S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 16, стр. 144–144 (2019) УДК 512.54, 510.53
DOI 10.33048/semi.2019.16.xxx MSC 20F10

ПОЛОЖИТЕЛЬНЫЕ ЭЛЕМЕНТЫ И ДОСТАТОЧНЫЕ УСЛОВИЯ РАЗРЕШИМОСТИ ПРОБЛЕМЫ ВХОЖДЕНИЯ В ПОДМОНОИД НИЛЬПОТЕНТНОЙ ГРУППЫ КЛАССА ДВА

В.А. РОМАНЬКОВ

Abstract. Over the past 20-25 years, a fruitful connection has emerged between group theory and computer science. Significant attention began to be paid to the algorithmic problems of group theory in view of their open applications. In addition to the traditional questions of solvability, the questions of complexity and effective solvability began to be studied. This paper provides a brief overview of this area. Attention is drawn to algorithmic problems related to rational subsets of groups which are a natural generalization of regular sets. The submonoid membership problem for free nilpotent groups, which has attracted the attention of a number of researchers in recent years, is considered. It is shown how the apparatus of subsets of positive elements makes it possible to obtain sufficient conditions for the solvability of this problem in the case of nilpotency class two. Note that the author announced a negative solution to this problem for a free nilpotent group of nilpotency class two of sufficiently large rank (the full proof is in print). This gives an answer to the well-known question of Lohrey-Steinberg about the existence of a finitely generated nilpotent

Roman'kov, V.A., Positive elements and sufficient conditions for solvability of the submonoid membership problem for nilpotent groups of class two.

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

Поступила ? апреля 2022 г., опубликована ? ?? 2022 г.

GROUP WITH AN UNDECIDABLE SUBMONOID MEMBERSHIP PROBLEM. IN VIEW OF THIS RESULT, FINDING SUFFICIENT CONDITIONS FOR THE DECIDABILITY OF THIS PROBLEM FOR NILPOTENT GROUPS OF CLASS TWO IS AN URGENT PROBLEM.
Keywords: nilpotent group, submonoid membership problem, rational set, positive elements, solvability.

1. Введение

За последние 20–25 лет обозначилась плодотворная связь между теорией групп и компьютерными науками. Особое внимание стало уделяляться алгоритмам, их сложности и эффективности. В данной работе представлен краткий обзор этой области исследований. Обращено внимание на алгоритмические вопросы связанные с рациональными подмножествами групп – естественным обобщением регулярных множеств, т.е. формальных языков, имеющих прямое отношение к компьютерным наукам. Рассмотрена проблема вхождения в конечно порожденные подмоноиды свободных нильпотентных групп, привлекающая внимание ряда исследователей в последние годы. Показано, как аппарат положительных подмножеств элементов позволяет получить достаточные условия разрешимости этой проблемы в случае класса нильпотентности два. Заметим, что автором в работе [50] анонсировано отрицательное решение этой проблемы для свободной нильпотентной группы класса два достаточно большого ранга (полное доказательство находится в печати). Тем самым дан ответ на известный вопрос Лори-Стейнберга (см. [23], проблема 24) о существовании конечно порожденной нильпотентной группы с неразрешимой проблемой вхождения в подмоноиды. Заметим, что до настоящего времени был известен только один результат по этой проблеме: в статье [12] доказана ее разрешимость для группы Гейзенберга, т.е. свободной нильпотентной группы класса два ранга два. Уже в этом, в определенном смысле минимальном случае, полученный алгоритм далеко нетривиален.

Алгоритмические проблемы в группах представляют классическую тему исследований в алгебре, имеющую топологические истоки и аналоги. В начале прошлого столетия Макс Ден определил три фундаментальные алгоритмические проблемы: равенства, сопряженности и вхождения в конечно порожденные подгруппы (кратко – вхождения), а Генрих Титце ввел в рассмотрение проблему изоморфизма. После более чем сорока лет исследования был получен ряд результатов показывающих неразрешимость этих проблем в классе всех конечно определенных групп. П.С. Новиков [36], [37] доказал неразрешимость проблемы равенства, из чего следуют неразрешимости проблем сопряженности и вхождения. С.И. Адян [1], [2] доказал неразрешимость проблемы изоморфизма любой фиксированной конечно определенной группе.

Круг алгоритмических проблем был с течением времени значительно расширен. Проблемы ставились для конкретных классов групп, например, многообразий. Появлялись совершенно новые проблемы. Соответственно расширялся и круг исследований. В работах С.И. Адяна [1], [2] и М. Рабина [38] была доказана алгоритмическая нераспознаваемость всех Марковских свойств.

В то же время оказалось, что в некоторых важных классах групп классические алгоритмические проблемы разрешимы. Например, все они оказались разрешимыми для полициклических, в частности, конечно порожденных нильпотентных групп. Наиболее сложными являлись проблемы сопряженности (для полициклических групп) и изоморфизма (для нильпотентных и полициклических групп). Первая была решена В.Н. Ремесленниковым [39] и независимо Э. Форманеком [14]. Вторая в нильпотентном случае – Ф. Грюневальдом и Д. Сегалом [16], [17] (а также при некотором условии (установленном впоследствии) – Р.А. Саркисяном [52], [53]); в полициклическом случае – Д. Сегалом [54].

В классе конечно определенных разрешимых групп оказались неразрешимыми все классические проблемы, начиная с проблемы равенства, неразрешимость которой установлена О.Г. Харлампович [21]. Построенные примеры имеют ступень разрешимости не меньше чем три. Метабелев случай особый, в нем основные проблемы Дена разрешимы. В классе конечно порожденных метабелевых групп разрешимость проблемы равенства установлена Е.И. Тимошенко [55], проблемы сопряженности – Г.А. Носковым [34], проблемы вхождения – Н.С. Романовским [41], [42]. Разрешимость проблемы изоморфизма – до сих пор открытый вопрос. Обзоры известных результатов по алгоритмическим проблемам теории групп содержатся в [3], [6], [7], [8], [9], [28], [35], [40], [46], [54]. См. также недавний обзор автора по алгоритмической теории разрешимых групп [51].

Алгоритмические проблемы оказали сильное влияние на развитие современной компьютерной науки. Начиная с 60-х годов прошлого столетия, в которые обозначился рост интереса к проблемам сложности, в центре внимания как математиков, так и специалистов в компьютерных науках, оказались вопросы вычислительной сложности теоретико-групповых алгоритмов. Некоторые идеи, известные в теории сложности, позволили получить результаты высокого уровня в алгоритмической теории групп. До этого алгоритмические проблемы теории групп исследовались в основном с точки зрения их разрешимости. Р. Липтоном и И. Залстейном [22] был разработан логарифмический по сложности алгоритм решения проблемы равенства в конечно порожденных линейных группах. Это был первый результат такого сорта. За последние годы появился целый ряд результатов об алгоритмах в теории групп, имеющих малую сложность (см., например, [4], [25], [26]). Эти результаты имеют практическое значение. Новые связи между теорией групп и теорией сложности были установлены в теории автоматов, компрессии данных и т.п.

В настоящее время алгоритмические проблемы теории групп приобрели еще большее внимание, поскольку на их трудноразрешимости в некоторых классах некоммутативных групп основываются схемы алгебраической криптографии, а сами группы служат платформами для реализации этих схем и соответствующих алгоритмов. Значительно возрос интерес к сложности алгоритмов, решающих такие задачи, возможности их эффективного использования в практических приложениях. Этим вопросам посвящены монографии [30], [31] и [49].

Проблему вхождения в подмоноид некоммутативной группы в настоящее время рассматривают как перенесение классической проблемы целочисленного линейного программирования, где фигурирует проблема вхождения в подмоноид свободной абелевой группы, на некоммутативную платформу. Возникло

и развивается новое направление исследований – некоммутативная дискретная оптимизация. Этому направлению посвящена глава "Discrete optimization in groups" в книге [5]. При этом особое внимание уделяется классу конечно порожденных нильпотентных групп, как наиболее близкому к классу абелевых групп.

В настоящей статье рассматривается проблема вхождения элементов группы в конечно порожденный подмоноид, представляющая важнейший фрагмент более общей проблемы вхождения в рациональное подмножество. В работе представлены достаточные условия для подмоноида свободной нильпотентной группы класса два, когда указанная проблема алгоримически разрешима. Они сформулированы на языке положительных множеств элементов группы (см. определения далее). Получен критерий приведения множества элементов свободной нильпотентной группы класса два к положительному виду и ряд других вспомогательных результатов, имеющих самостоятельное значение.

Структура работы следующая. В разделе 2 приводится ряд определений и краткий обзор результатов о проблеме вхождения в рациональные подмножества группы. Раздел 3 содержит утверждения о потенциально положительных элементах свободных абелевых групп и свободных нильпотентных групп класса 2. Раздел 4 посвящен подготовке к формулировке и доказательству основного результата – Теоремы 4. В разделе 5 приведена Теорема 4, в которой представлены достаточные условия разрешимости проблемы вхождения в конечно порожденный подмоноид свободной нильпотентной группы класса два.

