УДК 510.53, 512.54.05
AMS MSC2020: 20M05, 03B30

Алгоритмические проблемы для уравнений в свободных группах и полугруппах с ограничениями на решения

Дурнев В. Г., Зеткина А. И.

Ярославский государственный университет им. П. Г. Демидова

Аннотация. Рассматриваются алгоритмически неразрешимые проблемы для уравнений в свободных группах с «достаточно простыми» подгрупповыми ограничениями на решения, разрешенныхе относительно неизвестных с простой правой частью. Исследуются алгоритмически неразрешимые проблемы для уравнений в словах и длинах в свободных полугруппах с одним дополнительным ограничением на решение.

Ключевые слова: проблема совместности для систем уравнений, уравнения в свободных группах, уравнения в словах и длинах.

Светлой памяти
Михаила Абрамовича Тайцлина
посвящается

Введение

Трудно отрицать, что на протяжении всей многовековой истории «Алгебры» изучение уравнений играло достаточно важную роль. Приведем цитату из монографии Ж. А. Серре «Курс высшей алгебры» (Русский перевод, СПб: 1910): «Алгебра — это, по сути, жонглирование уравнениями». Конечно, с начала 20-х годов прошлого века «Алгебра» — это наука об алгебраических операциях. «Алгебра» изучает алгебраические структуры или даже алгебраические системы.

Важную роль в истории «Алгебры» играет изучение уравнений и их систем с различными ограничениями на решения. Эта традиция прослеживается со времен Диофанта (предположительно III век

н. э.), который начал изучать уравнения с рациональными (положительными) ограничениями на решения, то есть в современных обозначениях 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, то есть многочлены над множеством положительных рациональных чисел $\mathbb{Q}_+$. Диофанта интересовал, прежде всего, вопрос о нахождении какого-нибудь рационального решения конкретного уравнения и нахождение (получение, описание) всех его рациональных решений, отправляясь, как правило, от одного известного решения.

Вопрос, имеет ли рациональное решение рассматриваемое уравнение 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.

Важный вклад в изучение уравнений с ограничениями на решения внес П. Ферма, который 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 натуральное число 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» Л. Эйлера оно называется уравнением Пелля и обычно 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 [20]. 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 наличии 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 наличии 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, далеко обобщившим и расширившим метод Штурма для уравнений с одной неизвестной. Более того А. Тарский на этой основе разработал разрешающий алгоритм для элементарной теории поля действительных чисел, то есть алгоритм, позволяющий по произвольной замкнутой формуле Φ в сигнатуре $\langle 0, 1, +, \cdot, \leqslant \rangle$ определить, истинна ли она на поле действительных чисел. В этой связи необходимо указать на фундаментальный результат Ю. Л. Ершова, Дж. Акса и С. Кочена, которые 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 NP-полной.

В заключение напомним, что Д. Гильберт доказал следующую фундаментальную теорему:

Теорема 1. *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, если и только если многочлены $F_i(x_1, \ldots, x_n)$, $i \in I$, порождают в кольце $\mathbb{C}[x_1, \ldots, x_n]$ единичный идеал, то есть существуют такие многочлены $G_i(x_1, \ldots, x_n)$, $i \in I$, с комплексными коэффициентами, для которых выполняется равенств

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

1. Основные определения

Через M_m мы будем, как обычно, обозначать свободный моноид, то есть свободную полугруппу с пустым словом в качестве нейтрального элемента, ранга m со свободными образующими $a_1, \ldots, a_m$, а через F_m — свободную группу с теми же свободными образующими. Вместо a_1 и a_2 будем писать a и b соответственно.

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

Определение 1 (Система уравнений в свободной группе). *Системой уравнений с неизвестными $x_1, \ldots, x_n$ в свободной группе F_m называется выражение вида*

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

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 р е ш е н и е м системы (1), если при любом $i = 1, \ldots, k$ в группе F_m выполнено

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

Две системы уравнений с одними и теми же неизвестными называются э к в и в а л е н т н ы м и, если множества их решений совпадают. Используя, например, уравнение

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

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

Определение 2 (Система уравнений в свободном моноиде, свободной полугруппе). *Системой уравнений с неизвестными* $x_1, \ldots, x_n$ *в свободном моноиде (свободной полугруппе)* M_m *называется выражение вида*

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

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* (2), *если при любом* $i = 1, \ldots, k$ *в моноиде* M_m *выполнено*

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

Две системы уравнений с одними и теми же неизвестными называются эквивалентными, если множества их решений совпадают. При $m \geqslant 2$ система уравнений (2) равносильна одному уравнению

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

2. Из истории обсуждаемого вопроса

Исследование разрешимости уравнений в свободных группах было начато в конце 50-х годов прошлого века в связи с проблемой разрешимости элементарных теорий свободных групп, поставленной А. Тарским [40]. Этому вопросу посвящены, в частности, работы [12,24,26,37]. В 60-е годы прошлого века А. А. Марков предложил использовать системы уравнений в свободном моноиде M_m в качестве одного из подходов к отрицательному решению 10-й 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 [25] в конце 60-х годов прошлого века.

