2, F_2], \ldots, x_t \in [F_2, F_2],$$

*где $t$ – некоторое фиксированное число между 1 и $n$.*

Далее существенно усиливается этот результат. Причем в определенном смысле это усиление близко к окончательно возможному.

В ряде работ [5,16–19] рассматривались уравнения вида

$$w\,(\,x_1,\,\ldots\,,\,x_n\,)\,=\,g(\,a_1,\,\ldots,a_m\,),$$

где $w\,(\,x_1,\,\ldots\,,\,x_n\,)$ – групповое слово в алфавите неизвестных $x_1, x_2, \ldots, x_n$, т. е. не содержит констант $a_1, \ldots, a_m$, а $g(\,a_1,\,\ldots,a_m\,)$ – слово в алфавите констант $a_1, \ldots, a_m$, т. е. не содержит неизвестных. Они получили название уравнений, разрешенных относительно неизвестных, или уравнений с правой частью. Проблема разрешимости для таких уравнений иногда называется проблемой подстановки или проблемой сравнения с образцом.

Обозначим через $[u, v]$ коммутатор элементов $u$ и $v$, т. е. $[u, v] = uvu^{-1}v^{-1}$.

Теорема **2.** *В свободной группе $F_2$ со свободными образующими $a$ и $b$ можно построить такое семейство разрешенных относительно неизвестных уравнений*

$$w\,(\,x^k,\,x_1,\,\ldots\,,\,x_n\,)\,=\,[\,a,\,b\,],$$

*где $w\,(\,x^k,\,x_1,\,\ldots\,,\,x_n\,)$ – групповое слово в алфавите неизвестных $x$, $x_1, x_2, \ldots, x_n$, что невозможен алгоритм, позволяющий для произвольного натурального числа $k$ определить, существует ли решение уравнения*

$$w\,(\,x^k,\,x_1,\,\ldots\,,\,x_n\,)\,=\,[\,a,\,b\,],$$

*удовлетворяющее условию*

$$x_1\,\in\,[F_2,\,F_2],\,\ldots\,,\,x_t\,\in\,[F_2,\,F_2],$$

*где $t$ – некоторое фиксированное число между 1 и $n$.*

Теорема **3.** *Невозможен алгоритм, позволяющий по произвольному уравнению вида*

$$w\,(\,x_1,\,\ldots,\,x_n\,)\,=\,[a,b]$$

*в свободной группе $F_2$ определить, имеет ли оно такое решение $g_1,\ldots,g_n$, что*

$$g_1\,\in\,F_2^{(2)}.$$

Заметим, что слово $[a,b]$, стоящее в правой части рассматриваемых в доказанной теореме уравнений, имеет длину 4. Следующая теорема показывает невозможность дальнейшего уменьшения длины правой части.

Теорема **4.** *Существует полиномиальный алгоритм, позволяющий по произвольному разрешенному относительно неизвестных уравнению вида*

$$w\,(\,x_1,\,\ldots\,,\,x_n\,)\,=\,g(\,a,\,b\,),$$

*где $w\,(\,x_1,\,\ldots\,,\,x_n\,)$ – групповое слово в алфавите неизвестных $x_1,x_2,\ldots,x_n$, а $g(\,a,\,b\,)$ – элемент длины меньше 4 свободной группы $F_2$ со свободными образующими $a$ и $b$ определить, существует ли решение этого уравнения, удовлетворяющее условию*

$$x_1\,\in\,F_2^{(s)},\,\ldots\,,\,x_t\,\in\,F_2^{(s)},$$

*где $t$ – произвольное фиксированное число между 1 и $n$.*

Для уравнений с одним неизвестным ситуация иная.

Пусть $\mathbb{N}$ – $r$-й коммутант $F_n^{(r)}$ свободной группы $F_r$ или $r$-й член $(F_m)_r$ ее нижнего центрального ряда.