Далее в статье используются стандартные обозначения свободной абелевой группы A_r ранга r и свободной нильпотентной группы $N_{r,l}$ ранга r класса нильпотентности l. Через $[x,y] = x^{-1}y^{-1}xy$ обозначается коммутатор элементов x, y некоторой группы G, а через G' – ее коммутант. Для $X \subseteq G$ выражение $\text{гр}(X)$ обозначает подгруппу, а $\text{мон}(X)$ – подмоноид группы G, порожденные X. Как обычно, $\mathbb{Q}$ обозначает множество рациональных, $\mathbb{Z}$ – множество целых, а $\mathbb{N}$ – множество натуральных чисел. Для ненулевых целых чисел $t_1, \ldots, t_k$ через $\text{нод}(t_1, \ldots, t_k)$ обозначается их наибольший общий делитель, а через $\text{нок}(t_1, \ldots, t_k)$ – наименьшее общее кратное. Для кольца K через $\mathrm{M}_r(K)$ обозначается кольцо $r \times r$ матриц над K, а через $\mathrm{GL}_r(K)$ соответствующая группа всех обратимых матриц.

2. Проблема вхождения в рациональные подмножества группы

Приведем некоторые определения. Класс рациональных подмножеств $\mathrm{Rat}(G)$ группы G есть наименьший класс, содержащий все конечные подмножества группы (включая пустое), замкнутый относительно операций объединения, умножения и операции Клини порождения подмножеством K подмоноида K^* группы G. Понятие рационального подмножества группы является естественным обобщением классического понятия регулярного подмножества свободного моноида. Заметим, что произвольная подгруппа H группы G рациональна тогда и только тогда, когда она конечно порождена. Очевидно, что конечно порожденный подмоноид является рациональным подмножеством. Справедлив аналог теоремы Клини о задании регулярных подмножеств свободного моноида конечными автоматами: подмножество R группы G является рациональным тогда и только тогда, когда R является выпускным множеством конечного автомата над G. Детальные сведения относительно определений и основных

свойств рациональных подмножеств в группах см. в монографии [45] или статье [15].

В общем случае семейство $\mathrm{Rat}(G)$ не замкнуто относительно операций пересечения и дополнения. Результаты по характеризации конечно порожденных групп G, в которых $\mathrm{Rat}(G)$ является булевой алгеброй, то есть замкнутым не только относительно операции объединения, но и относительно операций пересечения и дополнения семейством, приведены в [48] и [45]. Вопрос о рациональности вербальных подмножеств свободных групп исследован в [29].

Исследованиями проблемы вхождения в рациональные подмножества групп занимались многие авторы. См. по этому поводу обзорную статью М. Лори [23]. В ней автор сформулировал проблему 24 о существовании конечно порожденной нильпотентной группы с неразрешимой проблемой вхождения в подмоноиды. Данная проблема неоднократно затрагивалась в докладах Б. Стейнберга на различных научных семинарах.

Автором в работе [50] анонсировано отрицательное решение этой проблемы (полное доказательство находится в печати). А именно: объявлено существование в свободной нильпотентной группе $N_{r,2}$ достаточно большого ранга r конечно порожденного подмоноида M, проблема вхождения в который алгоритмически неразрешима. Множество порождающих элементов подмоноида M эффективно строится по фиксированному диофантову многочлену $D(\zeta_1, \ldots, \zeta_s)$, определяющему неразрешимое семейство диофантовых уравнений вида $D(\zeta_1, \ldots, \zeta_s) = \upsilon, \upsilon \in \mathbb{Z}$, существование которого следует из результатов Ю.В. Матиясевича о неразрешимости 10-й проблемы Гильберта (см., например, [27]). Параметр r зависит от s и вида многочлена $D(\zeta_1, \ldots, \zeta_s)$. Представлен эффективный класс элементов $\{g(\upsilon), \upsilon \in \mathbb{Z}\}$ группы $N_{r,2}$ такой, что $g(\upsilon) \in M$ тогда и только тогда, когда соответствующее уравнение $D(\zeta_1, \ldots, \zeta_s) = \upsilon$ разрешимо в целых числах. Из этих результатов вытекает объявленная неразрешимость проблемы вхождения в подмоноид M.

Приведем некоторые известные результаты по проблеме вхождения в рациональные подмножества группы.

Положительные результаты:

- М. Бенуа [10]. Проблема вхождения в рациональные подмножества разрешима в свободных группах.
- С. Эйленберг, М. П. Шютценберже [13] (независимое доказательство в [32]). Проблема вхождения в рациональные подмножества разрешима в абелевых группах.
- З. Грюншлаг [18]. Разрешимость проблемы вхождения в рациональные подмножества сохраняется при конечных расширениях групп.
- М. Ю. Недбай [33]. Разрешимость проблемы вхождения в рациональные подмножества сохраняется при свободных произведениях групп.

Отрицательные результаты:

- В. А. Романьков [44]. Для любого $l \geq 2$ и достаточно большого r в свободной нильпотентной группе $N_{r,l}$ неразрешима проблема вхождения в рациональные подмножества.
- М. Лори, Б. Стейнберг [24]. Свободная метабелева группа M_r ранга $r \geq 2$ содержит конечно порожденный подмоноид с неразрешимой проблемой вхождения.

Доказательство в [44] основываются на неразрешимости 10-й проблемы Гильберта, а в [24] – на неразрешимости проблемы комбинаторного замощения. Относительно других многочисленных результатов по проблеме вхождения в рациональные подмножества групп см. обзор [23].

Для постановки алгоритмической проблемы необходимо указывать способ эффективного задания как самой группы, так и соответствующего проблеме семейства подмножеств, в рассматриваемом случае – семейства конечно порожденных подмоноидов. В данной работе предполагается, что группа задана конечным множеством порождающих элементов и определяющих соотношений, а любой ее конечно порожденный подмоноид задан своим конечным множеством порождающих элементов. В доказательствах фигурируют свободные абелевы и свободные нильпотентные группы, в качестве порождающих для которых выбраны их базисы. Считаем, что соотношения между порождающими элементами определяются тождествами коммутативности и нильпотентности, соответственно. Напомним, что тождество нильпотентности любого класса может быть задано конечным числом соотношений. Кроме этого используются известные нормальные формы записи элементов рассматриваемых групп. Эти сведения и другую подробную информацию о нильпотентных группах можно найти в лекциях Ф. Холла [19] и монографии М. Холла [20].

Стоит заметить, что проблема вхождения в конечно порожденный подмоноид свободной абелевой группы $A_r \simeq \mathbb{Z}^r$ имеет отношение к следующей задаче целочисленного линейного программирования.

Для данной матрицы $A \in \mathrm{M}_{m\times r}$ и вектора $b \in \mathbb{Z}^r$ определить, существует ли решение $x \in \mathbb{N}^m$ уравнения $xA = b$.

На теоретико-групповом языке это проблема вхождения в подмоноид группы A_r, порожденный строками матрицы A. Хорошо известно, что эта версия проблемы целочисленного линейного программирования принадлежит классу NP-полных проблем. Проблему вхождения в конечно порожденные подмоноиды произвольных групп в настоящее время рассматривают как естественное обобщение проблемы целочисленного линейного программирования. Обзор соответствующих результатов можно найти в книге [5].

3. Подмножества потенциально положительных элементов групп A_r и $N_{r,2}$

Определение 1. *Пусть $\mathcal{C}$ - многообразие групп. Обозначим через $F_r(\mathcal{C})$ свободную группу ранга r этого многообразия.*

- *Для фиксированного базиса $X_r = \{x_1, \ldots, x_r\}$ группы $F_r(\mathcal{C})$ нетривиальный элемент $g \in F_r(\mathcal{C})$ называется положительным, если он принадлежит подмоноиду $M = мон(X_r)$, порожденному элементами выбранного базиса X_r. Другими словами: если элемент g записывается в форме слова $g = g(x_1, \ldots, x_r)$ от положительных степеней элементов базиса X_r. Элемент g строго положителен, если в его записи присутствуют все элементы базиса X_r в положительных степенях.*
- *Элемент $g \in F_r(\mathcal{C})$ называется потенциально положительным, если он положителен в некотором базисе X'_r группы $F_r(\mathcal{C})$. Другими словами: если существует автоморфизм α группы $F_r(\mathcal{C})$ такой, что образ $\alpha(g)$ положителен.*

Данные определения естественно расширяются на подмножества элементов группы $F_r(\mathcal{C})$.

Наша следующая задача – дать критерии потенциальной положительности конечных подмножеств групп A_r и их пополнений $A_r^{\mathbb{Q}}$, а также групп $N_{r,2}$ для любого $r \in \mathbb{N}$.