В эти же годы было начато изучение систем уравнений в словах и длинах, то есть систем вида

$$\&_{t=1}^{k} w_t(x_1, \ldots, x_n) = u_t(x_1, \ldots, x_n) \,\&\, \&_{\{i,j\} \in A} |x_i| = |x_j|,$$

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-х годов в работах Ю. В. Матиясевича [21] и Н. К. Косовского [8–10].

В 1976 году Г. С. Маканин получил в теории уравнений в словах фундаментальный результат, который был опубликован в 1977 году в работах [13] и [14], — он построил алгоритм, позволяющий по произвольной системе уравнений в свободной полугруппе M_m определить, имеет ли она решение. Несколько позже в работе [15] 1982 года Г. С. Маканин построил алгоритм, позволяющий по произвольной системе уравнений в свободной группе F_m определить, имеет ли она решение — он построил такую рекурсивную функцию $\Phi(d)$, 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 $\Phi(d)$. 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 представлял интерес вопрос об алгоритмической природе фрагментов этой теории. Основные результаты в этой области были получены Г. С. Маканиным — вскоре после опубликования работы [15] ему удалось на том же пути доказать разрешимость экзистенциональной (универсальной) и позитивной теорий любой свободной группы [16]. При доказательстве разрешимости позитивной теории свободной группы Г. С. Маканин использовал результат Ю. И. Мерзлякова [22] об устранимости кванторов общности в позитивных формулах, относящихся к свободным группам. Вопрос о разрешимости позитивной теории свободной группы был сведен Ю. И. Мерзляковым [22] к следующей проблеме для уравнений с ограничениями на решения:

Существует ли алгоритм, который для произвольного уравнения

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

в свободной группе счетного ранга определяет, имеет ли оно такое

решение $g_1, \ldots, g_n$, *что* $g_1 \in F_{m_1}, g_2 \in F_{m_2}, \ldots, g_n \in F_{m_n}$, *где* $m_1 \leqslant m_2 \leqslant \ldots \leqslant m_n$, F_{m_i} — *свободная группа с образующими* $a_1, \ldots, a_{m_i}$.

Г. С. Маканин [16] построил искомый алгоритм, и тем самым доказал разрешимость позитивной теории свободной группы.

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 [2, 3] первым автором 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 его кандидатской диссертации 1973 года был сведен путем переноса методов Ю. И. Мерзлякова [22] со свободных групп на свободную счетнопорожденную полугруппу к следующей проблеме:

Существует ли алгоритм, который для произвольного 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 говорит, имеет ли оно решение $g_1, \ldots, g_n$, *где* $g_1 \in M_{m_1}, g_2 \in M_{m_2}, \ldots, g_n \in M_{m_n}$, $m_1 \leqslant m_2 \leqslant \ldots \leqslant m_n$, M_{m_i} — *свободная полугруппа с образующими* $a_1, \ldots, a_{m_i}$.

На основе этого сведения в работе [5] на стр. 150 отмечается «Нетрудно показать, что позитивная теория свободной полугруппы Π_∞ является рекурсивно перечислимой, но не известно, является ли она рекурсивной». Через Π_∞ обозначается свободная полугруппа счетного ранга.

Ю. М. Важенин и Б. В. Розенблат [1], используя фундаментальный результат Г. С. Маканина [13], доказали, что для решения последней задачи алгоритм существует, это позволило им установить разрешимость позитивной теории свободной полугруппы счетного ранга.

Обобщая эти ситуации, Г. С. Маканин поставил в «Коуровской тетради» [11] такую 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 [17].

К. Шульц [38] 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 следующее:

Теорема 2. *Существует алгоритм, который по уравнению*

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

в свободном моноиде M_m *и списку регулярных подмножеств (языков)* $H_1, \ldots, H_n$ *моноида* M_m *позволяет узнать, существует ли решение этого уравнения с условием* $x_1 \in H_1, \ldots, x_n \in H_n$.