Теорема **5.** *Существует полиномиальный алгоритм, позволяющий по любому уравнению с одним неизвестным*

$$w\,(\,x_1,\,a_1,\,\ldots,\,a_n\,)\,=\,1$$

*в свободной группе $F_n$ определить имеет ли оно такое решение $x_1$, что $x_1 \in \mathbb{N}$*

## Уравнения в свободной группе с одним ограничением на решения

Обозначим через $\varphi_i$ следующий эндоморфизм свободной группы $F_m$ ранга $m$ со свободными образующими $a_1, \ldots, a_m$

$$\varphi_i(a_j) \rightleftharpoons a_j \text{ п } j \neq i, \quad \varphi_i(a_i) \rightleftharpoons 1.$$

По аналогии с группой кос эндоморфизм $\varphi_i$ назовем " *эндоморфизмом выдергивания i-ой образующей*".

Полагаем

$$P_n^{(i)} \rightleftharpoons Ker\,\varphi_i \quad P_m \rightleftharpoons \bigcap_{i=1}^{m} P_m^{(i)}$$

и назовем $P_m^{(i)}$ *подгруппой i-чистых элементов*, а $P_m$ – *подгруппой чистых или гладких элементов.*

Ясно, что $P_m$ – нормальная подгруппа группы $F_m$, содержащаяся в ее коммутанте $F_m^{(1)}$ ($P_m \subseteq F_m^{(1)}$) и $P_2 = F_2^{(1)}$, но при $m \geq 3$ $P_m \neq F_m^{(1)}$.

Теорема **6.** *При $m \geq 3$ невозможен алгоритм, позволяющий по произвольному уравнению в группе $F_m$*

$$w(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1$$

*определить, имеет ли оно такое решение $x_1, \ldots, x_n$, что $x_1 \in P_m$.*

## О финитной аппроксимируемости для уравнений в свободных группах

Хорошо известно, что свободная группа $F_n$ является финитно аппроксимируемой. Это означает, что для любого неединичного элемента $g$ группы $F_n$ существует конечная факторгруппа $F_n/N$, в которой образ элемента $g$ отличен от единичного элемента. А. И. Мальцев [20] указал на важность изучения свойств финитной аппроксимируемости групп относительно различных предикатов: из их наличия в группе вытекает разрешимость соответствующей алгоритмической проблемы. Пусть $G$ – группа, $\rho$ – предикат, определенный на группе $G$ и ее гомоморфных образах. Говорят, что группа $G$ финитно аппроксимируема относительно $\rho$, если для любых элементов группы $G$, на которых предикат $\rho$ ложен, существует такая конечная факторгруппа $G/N$, что предикат $\rho$ ложен для образов в $G/N$ этих элементов. В ряде работ изучалась финитная аппроксимируемость, в частности, свободных групп, относительно таких предикатов, как сопряженность элементов, возможность извлечения корня $n$-ой степени и т.д. Г. Баумслаг [21] установил финитную аппроксимируемость свободных групп относительно сопряженности и возможности извлечения корня простой степени, т.е. относительно разрешимости уравнений вида $x^{-1}hx = g$ и $x^p = g$, где $h$ и $g$ – элементы свободной группы. В работе [22] установлена финитная аппроксимируемость свободных групп относительно разрешимости уравнений вида $[x, y] = g$ и $x^n = g$. В этой же работе построено уравнение вида $w(x_1, \ldots, x_4, a_1, a_2) = 1$ такое, что оно не имеет решения в свободной группе $F_2$ со свободными образующими $a_1$ и $a_2$, но уравнение $w(x_1, \ldots, x_4, \overline{a_1}, \overline{a_2}) = 1$ имеет решение в любой конечной факторгруппе $F_2/N$, где $\overline{a_1}$ и $\overline{a_2}$ – образы в факторгруппе $F_2/N$ при естественном гомоморфизме свободных образующих $a_1$ и $a_2$ группы $F_2$.