Вначале рассмотрим группу $A_r = \mathbb{Z}^r$ в аддитивной записи. Пусть $E_r = \{e_1, \dots, e_r\}$, где $e_1 = (1, 0, \dots, 0), \dots, e_r = (0, \dots, 0, 1)$ – стандартный базис. Элементами группы A_r являются целочисленные векторы $a = (\alpha_1, \dots, \alpha_r)$. Вектор a положителен (пишем $a \geq 0$), если его координаты удовлетворяют неравенствам $\alpha_i \geq 0, i = 1, \dots, r$, и потенциально положителен, если он положителен в некотором базисе группы A_r. Эквивалентно, если существует обратимое линейное преобразование (автоморфизм) μ группы $\mathbb{Z}^r$, для которого образ $\mu(a)$ положителен. Это означает, что для матрицы $T = T(\alpha) \in \mathrm{GL}_r(\mathbb{Z})$ данного преобразования выполнено неравенство $aT \geq 0$.

Пусть $A_r^{\mathbb{Q}} = \mathbb{Q}^r$ обозначает стандартное пополнение группы A_r до векторного пространства над $\mathbb{Q}$, а $A_r^{\mathbb{R}} = \mathbb{R}^r$ – над $\mathbb{R}$, с тем же самым базисом E_r. Таким образом зафиксированы вложения $\mathbb{Z}^r \subseteq \mathbb{Q}^r \subseteq \mathbb{R}^r$. При этом линейно независимые множества векторов из $\mathbb{Q}^r$ остаются линейно независимыми над $\mathbb{R}$ в $\mathbb{R}^r$. Понятия положительности и потенциальной положительности элементов и подмножеств естественным образом переносится на группы $\mathbb{Q}^r$ и $\mathbb{R}^r$.

Следующие две леммы понадобятся в дальнейших доказательствах теорем.

Лемма 1. *Пусть V – конечномерное векторное пространство над полем $\mathbb{Q}$ с базисом $E_r = \{e_1, \dots, e_r\}$. Пусть B – конечное множество векторов, у которых фиксированная координата, для определенности, последняя, неотрицательна. Пусть $B_0 \subseteq B$ – все векторы с нулевой, а $B_{>0}$ – с положительной выделенной координатой. Тогда можно перейти к новому базису $E'_r = \{e'_1, \dots, e'_r\}$, для которого $e'_1 = e_1, \dots, e'_{r-1} = e_{r-1}$ и $e'_r = e_r - \sum_{i=1}^{r-1} \gamma_i e_i$, $\gamma_i > 0$, в котором векторы из B_0 сохраняют свои координаты, а векторы из $B_{>0}$ имеют строго положительные координаты.*

Доказательство. Утверждение относительно B_0 очевидно.

Пусть $B_{>0} = \{b_1, \dots, b_k\}$, $b_i = (\alpha_{i,1}, \dots, \alpha_{i,r})$, $i = 1, \dots, k\}$. В базисе E'_r вектор $b_i \in B_{>0}$ выглядит следующим образом:

$$b_i = \sum_{j=1}^{r-1} (\alpha_{i,j} + \gamma_i \alpha_{i,r}) e_j + \alpha_{i,r} e'_r.$$

По предположению $\alpha_{i,r} > 0$. Выберем γ_i для каждого $i = 1, \dots, k$ таким образом, чтобы выполнялись неравенства $\alpha_{i,j} + \gamma_i \alpha_{i,r} > 0$. Тогда будет выполнено утверждение относительно $B_{>0}$.

□

Следствие 1. *Пусть B – конечный набор векторов пространства $\mathbb{Q}^r$ с фиксированным базисом E_r, у которых определенная координата, скажем, последняя, положительна. Тогда преобразование базиса, описанное в Лемме 1, позволяет получить базис E'_r, в котором все координаты векторов из B строго положительны.*

Доказательство. Утверждение прямо вытекает из Леммы 1. Нужно только заметить, что в ее обозначениях $B = B_{>0}$. □

Лемма 2. *Пусть система равенств и неравенств*

$$(1)\qquad \begin{cases} \alpha_{1,1}x_1 + \ldots + \alpha_{1,r}x_r = 0 \\ \ldots \\ \alpha_{k,1}x_1 + \ldots + \alpha_{k,r}x_r = 0 \\ \alpha_{k+1,1}x_1 + \ldots + \alpha_{k+1,r}x_r > \lambda \\ \ldots \\ \alpha_{k+l,1}x_1 + \ldots + \alpha_{k+l,r}x_r > \lambda \end{cases},$$

где $\alpha_{i,j} \in \mathbb{Q}, \lambda \in \mathbb{R}$, *имеет решение в вещественных числах. Тогда она имеет решение в рациональных числах*

Доказательство. Считаем, что зафиксирован базис $E_r = \{e_1, \ldots, e_r\}$ пространства $\mathbb{Q}^r$, являющийся также базисом его естественного пополнения – пространства $\mathbb{R}^r$. Наборы коэффициентов $b_i = (\alpha_{i,1}, \ldots, \alpha_{i,r}), i = 1, \ldots, k+l$, из (1) рассматриваются как элементы пространства $\mathbb{Q}^r$.

Пусть $v = (v_1, \ldots, v_r) \in \mathbb{R}^r$ – решение системы (1). После подстановки v вместо x в уравнения и неравенства системы (1) получим набор равенств, которые запишем на языке скалярных произведений:

$$(2)\qquad \begin{cases} \langle b_1, v\rangle = 0 \\ \ldots \\ \langle b_k, v\rangle = 0 \\ \langle b_{k+1}, v\rangle = \lambda + \delta_1 \\ \ldots \\ \langle b_{k+l}, v\rangle = \lambda + \delta_l \end{cases},$$

где $\delta_j > 0, j = 1, \ldots, l$. Полагаем $\delta = \min\{\delta_j : j = 1, \ldots, l\}$.

Пусть $\alpha = \max\{|\alpha_{i,j}| : i = k+1, \ldots, k+l; j = 1, \ldots, r\}$. Возьмем $\varepsilon > 0$ такое, что

$$(3)\qquad r \cdot \varepsilon \cdot \alpha < \delta.$$

Если некоторый вектор $v' = (v'_1, \ldots, v'_r) \in \mathbb{Q}^r$ удовлетворяет всем уравнением системы (1) и в то же время выполнены неравенства $|v_i - v'_i| \leq \varepsilon$, то v' является искомым решением системы (1). Перейдем к доказательству существования такого вектора.

Пусть $V = \mathrm{Lin}_{\mathbb{Q}}(\alpha_{1-k})$ – подпространство в $\mathbb{Q}^r$, порожденное векторами $\alpha_1, \ldots, \alpha_k$. Пусть $m = \dim(V)$ – его размерность. Тогда ортогональное дополнение $V^{\perp}_{\mathbb{Q}}$ в $\mathbb{Q}^r$ имеет размерность $r-m$. Запишем его базис $\tilde{E}_{r-m} = \{\tilde{e}_1, \ldots, \tilde{e}_{r-m}\}$ через базис E_r (если в системе (1) отсутствуют равенства, то $\tilde{E}_r = E_r$):

$$(4)\qquad \tilde{e}_i = \sum_{j=1}^{r} \gamma_{j,i} e_j,\ \gamma_{j,i} \in \mathbb{Q},\ i = 1, \ldots, r-m.$$

Базис $\tilde{E}_{r-m}$ является также базисом ортогонального дополнения $V^{\perp}_{\mathbb{R}}$ в $\mathbb{R}^r$.

Имеем разложение

$$(5)\qquad v = \sum_{i=1}^{r-m} \tilde{v}_i \tilde{e}_i,\ \tilde{v}_i \in \mathbb{R}.$$

Из равенств (4) и (5) получаем равенства

$$\begin{cases} \upsilon_1 = \sum_{i=1}^{r-m} \tilde{\upsilon}_i \gamma_{i,1} \\ \dots \\ \upsilon_r = \sum_{i=1}^{r-m} \tilde{\upsilon}_i \gamma_{i,r} \end{cases} . \tag{6}$$

Пусть $\gamma = \max\{|\gamma_{i,j}| : i = 1, \dots, r-m; j = 1, \dots, r\}$. Возьмем $\varepsilon' > 0$ такое, что

$$(r-m) \cdot \varepsilon' \cdot \gamma < \varepsilon, \tag{7}$$

где параметр ε тот же самый, что фигурирует в неравенстве (3). Выберем значения $\tilde{\upsilon}'_i \in \mathbb{Q}$ такие, что $|\tilde{\upsilon}_i - \tilde{\upsilon}'_i| \le \varepsilon'$. Определим набор $\upsilon' = (\upsilon'_1, \dots, \upsilon'_r) \in \mathbb{Q}^r$, где $\upsilon'_i = \sum_{j=1}^{r-m} \tilde{\upsilon}'_j \gamma_{i,j}$, $i = 1, \dots, r$. Из неравенства (7) следует, что

$$|\upsilon_i - \upsilon'_i| \le \varepsilon.$$

Тогда υ' будет являться решением системы (1).

