S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 19, №1, стр. 387–403 (2022) УДК 512.54, 510.53

DOI 10.33048/semi.2022.19.034 MSC 20F10

POSITIVE ELEMENTS AND SUFFICIENT CONDITIONS FOR SOLVABILITY OF THE SUBMONOID MEMBERSHIP PROBLEM FOR NILPOTENT GROUPS OF CLASS TWO

V.A. ROMAN'KOV

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 at least 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 group with an unsolvable submonoid membership problem. In view of this result, finding sufficient conditions for the solvability of this problem for nilpotent groups of class two is an urgent problem.

ROMAN'KOV, V.A., POSITIVE ELEMENTS AND SUFFICIENT CONDITIONS FOR SOLVABILITY OF THE SUBMONOID MEMBERSHIP PROBLEM FOR NILPOTENT GROUPS OF CLASS TWO.

The work was carried out within the state assignment for Sobolev Institute of Mathematics SB RAS (project FWNF-2022-0003).

Received April, 14, 2022, published July, 6, 2022.

Keywords: nilpotent group, submonoid membership problem, rational set, positive elements, solvability.

1. Introduction

Over the past 20–25 years, a fruitful connection has emerged between group theory and computer science. Significant attention began to be paid to algorithms, their complexity and effectiveness. This paper provides a brief overview of this area of research. Attention is drawn to algorithmic problems related to rational subsets of groups which are a natural generalization of regular sets, that is, formal languages, directly related to the computer science. We consider the problem of membership in finitely generated submonoids of free nilpotent groups (the submonoid membership problem), which has attracted the attention of a number of researchers in recent years. 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 in work [51] 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 (see [23], problem 24) about the existence of a finitely generated nilpotent group with an unsolvable submonoid membership problem. Note that until recently, only one result in this problem area has been known: in article [12], its solvability for the Heisenberg group, that is, a free nilpotent group of class two of rank two, was proved. Even in this, in a certain sense, minimal case, the obtained algorithm is far from being trivial.

Algorithmic problems in groups represent a classic research topic for algebra, which has a topological origin and analogues. At the beginning of the last century, Max Dehn introduced the word problem (Does a given word over the generators represent the identity?), the conjugacy problem (Are two given group elements conjugate?) and the membership problem (Does a given element belong to a given finitely generated subgroup?), and Heinrich Tietze introduced the isomorphism problem (Does two given groups are isomorphic?). After more than forty years of research, a number of results have been obtained showing the unsolvability of these problems in the class of all finitely presented groups. P.S. Novikov [37], [38] proved the unsolvability of the word problem, which leads to the unsolvability of the conjugacy and membership problems. S.I. Adian [1], [2] proved the unsolvability of the isomorphism problem.

Over time, the range of algorithmic problems has been expended significantly. The problems were stated for specific classes of groups, for example, varieties. Completely new problems have arisen. Accordingly, the range of research was expanded. In the works by S.I. Adian [1], [2] and M. Rabin [39], algorithmic unrecognizability for all Markov properties was proved.

At the same time it turned out that classical algorithmic problems are solvable for some important classes of groups. For example, all of them turned out to be solvable for polycyclic groups, in particular, finitely generated nilpotent ones. The most difficult problems were conjugacy (for polycyclic groups) and isomorphism (for nilpotent and polycyclic groups). The first of them was solved by V.N. Remeslennikov [40] and independently by E. Formanek [14]. The second one was solved for the nilpotent case by F. Grunewald and D. Segal [16], [17] (also taking into account some conditions (subsequently established), by R.A. Sarkisjan [53], [54]); for the polycyclic case the proof was given by D. Segal [55].

In the class of finitely generated solvable groups, all the classical problems turned out to be unsolvable, starting from the word problem, the unsolvability of which was established by O.G. Kharlampovich [21]. The constructed examples have a solvability class at least three. The metabelian case is a special case, for which the Dehn problems are solvable. In the class of finitely generated metabelian groups, the solvability of the word problem was established by E.I. Timoshenko [56], the conjugacy problem by G.A. Noskov [35], the membership problems by N.S. Romanovskii [42], [43]. The solvability of the isomorphism problem is still an open question. Reviews of the well-known results for algorithmic group theory problems can be found in [3], [6], [7], [8], [9], [28], [36], [41], [47], [55]. See also the recent review by the author on the algorithmic theory of solvable groups [52].

Algorithmic problems have had a strong influence on the development of modern computer science. Since the 1960s, when interest in complexity problems increased, the problems of computational complexity of group-theoretic algorithms have been in the focus of attention of both mathematicians and computer scientists. Some ideas well-known in complexity theory have made it possible to obtain high-level results in algorithmic group theory. Previously, algorithmic problems of group theory were studied mainly from the point of view of their solvability. R. Lipton and Y. Zalstein [22] developed an algorithm with logarithmic time complexity to solve the word problem in finitely generated linear groups. It was the first result of its kind. In recent years, a number of results have been obtained on algorithms in the theory of groups with low time complexity (see, for example, [4], [25], [26]). These results have practical value. New connections between group theory and complexity theory have been established in automata theory, data compression, etc.