Мы усилили этот результат – построили обладающее аналогичным свойством уравнение, разрешенное относительно неизвестных, т.е. имеющее вид

$$w(x_1, \ldots, x_m) = g,$$

где $g$ – некоторый фиксированный элемент группы $F_2$, а слово $w(x_1, \ldots, x_m)$ не содержит констант, т.е. слово только от переменных.

Теорема **7.** *При любом $n \geq 2$ и любых неотрицательных $m$, $p$ и $q$ уравнение*

$$((x^2u)^{2+p}(z^{-1}y^2vz)^{2+q}t^{2m+3})^4[u,v] = [a_1, a_2]$$

*не имеет решения в свободной группе $F_n$, однако уравнение*

$$((x^2u)^{2+p}(z^{-1}y^2vz)^{2+q}t^{2m+3})^4[u,v] = [\overline{a_1}, \overline{a_2}]$$

*имеет решение в любой конечной факторгруппе $F_n/N$, где через $\overline{a_1}$ и $\overline{a_2}$ обозначены образы свободных образующих $a_1$ и $a_2$ свободной группы $F_n$ относительно ее естественного гомоморфизма на факторгруппу $F_n/N$.*

Рассмотренное в теореме уравнение имеет вид $w(x_1, \ldots, x_6) = [a_1, a_2]$. Представляет интерес вопрос о возможности уменьшения числа неизвестных в левой части уравнения. Ясно, что оно не меньше двух, так как при $m = 1$ уравнение $w(x_1, \ldots, x_m) = g$ принимает вид $x_1^n = g$, а в работе [22] показано, что такое уравнение имеет решение в свободной группе $F_2$ тогда и только тогда, когда оно имеет решение в любой конечной факторгруппе $F_2/N$.

## NP-трудность проблемы разрешимости для уравнений с простой правой частью в свободной группе

Теорема **8.** *Проблема разрешимости в свободной группе $F_2$ для уравнений вида*

$$w(x_1, \ldots, x_n) = [a, b],$$

*где $w(x_1, \ldots, x_n)$ – слово в алфавите неизвестных, а $[a, b]$ – коммутатор свободных образующих $a$ и $b$ группы $F_2$ является $NP$-трудной.*

Заметим, что слово $[a, b]$ имеет длину 4. Для слов $g$ длины меньше 4 ситуация принципиально иная как показывает следующая теорема.

Теорема **9.** *Проблема разрешимости для уравнений вида*

$$w(x_1, \ldots, x_n) = g,$$

*где $w(x_1, \ldots, x_n)$ – групповое слово в алфавите неизвестных $\{x_1, \ldots, x_n, \ldots\}$, а $g$ – групповое слово длины меньше 4 в алфавите $\{a, b\}$ свободных образующих группы $F_2$ полиномиально разрешима.*

## Алгоритмические проблемы для уравнений в свободных моноидах

Через $M_n$ мы будем обозначать свободный моноид, т.е. свободную полугруппу с пустым словом в качестве нейтрального элемента, ранга $n$ со свободными образующими $a_1$, ..., $a_n$, а через $F_n$ – свободную группу с теми же свободными образующими. Вместо $a_1$ и $a_2$ будем писать $a$ и $b$ соответственно.

*Системой уравнений* с неизвестными $x_1$,..., $x_n$ в свободном моноиде (полугруппе) $M_m$ называется выражение вида

$$\mathop{\&}_{i=1}^{k} w_i(x_1, \ldots, x_n, a_1, \ldots, a_m) \;=\; u_i(x_1, \ldots, x_n, a_1, \ldots, a_m), \tag{1}$$

где $w_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ и $u_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ – слова в алфавите

$$\{\, x_1, x_2, \ldots, x_n, a_1, a_2, \ldots, a_m \,\}.$$

Набор $\langle g_1, \ldots, g_n \rangle$ элементов моноида $M_m$ называется *решением* системы (1), если при любом $i$ $(i = 1, \ldots, k)$ в моноиде $M_m$ выполняется равенство

$$w_i(g_1, \ldots, g_n, a_1, \ldots, a_m) \;=\; u_i(g_1, \ldots, g_n, a_1, \ldots, a_m).$$