□

Определение 2. *Подмножество $B = \{b_1, \dots, b_s\}$ группы A_r или группы $A_r^{\mathbb{Q}}$ называется положительно независимым, если равенство $\sum_{i=1}^{s} \alpha_i b_i = 0$ для $\alpha_i \in \mathbb{Q}, \alpha_i \ge 0, i = 1, \dots, s$, влечет равенства $\alpha_i = 0, i = 1, \dots, s$.*

В противном случае B называется положительно зависимым.

Следующая теорема доказана в [56]. К сожалению, в ее доказательстве есть существенный пробел. Поэтому мы даем новое доказательство, устраняющее этот пробел и другие неточности.

Теорема 1. *Подмножество элементов $B = \{b_1, \dots, b_s\}$ группы $A_r^{\mathbb{Q}} \simeq \mathbb{Q}^r$ потенциально положительно тогда и только тогда, когда B положительно независимо. Более того, для любого положительно независимого подмножества B найдется базис пространства $\mathbb{Q}^r$, в котором все координаты векторов из B строго положительны.*

Доказательство. Очевидно, что любое положительно зависимое подмножество B не является потенциально положительным.

Пусть B положительно независимое множество, записанное в базисе $E_r = \{e_1, \dots, e_r\}$ пространства $\mathbb{Q}^r$: $b_i = (\alpha_{i,1}, \dots, \alpha_{i,r})$, $i = 1, \dots, s$. Как и раньше, считаем, что E_r является базисом пространства $\mathbb{R}^r$. Используем индукцию по r. Утверждение очевидно при $r = 1$ и произвольном s, так как любая система, содержащая хотя бы два разнонаправленных вектора, положительно линейно зависима, а система однонаправленных векторов либо положительна, либо становится таковой при замене базисного вектора на противоположный. Предположим, что утверждение теоремы верно для любого пространства $\mathbb{Q}^n$ размерности $n < r$.

Рассмотрим порожденный векторами из B конус

$$C = C(b_1, ..., b_m) = \{\sum_{i=1}^{m} \alpha_i b_i, \alpha_i \in \mathbb{Q}, \alpha_i \ge 0, i = 1, \dots, m\}.$$

Подмножества $C, -C, C \setminus \{0\}, -C \setminus \{0\}$ выпуклые. В рассматриваемом случае подмножества $C \setminus \{0\}, -C \setminus \{0\}$ не пересекаются. Считаем пространство $\mathbb{Q}^r$ для любого n естественно вложенным в евклидово пространство $\mathbb{R}^r$. Обозначим

через $C^{\mathbb{R}}$ выпуклую оболочку конуса C в $\mathbb{R}^r$. Очевидно, что множества $C^{\mathbb{R}} \setminus \{0\}$ и $-C^{\mathbb{R}} \setminus \{0\}$ также не пересекаются.

Используем следующую версию теоремы Минковского о гиперплоскости, разделяющей выпуклые множества (см., например, монографию [11], стр. 46). Пусть U и W – не пересекающиеся выпуклые подмножества пространства $\mathbb{R}^n$. Тогда существует ненулевой вектор v и вещественное число λ такие, что $\langle x, v\rangle \geq \lambda$ для всех $x \in U$ и $\langle y, v\rangle \leq \lambda$ для всех $y \in W$; то есть гиперплоскость $\langle \cdot, v\rangle = \lambda$, для которой v – нормальный вектор, разделяет U и W.

Значит, существует гиперплоскость $H^{\mathbb{R}}$ пространства $\mathbb{R}^r$ разделяющая $U = C^{\mathbb{R}} \setminus \{0\}$ и $W = -C^{\mathbb{R}} \setminus \{0\}$. Все векторы из B разбиваются на два подмножества: B_0 – векторы, принадлежащие H, и $B_{>0}$ – векторы, не принадлежащие H.

Пусть $B_0 = \{b_1, \ldots, b_k\}$, $B_{>0} = \{b_{k+1}, \ldots, b_{k+l}$, $k + l = s$. Тогда v является решением системы (1).

По лемме 2) система (1) имеет решение $v' \in \mathbb{Q}^r$. Определим гиперплоскость H' пространства $\mathbb{Q}^r$ через нормаль v'. Выберем в H' базис $E'_{r-1} = \{e'_1, \ldots, e'_{r-1}\}$, в котором векторы $b_1, \ldots, b_k$ имеют строго положительные координаты. Дополним E'_{r-1} до базиса E'_r всего пространства $\mathbb{Q}^r$ вектором $e'_r = v'$. Заметим, что последние координаты векторов из $B = B_{>0}$ в этом базисе строго положительны. Тогда по Следствию 1 существует базис E''_r пространства $\mathbb{Q}^r$, в котором все координаты любого вектора из $B_{>0}$ строго положительны.

Остается заметить, что первые координаты всех векторов из B в базисе E''_r теперь строго положительны. По Следствию 1 существует базис E'''_r пространства $\mathbb{Q}^r$, в котором все координаты векторов из B строго положительны.

□

Следующая теорема установлена в [57], где ее доказательство опиралось на работу [56], содержащую пробел.

Теорема 2. *Подмножество нетривиальных элементов $B = \{b_1, \ldots, b_s\}$ группы $A_r = \mathbb{Z}^r$ потенциально положительно тогда и только тогда, когда оно положительно независимо. Для любого положительно независимого подмножества B найдется базис пространства $\mathbb{Q}^r$, в котором все координаты векторов из B строго положительны.*

Доказательство. Очевидно, что положительно зависимое подмножество B не является потенциально положительным.

Пусть $B = \{b_i = (\beta_{i,1}, \ldots, \beta_{i,r}), i = 1, \ldots, s\}$ – подмножество положительно независимых векторов группы $\mathbb{Z}^r \subseteq \mathbb{Q}^r$. По Теореме 1 существует матрица $T \in \mathrm{GL}_r(\mathbb{Q})$ такая, что $c_i = b_i T = (\gamma_{i,1}, \ldots, \gamma_{i,r})$ – вектор со строго положительными координатами для любого $i = 1, \ldots, s$.

Пусть $T = \nu^{-1} T_1$, где $\nu \in \mathbb{N}$ и $T_1 \in \mathrm{M}_r(\mathbb{Z})$. Пусть $t_1 = (\tau_{1,1}, \ldots, \tau_{r,1})^{\mathtt{t}}$ – первый столбец матрицы T_1 ($\mathtt{t}$ обозначает транспонирование). Пусть $\delta = \text{нод}(\tau_{1,1}, \ldots, \tau_{r,1})$. Тогда столбец $\tilde{t}_1 = \delta^{-1} t_1$ примитивен, то есть все его координаты взаимно просты в совокупности, и для любого i имеем $b_i \tilde{t}_1 = \lambda_i > 0$.

Хорошо известно, что любой целочисленный примитивный столбец, в нашем случае $\tilde{t}_1$, дополняется до целочисленной обратимой матрицы $\widetilde{T} \in \mathrm{GL}_r(\mathbb{Z})$.

Пусть $b_1 \widetilde{T} = (\mu_{1,1}, \ldots, \mu_{1,r})$. Если для некоторого j выполнено неравенство $\mu_{1,j} \leq 0$, изменим матрицу $\widetilde{T}$, прибавив к j-му столбцу 1-й столбец, умноженный на достаточно большое натуральное число δ_j, для которого $\delta_j \mu_{1,1} + \mu_{1,j} > 0$. Такая операция проводится для всех не строго положительных координат

вектора b_1. Получаем для новой матрицы $\widetilde{T}$ вектор $b_1\widetilde{T}$ со строго положительными координатами.

Так как для любого $i = 2, \dots, r$ первая координата вектора $b_i\widetilde{T}$ положительна, аналогичные операции можно применить для достижения строгой положительности координат всех векторов $b_i\widetilde{T}$ для измененной матрицы $\widetilde{T}$. После всех изменений получается матрица, которую обозначим через T'. Очевидно, что $T' \in \mathrm{GL}_r(\mathbb{Z})$. При этом векторы b_iT' имеют строго положительные координаты для всех $i = 1, ..., s$. Это означает, что векторы $b_1, ..., b_s$ приведены к строго положительному виду.

□

Пусть $N_r = N_{r,2}, r \geq 2, -$ свободная нильпотентная группа с базисом $\{x_1, ..., x_r\}$, и $A_r = N_r/N_r'$ – свободная абелева группа с базисом $\{a_1, \dots, a_r\}$, где $a_i = \bar{x}_i = x_iN_r'$. Для любого элемента $g \in N_r$ через $\bar{g}$ обозначим образ g относительно стандартного гомоморфизма $N_r \to A_r$. Аналогичное обозначение $\bar{U}$ используем также для подмножеств $U \subseteq N_r$.