Так как каждая конечно порожденная подполугруппа свободного моноида M_m 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.

Ф. Дикерт [32–34] построил алгоритм, позволяющий 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 определить, существует ли решение этого уравнения с условием $x_1 \in H_1, \ldots, x_n \in H_n$. Тем самым решена и проблема 9.25 Г. С. Маканина. Более того, в указанных работах дана оценка емкостной сложности рассматриваемых проблем.

Сказанное дает основания считать, что представляет интерес дальнейшее исследование различных обобщений проблемы 9.25 Г. С. Маканина для свободных групп, моноидов и полугрупп, получающихся путем ослабления ограничений, налагаемых на подгруппы (подполугруппы, подмоноиды, языки) $H_1, \ldots, H_n$.

3. Основные результаты

Основные наши результаты, которые мы хотели бы обсудить, содержатся в следующих теоремах, доказательства которых базируются прежде всего на фундаментальной теореме М. Дэвиса,

Дж. Робинсон, Х. Путнам, Ю. В. Матиясевича о диофантовости любого рекурсивно перечислимого множества [20].

Теорема 3. *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, определяющий для произвольного натурального числа k, существует ли решение уравнения

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

где $x_1 \in F_2^{(1)}, \ldots, x_t \in F_2^{(1)}$, t — некоторое фиксированное число между 1 и n, а $F_2^{(1)} = [F_2, F_2]$ — коммутант свободной группы F_2.

Как обычно через $F_2^{(2)} = [F_2^{(1)}, F_2^{(1)}]$ обозначается второй коммутант свободной группы F_2.

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

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

в свободной группе F_2 определить, имеет ли оно такое решение g_1, ..., 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 5. *Существует полиномиальный алгоритм, позволяющий по произвольному разрешенному относительно неизвестных уравнению вида*

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

где $w(x_1, \ldots, x_n)$ является групповым словом 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, для которого $x_1 \in F_2^{(s)}, \ldots, x_t \in F_2^{(s)}$, где t — произвольное фиксированное число между 1 и n, а $F_2^{(s)}$ — s-й коммутант свободной группы F_2.

Обозначим через φ_i следующий эндоморфизм свободной группы

F_m ранга m со свободными образующими $a_1, \ldots, a_m$

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

По аналогии с группой кос эндоморфизм φ_i назовем «эндоморфизмом выдергивания i-ой образующей».

Полагаем

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

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 $P_m \neq F_m^{(1)}$ при $m \geqslant 3$.

Теорема 6. *При $m \geqslant 3$ 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 $x_1 \in P_m$.

Следующую теорему можно рассматривать как усиление основного результата работы [31] о финитной неаппроксимируемости проблемы разрешимости уравнений в свободной группе.

Теорема 7. *При любом $n \geqslant 2$ 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.

В качестве некоторого дополнения к предыдущим теоремам может рассматриваться следующая теорема.

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 $w(x_1, \ldots, x_n)$ является групповым словом 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.

Следующие теоремы относятся к уравнениям в словах и длинах с некоторыми дополнительными ограничениями. Уже более полувека остается открытым вопрос о существовании алгоритма, позволяющего по произвольной системе уравнений с ограничениями на решения в свободном моноиде M_2 вида

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

определить, имеет ли она решение.

В связи с этим представляют интерес следующие 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 $x_1, \ldots, x_n$, с константами a и b и с параметром x, где A — некоторое подмножество множества $\{\{t, s\} \mid 1 \leqslant t, s \leqslant n\}$, 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 $x_1, \ldots, x_n$, с константами a и b и с параметром x, где A — некоторое подмножество множества $\{\{t, s\} \mid 1 \leqslant t, s \leqslant$

$n\}$, *что невозможен алгоритм, позволяющий для произвольного натурального числа* m *определить, имеет ли решение уравнение с ограничениями на решения*

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

Ф. Дикерт предложил (устное сообщение Ю. В. Матиясевича) изучать в свободных моноидах системы вида

$$\mathop{\&}_{i=1}^{k} w_i(x_1, \ldots, x_n, a_1, \ldots, a_m) \leqslant u_i(x_1, \ldots, x_n, a_1, \ldots, a_m), \qquad (3)$$

где для слов w и u в алфавите образующих свободного моноида запись $w \leqslant u$ означает, что последовательность букв w является подпоследовательностью букв u, то есть существуют такое число $n \leqslant |w|$ и такие слова $w_1, \ldots, w_k, u_1, \ldots, u_k, u_{k+1}$, что

$$w = w_1 \ldots w_k \quad u = u_1 w_1 u_2 \ldots u_k w_k u_{k+1},$$

рассматривая их как обобщение систем уравнений (1), так как $w = u$ тогда и только тогда, когда $w \leqslant u \,\&\, u \leqslant w$.