Две системы уравнений с одними и теми же неизвестными называются *эквивалентными*, если множества их решений совпадают. При $m \geq 2$ система уравнений $\mathop{\&}_{i=1}^{k} w_i = u_i$ равносильна одному уравнению

$$w_1 a_1 w_2 a_1 \ldots a_1 w_k \, w_1 a_2 w_2 a_2 \ldots a_2 w_k \;=\; u_1 a_1 u_2 a_1 \ldots a_1 u_k \, u_1 a_2 u_2 a_2 \ldots a_2 u_k.$$

В 60-ые годы прошлого века А.А. Марков предложил использовать системы уравнений в свободном моноиде $M_n$ в качестве одного из подходов к отрицательному решению 10-ой проблемы Д. Гильберта.

Системы уравнений в свободных моноидах (в свободных полугруппах) также называются системами уравнений в словах. Первые результаты в исследовании систем уравнений в словах были получены А.А. Марковым (не опубликовано) и Ю.И. Хмелевским [23]в конце 60-ых годов.

В эти же годы было начато изучение систем уравнений в словах и длинах, т.е. систем вида

$$\mathop{\&}_{i=1}^{m} w_i = u_i \;\&\; \mathop{\&}_{\{i,j\}\in A} |x_i| = |x_j|,$$

где через $|x| = |y|$ обозначен предикат “ *длины слов $x$ и $y$ равны*”. Первые результаты в исследовании систем уравнений в словах и длинах были получены в начале 70-ых годов в работах Ю.В. Матиясевича [24] и Н.К. Косовского [25-27].

Для слова $w$ в алфавите $\Sigma$ и буквы $a$ этого алфавита через $|w|_a$ будем обозначать число вхождений буквы $a$ в слово $w$.

В 1972-73 годах первый из авторов стал рассматривать системы уравнений в словах и длинах с дополнительным предикатом $|x|_a = |y|_a$ – “ *проекции слов $x$ и $y$ на выделенную букву $a$ равны*”. В работе [15], вышедшей из печати в 1974 году, он, в частности, доказал, что

*можно указать такое однопараметрическое семейство систем уравнений в свободном моноиде $M_2$,*

$$w(x, x_1, \ldots, x_n, a, b) = v(x, x_1, \ldots, x_n, a, b) \;\&\; \mathop{\&}_{\{i,j\}\in A} (|x_i| = |x_j| \,\&\, |x_i|_a = |x_j|_a)$$

*с неизвестными $x_1$, ..., $x_n$, с константами $a$ и $b$ и с параметром $x$, где $A$ – некоторое подмножество множества $\{\{t,s\} \mid 1 \le t,s \le n\}$, что невозможен алгоритм, позволяющий для произвольного натурального числа $m$ определить, имеет ли решение система уравнений*

$$w(a^m, x_1, \ldots, x_n, a, b) = v(a^m, x_1, \ldots, x_n, a, b) \,\&\, \mathop{\&}_{\{i,j\} \in A} (|x_i| = |x_j| \,\&\, |x_i|_a = |x_j|_a).$$

В этой же работе отмечалось, что аналогичный результат остается верным, если предикат $|x| = |y| \,\&\, |x|_a = |y|_a$ заменить предикатом $|x|_b = |y|_b \,\&\, |x|_a = |y|_a$.

Аналогичный результат содержался в опубликованной в 1988 году работе J.R. Buchi и S. Senger [28]

В 1976 году Г.С. Маканин получил в теории уравнений в словах фундаментальный результат, который был опубликован в 1977 году в работах [30]и [31], – он построил *алгоритм, позволяющий по произвольной системе уравнений в свободной полугруппе $M_n$ определить, имеет ли она решение.* Несколько позже в работе [6]Г.С. Маканин построил *алгоритм, позволяющий по произвольной системе уравнений в свободной группе $F_n$ определить, имеет ли она решение.*

После фундаментальных результатов Г.С. Маканина особый интерес стал представлять вопрос о существовании аналогичных алгоритмов для уравнений в свободных моноидах, полугруппах и группах с различными “не слишком сложными” и “достаточно естественными” ограничениями на решения.