Следующая теорема для случая $r = 2$ (то есть для группы Гейзенберга) доказана в [58].

Теорема 3. *Подмножество нетривиальных элементов $U = \{u_1, ..., u_s\}$ группы N_r потенциально положительно тогда и только тогда, когда подмножество $\bar{U} = \{\bar{u}_1, ..., \bar{u}_s\}$ положительно независимо в A_r.*

Доказательство. Очевидно, что если $\bar{U}$ положительно зависимо в A_r, то по Теореме 2 это подмножество не будет потенциально положительным в A_r. Тогда U не будет потенциально положительным в N_r.

Пусть подмножество $\bar{U}$ положительно независимо в A_r. Так как любой автоморфизм группы A_r индуцирован автоморфизмом группы N_r (см., например, обзор [43] или монографию [47]), то по Теореме 2 можно считать, что $\bar{U}$ строго положительно в A_r. Тогда каждый элемент $u_i \in U$ записывается в виде

$$u_i = \prod_{j=1}^{r} x_j^{\lambda_{i,j}} \prod_{k,l \in \{1,\dots,r\}, k>l} [x_k, x_l]^{\mu_{i,k,l}}, \lambda_{i,j} > 0, \mu_{i,k,l} \in \mathbb{Z}. \tag{8}$$

Коммутаторы от элементов базиса группы N_r упорядочим следующим образом: полагаем $[x_i, x_j] > [x_p, x_q]$, если $i > p$, или $i = p$ и $j > q$. Заметим, что представление, в котором коммутаторы записаны в соответствии с упорядочением, единственно.

Для нахождения положительного представления подмножества U исключим из записи (8) степени коммутаторов. При этом степени элементов базиса будут входить в запись несколько раз. Действуем следующим образом. Выберем натуральное число $\tau_{2,1} > \max\{|\mu_{i,2,1}| : i = 1, \dots, s\}$ и определим автоморфизм $\varphi_{2,1} : x_1 \mapsto x_2^{\tau_{2,1}} x_1 x_2^{\tau_{2,1}}, x_i \mapsto x_i$ для $i \geq 2$.

Тогда для $i = 1, \dots, s$ справедливо равенство следующего вида:

$$\varphi_{2,1}(u_i) = (x_2^{\tau_{2,1}} x_1 x_2^{\tau_{2,1}})^{\lambda_{i,1}} \prod_{j=2}^{r} x_j^{\lambda_{i,j}} [x_2, x_1]^{\mu_{i,2,1}} \cdot$$

$$\cdot \prod_{k>l, (k,l)\neq(2,1)} [x_k, x_l]^{\mu'_{i,k,l}}, \ \mu'_{i,k,l} \in \mathbb{Z}. \tag{9}$$

Для любого выражения $\varphi_{2,1}(u_i)$ заменим в точности одно из подслов вида $x_2^{\tau_{2,1}} x_1 x_2^{\tau_{2,1}}$ на $x_2^{\tau_{2,1}+\mu_{i,2,1}} x_1 x_2^{\tau_{2,1}-\mu_{i,2,1}} [x_2, x_1]^{-\mu_{i,2,1}}$. Сократятся степени коммутатора $[x_2, x_1]$. Степени базисных элементов останутся положительными.

Аналогично, применяя последовательно автоморфизмы

$$\varphi_{3,1}, \ldots, \varphi_{r,1}, \varphi_{3,2}, \ldots, \varphi_{r,r-1},$$

где

$$\varphi_{j,i} : x_i \mapsto x_j^{\tau_{j,i}} x_i x_j^{\tau_{j,i}}, x_k \mapsto x_k$$

для $k \neq i$ для достаточно больших соответствующих значений $\tau_{i,j}$, удалим шаг за шагом изменяющиеся степени коммутаторов

$$[x_3, x_1], \ldots, [x_r, x_1], [x_3, x_2], \ldots, [x_r, x_{r-1}]$$

из правых частей получающихся равенств

$$\varphi_{3,1}(\varphi_{2,1}(u_i)), \ldots, \varphi_{r,r-1}(\ldots(\varphi_{2,1}(u_i))).$$

Заметим, что на каждом следующем шаге изменяются степени только у коммутаторов порядка большего, чем порядок удаляемого коммутатора. Удаленные до этого коммутаторы не появляются. После проведения всех таких преобразований в итоге получим положительное слово. □

Замечание 1. Проверка выполнения условия потенциальной положительности конечного набора векторов группы A_r может быть осуществлена алгоритмически. Для этого упорядочиваются все базисы группы и все возможные ненулевые наборы неотрицательных ненулевых коэффициентов для проверяемых векторов. Затем параллельно проводится процесс переписывания проверяемых векторов в базисах и вычисления положительных линейных комбинаций с последовательными наборами коэффициентов. На конечном шаге мы получим либо положительную запись векторов, либо их положительную зависимость, показывающую согласно Теореме 2, что они не являются потенциально положительными.

4. Предварительные рассмотрения

Пусть $N_r = N_{r,2}$ – свободная нильпотентная группа ранга r ступени нильпотентности 2 с базисом $X_r = \{x_1, \ldots, x_r\}$, $A_r = N_r/N_r'$ – свободная абелева группа ранга r. Любой базис группы N_r индуцирует базис группы A_r. Верно и обратное утверждение: прообраз любого базиса группы A_r является базисом группы N_r. Следовательно, любой автоморфизм группы A_r индуцирован автоморфизмом группы N_r. Коммутант N_r' – свободная абелева центральная подгруппа группы N_r, в качестве базиса которой можно взять множество $\{[x_i, x_j] : i > j; i, j = 1, \ldots, r\}$ В любой конечно порожденной нильпотентной группе, в частности, в группе N_r разрешима проблема равенства. Также разрешима проблема вхождения в подгруппу, при этом можно эффективно записать элемент подгруппы как слово от ее порождающих элементов. Об этих и других фактах см., например, [19], [20]. В дальнейшем они почти всегда используются без ссылок.

Пусть M – конечно порожденный подмоноид группы N_r, заданный некоторым конечным множеством нетривиальных порождающих элементов $Y \cup U$, где Y – подмножество элементов с нетривиальными образами в A_r, а U – подмножество элементов из N_r'. Среди всех элементов из Y выберем максимальное по

включению подмножество $G = \{g_1, \ldots, g_k\}$, образ которого в A_r положительно независим. Полагаем $F = Y \setminus G = \{f_1, \ldots, f_l\}$.

По Теореме 2 считаем, что базис X_r группы N_r выбран таким образом, что в индуцированном базисе $\bar{X}_r$ группы A_r образы элементов из G будут строго положительными. Так как $\bar{G}$ – максимальное положительно независимое подмножество, любое подмножество вида $\bar{G} \cup \{\bar{f}_j\}$ для $j = 1, \ldots, l$ будет положительно зависимым. Это означает существование неотрицательных целых чисел $\alpha_{i.j}, i = 1, \ldots, k, \beta_j \neq 0$ таких, что

$$\prod_{i=1}^{k} \bar{g}_i^{\alpha_{i,j}} = \bar{f}_j^{-\beta_j},\ j = 1, \ldots, l. \tag{10}$$

Значит, любой из элементов $\bar{f}_j$ является строго отрицательным, то есть все коэффициенты его канонического разложения по базису E_r строго меньше нуля.

Полагаем $M_1 = \text{мон}(\bar{G})$, $M_2 = \text{мон}(\bar{F})$. Подмоноид $\bar{M}_G = \text{мон}(\bar{G})$ состоит из положительных элементов, а $\bar{M}_F = \text{мон}(\bar{F})$ – из отрицательных.

В последующем рассуждении базис группы N_r может меняться и порождающие моноида M из G и F могут не сохранять эти свойства, поэтому будем говорить о них, как первоначально положительных и отрицательных элементах.

Если $G = \emptyset$, то $F = \emptyset$. В этом случае проблема вхождения в подмоноид $M \leq N_2'$ разрешима по приведенной в разделе 2 теореме Эйленберга-Шютценберже. Поэтому считаем, что $G \neq \emptyset$.

Считаем, что β_j – минимальное число, для которого $\bar{f}_j^{-\beta_j} \in \bar{M}_G$, $j = 1, \ldots, l$. Пусть $\beta = \text{нок}(\beta_j : j = 1, \ldots, l)$. Тогда для любого элемента $\bar{f} \in \bar{M}_F$ элемент $\bar{f}^{-\beta}$ принадлежит $\bar{M}_G$. То есть обратный к $\bar{f}^{\beta}$ элемент лежит в $\bar{M}_G$.