Отношение $w \leqslant u$ является отношением частичного порядка на моноиде M_m, то есть оно рефлексивно, транзитивно и антисимметрично. Это еще один довод для обоснования естественности рассмотрения систем неравенств вида (1).

Вопрос об алгоритмической разрешимости проблемы совместности для систем неравенств (3) в настоящее время открыт. Но если к отношению $w \leqslant u$ добавить предикат равенства длин, то получим алгоритмически неразрешимую задачу.

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

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

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

определить, имеет ли она решение.

4. Заключение

Обсуждаемые в докладе вопросы, на наш взгляд, вписываются в две фундаментальные проблемы, которые в 60-е годы прошлого века сформулировал Сергей Иванович Адян:

- Где «проходит граница» между областями «Алгоритмически разрешимые проблемы» и «Алгоритмически неразрешимые проблемы»?

- Какие дополнительные условия «превращают» «Алгоритмически разрешимую проблему» в «Алгоритмически неразрешимую проблему»?

Список литературы

[1] *Важенин, Ю. М.* Разрешимость позитивной теории свободной счетнопорожденной полугруппы / Ю. М. Важенин, Б. В. Розенблат // Математический сборник. — 1981. — Т. 116, № 1. — С. 120–127.

[2] *Дурнев, В. Г.* Позитивная теория свободной полугруппы // Доклады АН СССР. — 1973. — Т. 211, № 4. — С. 772–774.

[3] *Дурнев, В. Г.* О позитивных формулах на свободных полугруппах // Сибирский математический журнал. — 1974. — Т. 25, № 5. — С. 1131–1137.

[4] *Дурнев, В. Г.* Неразрешимость позитивной $\forall\exists^3$-теории свободной полугруппы // Сибирский математический журнал. — 1995. — Т. 36, № 5. — С. 1067–1080.

[5] *Дурнев, В. Г.* О позитивной теории свободной полугруппы // Сб. «Вопросы теории групп и полугрупп». — Тула : Тульский государственный педагогический институт им. Л. Н. Толстого. — 1972. — С. 122–172.

[6] *Дурнев, В. Г.* Об уравнениях на свободных полугруппах и группах // Математические заметки. — 1974. — Т. 16, № 5. — С. 717–724.

[7] *Дурнев, В. Г.* О проблеме разрешимости для уравнений с одним коэффициентом // Математические заметки. — 1996. — Т. 59, № 6. — С. 832–845.

[8] *Косовский, Н. К.* Некоторые свойства решений уравнений в свободной полугруппе // Записки научных семинаров Ленинградского отделения Математического института АН СССР. Ленинград. — 1972. — Т. 32. — С. 21–28.

[9] *Косовский, Н. К.* О множествах, представимых в виде решений уравнений в словах и длинах // Вторая всесоюзная конференция по математической логике. Тезисы кратких сообщений. — М . — 1972. — С. 23.

[10] *Косовский, Н. К.* О решении систем, состоящих одновременно из уравнений в словах и неравенств в длинах слов // Записки научных семинаров Ленинградского отделения Математического института АН СССР. Ленинград. — 1973. — Т. 33. — С. 24–29.

[11] Коуровская тетрадь. Издание 17-е, дополненное, включающее Архив решенных задач / Сост. В. Д. Мазуров, Е. И. Хухро. — Новосибирск : Институт математики СО РАН, 2010. — 219 с.

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

[13] *Маканин, Г. С.* Проблема разрешимости уравнений в свободной полугруппе// Доклады АН СССР. — 1977. — Т. 233, № 2. — С. 287–290.

[14] *Маканин, Г. С.* Проблема разрешимости уравнений в свободной полугруппе // Математический сборник. — 1977. — Т. 103 (145), № 2 (6). — С. 147–236.

[15] *Маканин, Г. С.* Уравнения в свободной группе // Известия АН СССР. Серия математика. — 1982. — Т. 46, № 6. — С. 1199–1273.

[16] *Маканин, Г. С.* Универсальная теория и позитивная теория свободной группы // Известия АН СССР. Серия математика. — 1984. — Т. 48, № 4. — С. 735–749.