В работах [32], [33] была доказана алгоритмическая неразрешимость позитивной $\exists\forall\exists^3$-теории любой конечно порожденной нециклической свободной полугруппы. Вопрос о разрешимости позитивной теории свободной полугруппы счетного ранга в кандидатской диссертации первого автора был легко сведен к следующей проблеме *существует ли алгоритм, позволяющий для произволь-*

*ного уравнения*

$$w(x_1, \ldots, x_n, a_1, \ldots, a_m) = u(x_1, \ldots, x_n, a_1, \ldots, a_m)$$

*в свободной полугруппе счетного ранга определить, имеет ли оно такое решение* $g_1, \ldots, g_n$, *что*

$$g_1 \in M_{m_1},\ g_2 \in M_{m_2}, \ldots, g_n \in M_{m_n},$$

*где* $m_1 \leq m_2 \leq \ldots \leq m_n$, $M_{m_i}$ *- свободная полугруппа с образующими* $a_1, \ldots, a_{m_i}$. Сведение осуществлено путем переноса методы Ю.И. Мерзлякова [7] со свободных групп на свободную счетнопорожденную полугруппуэ Ю.М. Важенин и Б.В. Розенблат [35]используя результат Г.С. Маканина [30] доказали, что для решения последней задачи алгоритм существует, это позволило им установить *разрешимость позитивной теории свободной полугруппы счетного ранга.*

К. Шульц [36] рассмотрел аналогичную сформулированной выше проблеме 9.25 Г.С. Маканина проблему для уравнений в свободных моноидах (свободных полугруппах) с регулярными ограничениями на решения и доказал, что *существует алгоритм, который по уравнению*

$$w(x_1, \ldots, x_m, a_1, \ldots, a_n) = u(x_1, \ldots, x_m, a_1, \ldots, a_n)$$

*в свободном моноиде* $M_n$ *и списку регулярных подмножеств (языков)* $H_1$,..., $H_m$ *моноида* $M_n$ *позволяет узнать, существует ли решение этого уравнения с условием*

$$x_1 \in H_1, \ldots, x_m \in H_m.$$

Так как каждая конечно порожденная подполугруппа свободного моноида $M_n$ является регулярным подмножеством (языком), то решенная К. Шульцем проблема для уравнений с ограничениями на решения в свободных полугруппах является естественным аналогом проблемы Г.С. Маканина.

V. Diekert [37], [38] построил *алгоритм, позволяющий по произвольному уравнению*

$$w\,(\,x_1,\ldots,x_m,a_1,\ldots,a_n\,)\,=\,1$$

*в свободной группе $F_n$ и списку регулярных подмножеств (языков) $H_1$,..., $H_m$ группы $F_n$ определить, существует ли решение этого уравнения с условием*

$$x_1\,\in\,H_1,\ldots,x_m\,\in\,H_m.$$

Тем самым решена и проблема Г.С. Маканина.

Сказанное дает основания считать, что представляет интерес дальнейшее исследование различных обобщений проблемы Г.С. Маканина для свободных групп, моноидов и полугрупп, получающихся путем ослабления ограничений, налагаемых на подгруппы (подполугруппы, подмоноиды, языки) $H_1$,..., $H_m$.

В силу теоремы К. Шульца для получения алгоритмически неразрешимых проблем для уравнений в свободных моноидах (полугруппах) с подполугрупповыми ограничениями на решения необходимо рассматривать, в первую очередь, бесконечно порожденные свободные подполугруппы, среди которых имеются как нерегулярные, так и регулярные языки, например, подполугруппа, порожденная всевозможными словами вида $ab^na$ $(n=1,2,...)$ свободно ими порождается и является регулярным языком.