Пусть $\bar{H}$ обозначает подмоноид группы A_r, состоящий из всех обратимых элементов моноида $\bar{M}$. Тогда $\bar{H}$ – подгруппа группы A_r. Подчеркнем, что по построению любой элемент из $\bar{H}$ имеет прообраз в M. Пусть $\widetilde{H}$ – полный прообраз подгруппы $\bar{H}$ в M. Для любого элемента $h \in \widetilde{H}$ существует перестановочный с ним элемент $h^- \in \widetilde{H}$ такой, что $hh^- \in N_r' \cap M$, то есть $\bar{h}\bar{h}^- = 1$. Элемент h^- определяется неоднозначно. Им может быть любой из прообразов элемента $\bar{h}^{-1}$ в $\widetilde{H}$.

Пусть $I(\bar{F})$ обозначает подгруппу группы A_r, состоящую из всех элементов группы A_r линейно зависимых с элементами из $\bar{F}$. Другими словами, $I(\bar{F})$– изолятор подгруппы $\text{гр}(\bar{F})$ в группе A_r. Подгруппа $\bar{H}$ содержится в $I(\bar{F})$ и имеет в ней конечный индекс. Это следует из того, что любой элемент из $\bar{F}$ в некоторой ненулевой степени попадает в $\bar{H}$, и конечной порожденности любой подгруппы из A_r.

5. Основной результат

Приведем ряд достаточных условий на порождающие элементы подмоноида M, при которых проблема вхождения в M алгоритмически разрешима. Используем введенные в предыдущем разделе понятия и обозначения.

Теорема 4. *Проблема вхождения в подмоноид M в группе N_r алгоритмически разрешима в следующих случаях:*

(1) *Когда конечное множество порождающих элементов подмоноида M состоит из множества элементов G, образы которых потенциально положительны в A_r, и множества U элементов из N'_r. Другими словами, когда $F = \emptyset$.*
(2) *Когда изолятор $I(\bar{F})$ подгруппы, порожденной множеством $\bar{F}$, совпадает с A_r.*

Доказательство. По Теореме 2 выберем базис X_r группы N_r так, что образы элементов из G будут строго положительными в A_r относительно индуцированного базиса $\bar{X}_r$.

Тогда для элемента $h \in N_r$ множество полугрупповых слов вида $g_{i_1} \dots g_{i_q}; g_{i_t} \in G$, таких, что $h = g_{i_1} \dots g_{i_q} w, w \in N'_r$, конечно. Для каждого из них проверим вхождение w в мон(U). Элемент h принадлежит M тогда и только тогда, когда хотя бы одно такое вхождение имеет место. Утверждение (1) доказано.

По условию теоремы изолятор $I(\bar{F})$ совпадает с A_r, значит, подгруппа $\bar{H}$ имеет конечный индекс в A_r. Для любого базисного элемента x_i существует пара перестановочных элементов полного прообраза $\widetilde{H}$ подгруппы $\bar{H}$ в M вида

$$h_i = x_i^{\alpha_i} c_{i,1}, h_i^- = x_i^{-\alpha_i} c_{i,2}; c_{i,1}, c_{i,2} \in N'_r, \alpha_i > 0. \tag{11}$$

Обозначим $c_i = h_i h_i^- = c_{i,1} c_{i,2}$. Элемент c_i принадлежит $M \cap N'_r$ и имеет следующее однозначное представление:

$$c_i = \prod_{k,l=1,\dots,r; k>l} [x_k, x_l]^{\gamma_{i,k,l}}, i = 1, \dots, r. \tag{12}$$

Выделим в этом представлении степень коммутатора $[x_p, x_q]$, полагая

$$c_i = [x_p, x_q]^{\gamma_{i,p,q}} \tilde{c}_i(p,q), i = 1, \dots, r, \tag{13}$$

где $\tilde{c}_i(p,q))$ не содержит в своей записи коммутатора $[x_p, x_q]$.

Покажем, что для фиксированной пары чисел $p, q; p > q$, можно построить новые элементы вида $h_i, h_i^- \in M, i = 1, \dots, r$, с указанными свойствами, для которых элементы $c_{i,1}, c_{i,2}$ из выражений (11), а значит, правые части выражений (12) и (13), не содержат множителя $[x_p, x_q]$. Для этого вначале получим два элемента из $M \cap N'_r$, в каноническом разложении которых по степеням коммутаторов типа (12) и (13) показатель степени при $[x_p, x_q]$ у одного элемента строго положителен, а у другого строго отрицателен.

Возьмем для определенности $p = 2, q = 1$, в других случаях рассуждения аналогичны. Для любого числа $\kappa \in \mathbb{N}$ имеем равенство

$$(h_2 h_2^-)^\kappa (h_1 h_1^-)^\kappa = c_2^\kappa c_1^\kappa = [x_2, x_1]^{\kappa(\gamma_{1,2,1} + \gamma_{2,2,1})} \tilde{c}_{2,1}(\kappa), \tag{14}$$

где $\tilde{c}_{2,1}(\kappa) = \tilde{c}_1(2,1)^\kappa \tilde{c}_2(2,1)^\kappa$ не содержит множителя $[x_2, x_1]$. Затем запишем левую часть равенства (14) в виде $(h_2^-)^\kappa h_2^\kappa h_1^\kappa (h_1^-)^\kappa$ и вычислим следующее выражение, полученное перестановкой h_2^κ и h_1^κ:

$$(h_2^-)^\kappa h_1^\kappa h_2^\kappa (h_1^-)^\kappa = [x_2, x_1]^{\kappa(\gamma_{1,2,1} + \gamma_{2,2,1}) - \kappa^2 \alpha_1 \alpha_2} \tilde{c}_{2,1}(\kappa). \tag{15}$$

Выражение $\kappa^2 \alpha_1 \alpha_2 > 0$ как функция от κ растет быстрее, чем $\kappa(\gamma_{1,2,1} + \gamma_{2,2,1})$, поэтому при достаточно больших значениях κ показатель при $[x_2, x_1]$ равенстве (15) будет отрицательным. Обозначим его через $-\nu, \nu > 0$.

Записав выражение левой части равенства (14) в виде $h_2^\kappa (h_2^-)^\kappa h_1^\kappa (h_1^-)^\kappa$, вычислим следующее выражение:

$$h_2^\kappa h_1^\kappa (h_2^-)^\kappa (h_1^-)^\kappa = [x_2, x_1]^{\kappa(\gamma_{1,2,1} + \gamma_{2,2,1}) + \kappa^2 \alpha_1 \alpha_2} \tilde{c}_{2,1}(\kappa). \tag{16}$$

Также, как и выше, показываем, что при достаточно больших значениях κ показатель степени коммутатора $[x_2, x_1]$ будет положительным. Обозначим его через μ. При этом, конечно, считаем, что κ выбрано достаточно большим, чтобы обеспечить оба условия на μ и ν.

Итак, подмоноид M содержит два элемента $d(\mu), d(\nu) \in N'_r$, в каноническую запись которых коммутатор $[x_2, x_1]$ входит в степени $\mu > 0$ и $-\nu\,(\nu > 0)$, соответственно.

Возьмем элемент $h_i = x_i^{\alpha_i}[x_2, x_1]^{\rho_i}\tilde{c}_i$, где $\tilde{c}_i$ не содержит в канонической записи коммутатора $[x_2, x_1]$. Рассмотрим его степень $h_i^{\mu\nu}$. Если $\rho_i = 0$, оставляем эту степень без изменений. Если $\rho_i > 0$, умножим эту степень на $d(\nu)^{\mu\rho_i}$. В результате получится элемент отличающийся от $x_i^{\alpha_i\mu\nu}$ на множитедь из N'_r, не содержащий в канонической записи $[x_2, x_1]$. Если $\rho_i < 0$, умножим данную степень на $d(\mu)^{\nu\rho_i}$, также исключая $[x_2, x_1]$. Аналогичные операции выполняем для элемента h_i^-. Для дальнейших вычислений используем вместо пары h_i, h_i^- полученную пару элементов.

Подобные преобразования проводим для любого $i = 1, \ldots, r$. В результате мы получаем новый набор элементов (для упрощения записи сохраняем для них первоначальные обозначения) $h_i, h_i^-, i = 1, \ldots, r, h_i = x_i^{\beta_i}c_{i,1}, h_i^- = x_i^{-\beta_i}c_{i,2}$, для которых канонические записи элементов $c_{i,1}, c_{i,2} \in N'_r$ не содержат степеней коммутатора $[x_2, x_1]$. Действуя аналогично с полученными элементами, мы последовательно исключаем подобным образом из записи степени других коммутаторов.