At present, even more attention is paid to algorithmic problems of group theory, since their unsolvability in some classes of noncommutative groups serves as the basis for schemes of algebraic cryptography, and the groups themselves serve as platforms for the implementation of these schemes and corresponding algorithms. Interest in the complexity of algorithms for solving such problems has increased significantly along with the possibilities of their practical application. Studies on [30], [31] and [50] are devoted to these issues.

This article deals with the submonoid membership problem (Does a given element belong to a given finitely generated submonoid?), which is the most important fragment of the more general rational subset membership problem (Does a given element belong to a given rational subset?). We give sufficient conditions for a submonoid of a free nilpotent group of the class two when the specified problem is algorithmically solvable. They are formulated using the language of positive sets of group elements (see definitions below). A criterion is obtained for reducing the set of elements of a free nilpotent group of the class two to a positive form, as well as a number of other auxiliary results having their own independent value.

The submonoid membership problem for a noncommutative group is currently considered as a transfer of the classical problem of integer linear programming, where the submonoid membership problem for a free abelian group is considered, to a noncommutative platform. A new direction of research has emerged and is developing, called noncommutative discrete optimization. The chapter "Discrete optimization in groups" in the book [5] is devoted to this research topic. In addition, special attention is paid to the class of finitely generated nilpotent groups, as the closest to the class of abelian groups.

The structure of the article is as follows. Section 2 provides a number of definitions and a brief overview of the results on the rational subset membership problem in groups. Section 3 contains statements about potentially positive elements of free abelian groups and free nilpotent groups of class two. Section 4 is devoted to the preparation for the formulation and proof of the main result, which is Theorem 4. Section 5 presents Theorem 4, which sets out sufficient conditions for the solvability of the submonoid membership problem for a free nilpotent group of class two.

Further in the article we use standard notation for the free abelian group A_r of rank r and the free nilpotent group $N_{r,l}$ of rank r of nilpotence class l. By $[x, y] = x^{-1}y^{-1}xy$ we denote the commutator of elements x, y of some group G, and G' denotes its derived subgroup. For $X \subseteq G$, the expression $\mathrm{gr}(X)$ denotes the subgroup, and $\mathrm{mon}(X)$ means the submonoid of the group G, generated by X. As usual, $\mathbb{Q}$ denotes the set of rational numbers, $\mathbb{Z}$ the set of integers, and $\mathbb{N}$ is the set of natural numbers.

For nonzero integers $t_1, \dots, t_k$ $\gcd(t_1, \dots, t_k)$ marks their greatest common divisor, and $\mathrm{lcm}(t_1, \dots, t_k)$ stands for the least common multiple. For a ring K by $\mathrm{M}_r(K)$ we denote the ring of $r \times r$ of matrices over K, and by $\mathrm{GL}_r(K)$ the corresponding group of all invertible matrices.

2. The rational subset membership problem

Now we will give some definitions. The class of rational subsets $\mathrm{Rat}(G)$ of the group G is the smallest class that includes all finite subsets of the group (including the empty one) closed by the union, multiplication, and Kleene operation of generating the submonoid K^* from the subset K. The notion of a rational subset of a group is a natural generalization of the classical notion of a regular subset of a free monoid. Note that an arbitrary subgroup H of a group G is rational if and only if it is finitely generated. Obviously, a finitely generated submonoid is a rational subset.

The analogue of Kleene theorem on defining regular subsets of a free monoid by finite automata is correct: a subset R of a group G is rational if and only if R is the output set of a finite automaton over G. For more information on definitions and basic properties of rational subsets in groups, see the monograph [46] or the article [15].

In general, the $\mathrm{Rat}(G)$ is not closed under intersection and complement. The results on characterisation of finitely generated groups G, where $\mathrm{Rat}(G)$ is a boolean algebra, that is, closed not only under the union operation, but also by intersection and complement, are given in [49] and [46]. The question of the rationality of verbal subsets of free groups is studied in [29].

Many authors have studied the rational subset membership problem for groups. In connection with this question, see the review article by M. Lohrey [23]. In his work, the author formulates problem 24 on existence of a finitely generated nilpotent group with an unsolvable the submonoid membership problem. This issue has been repeatedly raised in B. Steinberg's talks at numerous scientific seminars.

The author in [51] announced a negative solution to this problem (the full proof is currently in print). Specifically, he claimed that there exists a finitely generated submonoid M of a free nilpotent group $N_{r,2}$ of a sufficiently large rank r, for which the membership problem is algorithmically unsolvable. A set of generating elements of M is effectively constructed by a fixed Diophantine polynomial $D(\zeta_1, \ldots, \zeta_s)$, that defines the unsolvable family of Diophantine equations of the form $D(\zeta_1, \ldots, \zeta_s) = v, v \in \mathbb{Z}$, whose existence follows from the results of Y.V. Matiyasevich on unsolvability of Hilbert's 10th problem (see, for example, [27]). The parameter r depends on s and the form of the polynomial $D(\zeta_1, \ldots, \zeta_s)$. An effective class of elements $\{g(v), v \in \mathbb{Z}\}$ of the group $N_{r,2}$ such that $g(v) \in M$ if and only if the corresponding equation $D(\zeta_1, \ldots, \zeta_s) = v$ has a solution in integers, is presented. These results yield the announced unsolvability of the membership problem for submonoid M.