В литературе по формальным языкам и грамматикам достаточно часто встречается рекурсивный язык $L_1$ в алфавите $\{a,b\}$, который состоит из всех слов $w$ в алфавите $\{a,b\}$, для которых $|w|_a=|w|_b$. Пользуясь известным критерием свободности для подполугрупп свободной полугруппы, легко доказать, что $L_1$ – *свободная подполугруппа счетного ранга.* Конечно, рекурсивный

язык $L_1$ не является регулярным, однако с точки зрения сложности разрешимости для него алгоритмических проблем он скорее "ближе" к регулярным языкам, чем к произвольным рекурсивным.

Поэтому представляют интерес, на наш взгляд, следующие две теоремы.

Теорема **10.** *Можно указать такое однопараметрическое семейство уравнений с ограничениями на решения в свободном моноиде* $M_2$,

$$w(x, x_1, \ldots, x_n, a, b) = v(x, x_1, \ldots, x_n, a, b) \,\&\, \mathop{\&}_{\{i,j\} \in A} |x_i| = |x_j| \;\&\; |x_1|_b = |x_2|_b$$

*с неизвестными* $x_1$, ..., $x_n$, *с константами* $a$ *и* $b$ *и с параметром* $x$, *где* $A$ – *некоторое подмножество множества* $\{\{t, s\} \mid 1 \le t, s \le n\}$, *что невозможен алгоритм, позволяющий для произвольного натурального числа* $m$ *определить, имеет ли решение уравнение с ограничениями на решения*

$$w(a^m, x_1, \ldots, x_n, a, b) = v(a^m, x_1, \ldots, x_n, a, b) \,\&\, \mathop{\&}_{\{i,j\} \in A} |x_i| = |x_j| \;\&\; |x_1|_b = |x_2|_b.$$

Теорема **11.** *Можно указать такое однопараметрическое семейство уравнений с ограничениями на решения в свободном моноиде* $M_2$,

$$w(x, x_1, \ldots, x_n, a, b) = v(x, x_1, \ldots, x_n, a, b) \,\&\, \mathop{\&}_{\{i,j\} \in A} |x_i| = |x_j| \;\&\; x_1 \in L_1$$

*с неизвестными $x_1$, ..., $x_n$, с константами $a$ и $b$ и с параметром $x$, где $A$ – некоторое подмножество множества $\{\{t,s\} \mid 1 \le t,s \le n\}$, что невозможен алгоритм, позволяющий для произвольного натурального числа $m$ определить, имеет ли решение уравнение с ограничениями на решения*

$$w(a^m, x_1, \ldots, x_n, a, b) = v(a^m, x_1, \ldots, x_n, a, b) \,\&\, \mathop{\&}_{\{i,j\} \in A} |x_i| = |x_j| \;\&\; x_1 \in L_1.$$

## Уравнения и неравенства в словах и длинах

V. Diekert предложил (устное сообщение Ю.В. Матиясевича) изучать в свободных полугруппах системы вида

$$\mathop{\&}_{i=1}^{k} w_i(x_1, \ldots, x_n, a_1, \ldots, a_m) \le u_i(x_1, \ldots, x_n, a_1, \ldots, a_m), \tag{2}$$

где для слов $w$ и $u$ в алфавите образующих свободной полугруппы запись $w \le u$ означает, что *последовательность букв $w$ является подпоследовательностью букв $u$* , т.е. существуют такое число $n \le |w|$ и такие слова $w_1$, ..., $w_n$, $u_1$, ..., $u_n$, $u_{n+1}$, что

$$w = w_1 \ldots w_n \quad u = u_1 w_1 u_2 \ldots u_n w_n u_{n+1},$$

рассматривая их как обобщение систем уравнений (1), так как

$w = u$ тогда и только тогда, когда $w \le u \,\&\, u \le w$ .