В результате получим пары взаимно обратных элементов моноида M вида $x_i^{\pm\xi_i}, \xi_i > 0$. Следовательно, коммутаторы $[x_i^{\xi_i}, x_j^{\xi_j}] = [x_i, x_j]^{\xi_i\xi_j}$ и обратные к ним принадлежат моноиду M. Подгруппа $T \leq M$, порожденная этими коммутаторами, имеет конечный индекс в N_r. Произвольный элемент принадлежит M тогда и только тогда, когда его образ принадлежит образу M в факторгруппе N_r/T. Эта фактор группа почти абелева. Действительно, если период фактор группы N_r/T равен t, то абелевой будет степень N_r^t. Из приведенных в разделе 2 результатов Эйленберга-Шютценберже и Грюншлага следует, что в N_r/T разрешима проблема вхождения в конечно порожденный подмоноид. Значит, проблема вхождения в M разрешима в N_r. Так как подмоноид M произволен, утверждение (2) теоремы доказано.

□

Заметим, что проблема вхождения в конечно порожденный подмоноид нильпотентной группы сводится к аналогичной проблеме для соответствующей свободной нильпотентной группы.

Замечание 1. *Пусть $N = N_{r,l}/R$ – конечно порожденная нильпотентная группа, $M =$ мон$(m_1, \ldots, m_k)$ – ее подмоноид. Возьмем набор $\{\tilde{m}_1, \ldots, \tilde{m}_k\}$ прообразов порождающих элементов моноида M в группе $N_{r,l}$. Нормальная подгруппа R группы $N_{r,l}$ конечно порождена, поэтому $R =$ гр$(r_1, \ldots, r_t)$ для некоторых элементов $r_i \in N_{r,l}$. Подмоноид $\tilde{M} = (\tilde{m}_1, \ldots, \tilde{m}_k, r_1^{\pm 1}, \ldots, r_t^{\pm 1})$ является полным прообразом M в $N_{r,l}$. Проблема вхождения в M для группы N очевидно равносильна проблеме вхождения в $\tilde{M}$ для группы $N_{r,l}$.*

Отсюда следует, что полученные в Теореме 4 достаточные условия разрешимости проблемы вхождения в подмоноид могут быть применены к произвольной конечно порожденной нильпотентной группе класса два.

References

[1] S. I. Adian, *Algorithmic unsolvability of problems of recognition of certain properties of groups*, Dokl. Akad. Nauk SSSR, **103**:4 (1955), 533–535. (In Russian).

[2] S.I. Adian, *Unsolvability of some algorithmic problems in the theory of groups*, Trudi Mosc. Mat. Obsc., **6**, GITTL, Moscow, 1957, 231–298. (In Russian).

[3] S.I. Adian, V.G. Durnev, *Decision problems for groups and semigroups*, Russian Math. Surveys, 2000, **55**:2 (2000), 207–296. *http* : *//www.mathnet.ru/php/archive.phtml?wshow* = *paper&jrnid* = *rm&paperid* = 267&$option_lang = eng$ http://dx.doi.org/10.1070/RM2000v055n02ABEH000267

[4] *Algorithmic Problems in Group Theory*, Dagstuhl Reports, **9**:3, 83–110. Ed-s: V. Diekert, O. Kharlampovich, M. Lohrey, and A. Myasnikov. Dagstuhl Reports. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany. *https* : *//drops.dagstuhl.de/opus/volltexte*/2019/11293/*pdf*/$dagrep_v009_i003_p083_19131.pdf$

[5] F. Bassino, I. Kapovich, M. Lohrey, A. Miasnikov, A. Nicaud, A. Nikolaev, I. Rivin, V. Shpilrain, A. Ushakov, and P. Weil, *Complexity and Randomness in Group Theory: GAGTA BOOK 1*, Walter de Gruyter GmbH, Berlin, Boston, 2020, 386 p. https://zh.art1lib.com/book/83551370/cb3430 DOI:10.1515/9783110667028-007

[6] G. Baumslag, F. B. Cannonito, and D. J. S. Robinson, *The algorithmic theory of finitely generated metabelian groups,* Trans. Amer. Math. Soc., **344**:2 (1994), 629–648.

[7] G Baumslag, F. B. Cannonito, D. J. S. Robinson, and D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra, **141** (1991), vol. 141, 118–149. https://www.semanticscholar.org/paper/The-algorithmic-theory-of-polycyclic-by-finite-Baumslag-Cannonito/7f77bdfa9684b669fd732557c5702e109a6644e4 DOI:10.1016/0021-8693(91)90221-S

[8] G. Baumslag, D. Gildenhuys, and R. Strebel, *Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. I,* J. Pure Appl. Algebra, **39** (1986), 53–94. https://www.sciencedirect.com/science/article/pii/0022404986901362 https://doi.org/10.1016/0022-4049(86)90136-2

[9] G. Baumslag, D. Gildenhuys, and R. Strebel, *Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. II,* J. Algebra, **97** (1985), 278–285. https://core.ac.uk/display/82545850 https://www.semanticscholar.org/paper/Algorithmically-insoluble-problems-about-finitely-Baumslag-Gildenhuys/2a9e7e22f1e6bd15941cefcba794309884f2c124 DOI:10.1016/0021-8693(85)90085-7

[10] M. Benois, *Parties rationnelles du groupe libre*, C. R. Acad. Sci. Paris, Ser. A, **269** (1969), 1181–1190. (In French).

[11] S. P. Boyd, L. Vandenberghe, *Convex Optimization*, Cambridge University Press, Cambridge, 2004, XIV + 716 p.

[12] T. Colcombet, J. Ouaknine, P. Semukhin, J. Worrell, *On Reachability Problems for Low-Dimensional Matrix Semigroups* In: 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019). Ed-s: C. Baier, I. Chatzigiannakis, P. Flocchini, and S. Leonardi; Article No. 44; pp. 44:1–44:15. Leibniz International Proc. in Informatics Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany.

[13] S. Eilenberg, M. P. Schutzenberger, *Rational sets in commutative monoids*, J. Algebra, **13** (1969), 173–191. https://www.sciencedirect.com/science/article/pii/0021869369900702

[14] E. Formanek, *Conjugacy separability in polycyclic groups*, J. Algebra, **42**:1 (1976), 1–10. *https* : *//www.academia.edu*/24492385/$Conjugate_separability_in_polycyclic_groups$

[15] R. H. Gilman, *Formal Languages and Infinite Groups, Geometric and computational perspectives on infinite groups*, In: DIMACS, Ser. Discrete Math. Theor. Comput. Sci. 25, Providence, 1996, 27–51.*https* : *//www.semanticscholar.org/paper/Formal* − *languages* − *and* − *infinite* − *groups* − *Gilman*/$c8d5773a482d4191573ddfa1909de4abd4546706$

[16] F. Grunewald, D. Segal, *The solubility of certain decision problems in arithmetic and algebra*, Bull. Amer. Math. Soc., **1**:6 (1979), 915–918. https://www.ams.org/journals/bull/1979-01-06/S0273-0979-1979-14692-5/S0273-0979-1979-14692-5.pdf

[17] F. Grunewald, D. Segal, *Some general algorithms. I. Arithmetic groups. II. Nilpotent groups*, Annals of Math., **112**:3 (1980), 531–583. https://www.jstor.org/stable/1971092

[18] Z. Grunschlag, *Algorithms in Geometric Group Theory*, PhD thesis, University of California at Berkley, 1999, XXI + 123 p. *https* : *//www.proquest.com/openview/*471829*b*4*c*11*c*22615*ed*26*d*212273932*a/*1?*pq* − *origsite* = *gscholar*&*cbl* = 18750&*diss* = *y*

[19] P. Hall, *Nilpotent groups*, Canad. Math. Cong. Summer Sem., University of Alberta, Vancouver, 1957. 12–30.

[20] M. Hall Jr., *The theory of groups*, Macmillan Company, New York, 1959, XIII + 434 p.

[21] O. G. Harlampovich, *A finitely presented solvable group with undecidable word problem,* Math. USSR-Izvestiya, **19**:1 (1982), 151–169. *https* : *//www.semanticscholar.org/paper/A* − *FINITELY* − *PRESENTED* − *SOLVABLE* − *GROUP* − *WITH* − *UNSOLVABLE* − *Harlampovi%C*4%8*D/c*024*dfca*620*d*55*fb*56*da*0*abb*0*e*5*e*78*b*2*fca*4*af*69

[22] R. Lipton, Y. Zalstein, *Word problems solvable in logspace*, J. Assoc. Comput. Math., **24** (1977), 522–526. https://dl.acm.org/doi/10.1145/322017.322031

[23] M. Lohrey, *The rational subset membership problem for groups: a survey*, In: Groups St Andrews 2013, Edited by C. M. Campbell, M. R. Quick, E. F. Robertson, C. M. Roney-Dougal, Publisher: Cambridge University Press, 2015, 368–389.