[17] *Малхасян, А. Ш.* О разрешимости в подгруппах уравнений в свободной группе // Сборник «Прикладная математика». — 1986. — Т. 2. — С. 42–47.

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

[19] *Мальцев, А. И.* О гомоморфизмах на конечные группы // Ученые записки Ивановского педагогического института. — 1958. — Т. 18. — С. 49–60.

[20] *Матиясевич, Ю. В.* Диофантовость перечислимых множеств // Доклады АН СССР. — 1970. — Т. 130, № 3. — С. 495–498.

[21] *Матиясевич, Ю. В.* Связь систем уравнений в словах и длинах с 10-ой проблемой Гильберта // Исследования по конструктивной математике и математической логике. Записки научных семинаров Ленинградского отделения Математического института АН СССР. Ленинград. — 1968. — Т. 8. — С. 132–143.

[22] *Мерзляков, Ю. И.* Позитивные формулы на свободных группах // Алгебра и логика. — 1966. — Т. 5, № 4. — С. 25–42.

[23] *Разборов, А. А.* О системах уравнений в свободной группе // Известия АН СССР. Серия математика. — 1984. — Т. 48, № 4. — С. 779–832.

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

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

[26] *Appel, K. I.* One-variable equations in free groups // Proceedings of the American Mathematical Society. — 1968. — Vol. 19. — P. 912–918.

[27] *Baumslag, G.* Residual nilpotency and relations in free groups // Journal of Algebra. — 1965. — Vol. 2. — P. 271–282.

[28] *Birman, J. S.* Braids, links and mapping class groups. — Princeton, New Jersey : Princeton University Press, 1974.

[29] *Büchi, J. R.* Definability in the existential theory of concatenation / J. R. Buchi, S. Senger // Zeitschrift für mathematische Logik und Grundlagen der Mathematik — 1988. — V. 34, № 4. — P. 337–342.

[30] *Büchi, J. R.* Coding in the existential theory of concatenation / J. R. Buchi, S. Senger // Archive for Mathematical Logic. — 1986/87. Bd. 26. — P. 101–106.

[31] *Coulbois, T.* Equations in free groups are not finitely approximable / T. Coulbois, A. Khelif // Proceedings of the American mathemetical society. — 1999. — V. 127, № 4. — P. 963–965.

[32] *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.

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

[34] *Diekert, V.* The existential theory of equations with rational constraints in free groups is PSPACE-complete / V. Diekert, C. Gutierrez, C. Hagenah // Informatiion and Computation. — 2005. — Vol. 202. — P. 105–140.

[35] *Edmunds, C. C.* On the endomorphisms problem for free group // Communications in Algebra. — 1975. — Vol. 3. — P. 7–20.

[36] *Gassner, B. J.* On braid groups // Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. — 1961. — Vol. 25. — P. 10–22.

[37] *Lyndon, R. C.* Equations in free groups // Transactions of the American Mathematical Society. — 1960. — Vol. 96. — P. 445–457.

[38] *Schulz, K. U.* Makanin's Algorithm for Word Equations - Two Improvements and a Generalization // Lecture Notes in Computer Science. — 1990. — Vol. 572. — P. 85–150.

[39] *Schupp, P. E.* On the substitution problem for free groups // Proceedings of the American Mathematical Society. — 1969. — Vol. 23. — P. 421–423.

[40] *Tarski, A.* Undecidable theories / A. Tarski, A. Mostowski, R. M. Robinson. — NY. — 1953.

Библиографическая ссылка

Дурнев, В. Г. Алгоритмические проблемы для уравнений в свободных группах и полугруппах с ограничениями на решения / В. Г. Дурнев, А. И. Зеткина // Всероссийская научная конференция «Математические основы информатики и информационно-коммуникационных систем». Сборник трудов. — Тверь : ТвГУ, 2021. — С. 25–41.
https://doi.org/10.26456/mfcsics-21-3

Сведения об авторах

1. Валерий Георгиевич Дурнев
Ярославский государственный университет им. П. Г. Демидова. Профессор кафедры компьютерной безопасности и математических методов обработки информации

Россия, 150000, Ярославль, ул. Советская, 14/2, ЯрГУ
E-mail: durnev@uniyar.ac.ru

2. Алена Игоревна Зеткина
Ярославский государственный университет им. П. Г. Демидова. Аспирант

Россия, 150000, Ярославль, ул. Советская, 14/2, ЯрГУ
E-mail: a.zetkina1@uniyar.ac.ru