Отношение $w \leq u$ является отношением частичного порядка на полугруппе $\Pi_m$, т.е. оно рефлексивно, транзитивно и антисимметрично. Это еще один довод для обоснования естественности рассмотрения систем неравенств вида (2).

Вопрос об алгоритмической разрешимости проблемы совместности для систем неравенств (2) в настоящее время открыт. Но если к отношению $w \leq u$ добавить предикат равенства длин, то получим алгоритмически неразрешимую задачу.

В дальнейшем равенство $w = u$ будет использоваться как сокращенная запись конъюнкции неравенств $w \leq u \,\&\, u \leq w$.

Теорема **12.** *Невозможен алгоритм, позволяющий для произвольной системы вида*

$$\mathop{\&}_{i=1}^{k} w_i \leq u_i \;\&\; \mathop{\&}_{\{i,j\} \in A} |x_i| = |x_j|$$

*определить, имеет ли она решение.*

## Литература


[1]Tarski A., Mostowski A., Robinson R.M. Undecidable theories. NY., 1953.

[2] Lyndon R.C. Equations in free groups // Trans. Amer. Math. Soc. 1960. Volume 96. P. 445 – 457.

[3] Лоренц А.А. О представлении множеств решений систем уравнений с одним неизвестным в свободных группах. // Доклады АН СССР. 1968. Том 178. №2. С. 290 – 292.

[4] Appel K.I. One-variable equations in free groups. // Proc. Amer. Math. Soc. 1968. Volune 19. P. 912 – 918.

[5] Хмелевский Ю.И. Системы уравнений в свободной группе. I, II. // Известия АН СССР. Серия математика. 1971. Том 35. №6. С. 1237 – 1268. 1972. Том 36. №1. С. 110 – 179.

[6] Маканин Г.С. Уравнения в свободной группе. // Известия АН СССР. Серия математика. 1982. Том 46. №6. С. 1199 – 1273.

[7] Маканин Г.С. Универсальная теория и позитивная теория свободной группы. // Известия АН СССР. Серия математика. 1984. Том 48. №4. С. 735 – 749.

[8] Мерзляков Ю.И. Позитивные формулы на свободных группах. // Алгебра и логика. 1966. Том 5. №4. С. 25 – 42.

[9] Разборов А.А. О системах уравнений в свободной группе. // Известия АН СССР. Серия математика. 1984. Том 48. №4. С. 779 – 832.

[10] Gassner B.J. On braid groups. // Abh. Math. Sem. Univ. Hamburg. 1961. Volume 25. P. 10 – 22.

[11] Birman J.S. Braids, links and mapping class groups. Ann.of Math. Studies №82. Princeton University Press. Princeton, 1974.

[12] Коуровская тетрадь. Издание 17-е, дополненное и включающее Архив решенных задач // Новосибирск: Институт математики СО РАН. 2010.

[13] Малхасян А.Ш. О разрешимости в подгруппах уравнений в свободной группе. // Сборник "Прикладная математика". 1986. Том 2. С. 42 – 47.

[14] Diekert V. Makanin's Algorithm for Solving Word Equations with Regular Constraints. Preliminary version of the chapter in M. Lothaire. Algebraic Combinatorics on Words. Report Nr. 1998/02. Fakultat Informatik. Universitat Stuttgart. 1998.

[15] Дурнев В.Г. Об уравнениях на свободных полугруппах и группах. // Матем. заметки. 1974. Том 16. №5. С. 717 – 724.

[16] Мальцев А.И. Об уравнении $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ в свободной группе. // Алгебра и логика. 1962. Том 1. №5. С. 45 – 50.

[17] Schupp P.E. On the substitution problem for free groups. // Proc. Amer. Math. Soc. 1969. Volume 23. P. 421 – 423.

[18] Edmunds C.C. On the endomorphisms problem for free group. // Com. Algebra. 1975. Volume 3. P. 7 – 20.