[24] M. Lohrey, B. Steinberg, *Tilings and submonoids of metabelian groups*, Theory of Computing Systems, **48**:2 (2011), 411–427. https://www.cambridge.org/core/books/abs/groups-st-andrews-2013/rational-subset-membership-problem-for-groups-a-survey/756D48B6B4D03FD52E9670A2D2A362DC

[25] J. Macdonald, A. Myasnikov, A. Nikolaev, and S. Vassileva, *Logspace and compressed-word computations in nilpotent groups*, arXiv: 1503.03888v1 [math. GR] 12 March 2015, 38 p. https://arxiv.org/abs/1503.03888

[26] J. Macdonald J., A. Miasnikov, and D. Ovchinnikov, *Low-complexity computations for nilpotent subgroup problems*, Int. J. Algebra and Comput., **29**:4 (2019), 639–661. https://www.worldscientific.com/doi/abs/10.1142/S021819671950019X

[27] Y. Matijasevic, J. Robinson, *Reduction of Diophantine equation to one in 13 unknowns*, Acta Arith., **27** (1975), 521–553. http://matwbn.icm.edu.pl/ksiazki/aa/aa27/aa27125.pdf

[28] Ch. F. Miller, III, *Decision Problems in Algebraic Classes of Groups (A Survey)*, Studies in Logic and the Foundations of Mathematics, **71** (1973), 507–523. https://www.sciencedirect.com/science/article/abs/pii/S0049237X08719177

[29] A. Myasnikov, V. Roman'kov, *On rationality of verbal subsets in a group*, Theory of Computing Systems, 2013. **52**:4 (2013), 587–598. http://www.scopus.com/inward/record.url?eid=2-s2.0-84876130837&partnerID=MN8TOARS DOI: 10.1007/s00224-012-9394-3

[30] A. Myasnikov, V. Shpilrain and A. Ushakov, *Group-based cryptography*, Advances courses in Math. CRM, Barselona. Birkhäuser Verlag, Basel-Berlin-New York, 2008. 183 p. https://link.springer.com/book/10.1007/978-3-7643-8827-0

[31] A. Myasnikov, V. Shpilrain and A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, Amer. Math. Soc. Surveys and Monographs, Amer. Math. Soc., Providence R.I., 2011. 385 p. https://www.ams.org/books/surv/177/surv177-endmatter.pdf

[32] M. Yu. Nedbay, *The rational subset membership problem for finitely generated abelian groups*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 3 (1999), 37–41. (In Russian). https://omsu.ru/vestnik/articles/y1999-i3/a037/article.html

[33] M. Yu. Nedbay, *The rational subset membership problem for free products of groups*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 2 (2000), 17–18. (In Russian).

[34] G. A. Noskov, *Conjugacy problem in metabelian groups,* Math. Notes, **31**:4 (1982), 252–258. https://link.springer.com/article/10.1007/BF01138933

[35] G. A. Noskov, V. N. Remeslennikov, and V. A. Roman'kov, *Infinite groups*, J. Soviet Math., **18**:5 (1982), 669–735. http://www.scopus.com/inward/record.url?eid=2-s2.0-34250230761&partnerID=MN8TOARS DOI: 10.1007/BF01091962

[36] P.S. Novikov, *On the algorithmic unsolbability of the word problem*, Dokl. Acad. Sci. USSR, **85**:4 (1952), 709–712. (In Russian).

[37] P.S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov., **44**, Acad. Sci. USSR, Moscow, 1955, 3–143. (In Russian).

[38] M. O. Rabin, *Recursive unsolvability of group theoretic problems*, Annals of Math. (2), **67** (1958), 172–194. https://www.jstor.org/stable/1969933

[39] V.N. Remeslennikov, *Conjugacy in polycyclic groups*, Algebra and Logic, **8**:6 (1969), 404–411. http://iitam.omsk.net.ru/ remesl/articles/polycyclicgroups.pdf

[40] V. N. Remeslennikov, V. A. Roman'kov, *Model-theoretic and algorithmic questions in group theory*, J. Soviet Math., **31**:3 (1985), 2887–2939. http://www.scopus.com/inward/record.url?eid=2-s2.0-0039812508&partnerID=MN8TOARS DOI: 10.1007/BF02106805

[41] N. S. Romanovskii, *Some algorithmic problems for solvable groups.* Algebra and Logic, **13**:1 (1974), 13–16. https://link.springer.com/article/10.1007/BF01462922?LI=true

[42] N. S. Romanovskii, *The occurrence problem for extensions of abelian groups by nilpotent groups,* Siberian Math. J., **21** (1980), 170–174. https://www.semanticscholar.org/paper/The-occurrence-problem-for-extensions-of-Abelian-by-Romanovskii/5ddbcb440afe8a58982f1e60f131e4e4e9dbd764

[43] V. A. Roman'kov, *Automorphisms of groups*, Acta Applicandae Mathematicae. An International Survey Journal of Applying Mathematics and Math. Appl., **29**:3 (1992), 241–280. http://www.scopus.com/inward/record.url?eid=2-s2.0-0011882049&partnerID=MN8TOARS DOI: 10.1007/BF00047221

[44] V. A. Roman'kov, *On the occurence problem for rational subsets of a group*, In: Combinatorial and computing methods in mathematics, Omsk State University, Omsk, 1999, 235–242.

[45] V. A. Roman'kov, *Rational Subsets in Groups*, Omsk State Univrersity, Omsk, 2014. 176 p. (In Russian).

[46] V. A. Roman'kov, *On algorithmic problems in group theory*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 2(84) (2017), 18–27. (In Russian). https://cyberleninka.ru/article/n/ob-algoritmicheskih-problemah-teorii-grupp

[47] V. A. Roman'kov, *Essays in algebra and cryptology. Solvable groups*, Omsk State University, Omsk, 2017, 268 p.

[48] V. A. Roman'kov, *Polycyclic, metabelian, or soluble of type $(FP)_\infty$ groups with Boolean algebra of rational sets and biautomatic soluble groups are virtually abelian*, Glasgow Mathematical Journal, **60**:1 (2018), 209–218. http://www.scopus.com/inward/record.url?eid=2-s2.0-85015015651&partnerID=MN8TOARS DOI: 10.1017/S0017089516000677

[49] V.A. Roman'kov, *Algebraic cryptology*, OmSU, Omsk, 2020. 261 p. (In Russian).

[50] V. A. Roman'kov, *Two problems for solvable and nilpotent groups.* Algebra and Logic, **59** (2021), 483–492. http://www.scopus.com/inward/record.url?eid=2-s2.0-85054964522&partnerID=MN8TOARS https://doi.org/10.1515/gcc-2018-0009

[51] V. A. Roman'kov, *Algorithmic theory of solvable groups*, Prikl. Diskr. Mat., **52** (2021), 16–64. http://www.mathnet.ru/links/0fe4641973a3622e9178f5cfcd783670/pdm736.pdf

[52] R.A. Sarkisjan, *Algorithmic questions for linear algebraic groups, I*, Math. USSR-Sbornik, 41:2 (1982), 149–189. *http : //www.mathnet.ru/php/archive.phtml?wshow = paper&jrnid = sm&paperid =* 2788*&option_lang = eng*

[53] R. A. Sarkisjan, *Algorithmic questions for linear algebraic groups, II*, Math. USSR-Sbornik, **41**:3(1982), 329–359. *http : //www.mathnet.ru/php/archive.phtml?wshow = paper&jrnid = sm&paperid =* 2803*&option_lang = eng*

[54] D. Segal, *Decidable properties of polycyclic groups,* Proc. London Math. Soc., **61** (1990), 497–528. *https : //citeseerx.ist.psu.edu/viewdoc/download?doi =* 10.1.1.137.5279*&rep = rep*1*&type = pdf*

[55] E. I. Timoshenko, *Algorithmic problems for metabelian groups,* Algebra and Logic, **12**:2 (1973), 132–137. https://link.springer.com/article/10.1007/BF02219297

[56] O. A, Yurak, *On the simultaneous reduction of elements of abelian groups to positive form*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 3 (2006), 18–19. (In Russian). https://cyberleninka.ru/article/n/ob-odnovremennom-privedenii-elementov-abelevyh-grupp-k-polozhitelnomu-vidu

[57] O. A, Yurak, *On the simultaneous reduction of elements of abelian groups to positive form, II*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 4 (2006), 7–8. (In Russian). https://cyberleninka.ru/article/n/ob-odnovremennom-privedenii-elementov-abelevyh-grupp-k-polozhitelnomu-vidu-ii

[58] O. A. Yurak, *Positive elements of the Heisenberg group*, Vestnik Omskogo universiteta = Herald of Omsk University, no. 2 (2008), 16–19. (In Russian). https://cyberleninka.ru/article/n/polozhitelnye-elementy-gruppy-geyzenberga

Vitalii Anatolievich Roman'kov
Sobolev Institute of Mathematics, Omsk Branch,
Pevtsov st., 13,
644099, Omsk, Russia
Email address: romankov48@mail.ru