[19] Дурнев В.Г. О проблеме разрешимости для уравнений с одним коэффициентом. // Матем. заметки. 1996. Том 59. №6. С. 832 – 845.

[20] Мальцев А. И. О гомоморфизмах на конечные группы. // Ученые записки Ивановского пед. ин-та. 1958. Том 18. С. 49 – 60.

[21] Baumslag G. Residual nilpotency and relations in free groups. // J. of Algebra. 1965. Volume 2. P. 271 – 282.

[22] Coulbois T. and Khelif A. Equations in free groups are not finitely approximable. // Proceedings of the American mathemetical society. 1999. Volume 127. №4. P. 963 – 965.

[23]Хмелевский Ю.И. Уравнения в свободной полугруппе. М.: Наука. 1971. (Тр. МИАН.) Т. 107).

[24]Матиясевич Ю.В. Связь систем уравнений в словах и длинах с 10-ой проблемой Гильберта // Исследования по конструктивной математике и математической логике. Записки научн. семинаров Ленингр. отд. Матем. ин-та. АН СССР. Л. 1968. Т. 8. С. 132 - 143.

[25]Косовский Н.К. Некоторые свойства решений уравнений в свободной полугруппе // Записки научн. семинаров Ленингр. отд. Матем. ин-та. АН СССР. Л. 1972. Т. 32. С. 21 - 28.

[26]Косовский Н.К. О множествах, представимых в виде решений уравнений в словах и длинах // Вторая всесоюзная конфер. по матем. логике. Тезися кратких сообщений. М. 1972. С. 23.

[27]Косовский Н.К. О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов// Записки научн. семинаров Ленингр. отд. Матем. ин-та. АН СССР. Л. 1973. Т. 33. С. 24 - 29.

[28]Buchi J. R., Senger S. Definability in the existential theory of concatenation // Z. math. Log. und Grundl. Math. 1988. V. 34. № 4. P. 337 - 342.

[29]Buchi J. R., Senger S. Coding in the existential theory of concatenation // Arch. Math. Logik. 1986/87. Bd. 26. P. 101 - 106.

[30]Маканин Г.С. Проблема разрешимости уравнений в свободной полугруппе// ДАН СССР. 1977. Т. 233. № 2. С. 287 - 290.

[31]Маканин Г.С. Проблема разрешимости уравнений в свободной полугруппе// Матем. сбор. 1977. Т. 103 (145). № 2 (6). С. 147 - 236.

[32]Дурнев В.Г. Позитивная теория свободной полугруппы// ДАН СССР. 1973. Т. 211. № 4. С. 772 - 774.

[33]Дурнев В.Г. О позитивных формулах на свободных полугруппах// Сиб. матем. журн. 1974. Т. 25. № 5. С. 1131 - 1137.

[34]Дурнев В.Г. Неразрешимость позитивной $\forall\exists^3$-теории свободной полугруппы// Сиб. матем. журн. 1995. Т. 36. № 5. С. 1067 - 1080.

[35]Важенин Ю.М., Розенблат Б.В. Разрешимость позитивной теории свободной счетнопорожденной полугруппы // Матем. сборник. 1981. Т. 116. № 1. С. 120 - 127.

[36]Schulz K.U. Makanin's Algprithm for Word Equations - Two Improvements and a Generalization // Lecture Notes in Computer Science. 1990. V. 572. P. 85 - 150.

[37]Diekert V., Gutierrez C., Hagenah C. The existential theory of equations with rational constraints in free groups is PSPACE-complete. In A. Ferreira and H Reichel, editors, Proc. 18-th Annual Symposium on Theoretical Aspects of Computer Science (STACS'01), Dresden (Germany), 2000, number 2010 in Leture Notes in Computer Science. P. 170 - 182. Springer-Verlag, 2001.

[38]Diekert V., Gutierrez C., Hagenah C. The existential theory of equations with rational constraints

in free groups is PSPACE-complete // Informatiion and Computation. 2005. V. 202. P. 105 - 140.