We present some well-known results on the rational subset membership problem for groups.

Positive results:

- M. Benois [10]. Every free group of finite rank has a solvable rational subset membership problem.
- S. Eilenberg, M.P. Schützenberger [13] (independent proof is in [32]). Every finitely generated abelian group has a solvable rational subset membership problem.
- Z. Grunschlag [18]. The solvability of the rational subset membership problem is preserved for finite extensions of groups.
- M.Yu. Nedbay [33]. The solvability of the rational subset membership problem is preserved for free products of groups.

Negative results:

- V.A. Roman'kov [45]. There exists a number r such that the free nilpotent group $N_{r,l}$ of class $l \geq 2$ has an unsolvable rational subset membership problem.
- M. Lohrey, B. Steinberg [24]. The free metabelian group M_2 of rank 2 contains a fixed finitely generaled submonoid with an unsolvable membership problem.

The proof in [45] is based on the unsolvability of Hilbert's 10th problem, and in [24] is based on the unsolvability of the combinatorial tiling problem. For other results on the rational subset membership problem for groups, see [23].

It is worth noting that the submonoid membership problem for a free abelian froup $A_r \simeq \mathbb{Z}^r$ is related to the following problem of integer linear programming.

For the given matrix $A \in \mathrm{M}_{m\times r}$ and the vector $b \in \mathbb{Z}^r$, define whether there exists a solution $x \in \mathbb{N}^m$ of the equation $xA = b$.

In the language of group theory, this is the submonoid membership problem for the group A_r generated by the rows of the matrix A. It is well known that this version of the problem of integer linear programming belongs to the class of NP-complete problems. The submonoid membership problem for groups is currently considered as a natural generalisation of the integer linear programming problem. An overview of the relevant results can be found in the book [5].

3. Subsets of potentially positive elements of the groups A_r and $N_{r,2}$

Definition 1. *Let $\mathcal{C}$ be a variety of groups. We denote by $F_r(\mathcal{C})$ a free group of rank r of this variety.*

- *For the fixed basis $X_r = \{x_1, \dots, x_r\}$ of the group $F_r(\mathcal{C})$, a nontrivial element $g \in F_r(\mathcal{C})$ is said to be positive, if it belongs to the submonoid $M = mon(X_r)$, generated by elements of the chosen basis X_r. In other words, if the element g can be written in the form of a word $g = g(x_1, \dots, x_r)$ in positive powers of elements of the basis X_r. A positive element g is strictly positive if its expression in the form of a reduced word contains all elements of the basis X_r.*
- *An element $g \in F_r(\mathcal{C})$ is called potentially positive, if it is positive in some basis X_r' of the group $F_r(\mathcal{C})$. In other words: if there exists an automorphism α of the group $F_r(\mathcal{C})$ such that the image $\alpha(g)$ is positive.*

The above definitions naturally extend to subsets of elements of the group $F_r(\mathcal{C})$.

Our next task is to provide criteria for the potential positivity of finite subsets in groups A_r and their completions $A_r^{\mathbb{Q}}$, as well as in groups $N_{r,2}$ for each $r \in \mathbb{N}$.

First, consider the group $A_r = \mathbb{Z}^r$ in additive notation. Suppose that $E_r = \{e_1, \dots, e_r\}$, where $e_1 = (1, 0, \dots, 0), \dots, e_r = (0, \dots, 0, 1)$ is a standard basis. The elements of the group A_r are integer vectors $a = (\alpha_1, \dots, \alpha_r)$. A vector a is positive (we write $a \geq 0$), if its coordinates satisfy the inequalities $\alpha_i \geq 0, i = 1, \dots, r$, and potentially positive if it is positive in some basis of the group A_r. Equivalently, if there exists an invertible linear transform (automorphism) μ of the group $\mathbb{Z}^r$, for which the image $\mu(a)$ is positive. That means that for the matrix $T = T(\alpha) \in \mathrm{GL}_r(\mathbb{Z})$ of the said transform, the inequality $aT \geq 0$ is fulfilled.

Suppose that $A_r^{\mathbb{Q}} = \mathbb{Q}^r$ denotes the standard completion of the group A_r to a vector space over $\mathbb{Q}$, and $A_r^{\mathbb{R}} = \mathbb{R}^r$ over $\mathbb{R}$, with the same base E_r. Thus, the inclusions $\mathbb{Z}^r \subseteq \mathbb{Q}^r \subseteq \mathbb{R}^r$ are fixed. Moreover, linearly independent sets of vectors from $\mathbb{Q}^r$ remain linearly independent over $\mathbb{R}$ in $\mathbb{R}^r$. The concepts of positivity and potential positivity of elements and subsets are naturally transferred to the groups $\mathbb{Q}^r$ and $\mathbb{R}^r$.

For further proofs of the theorems, we will need the following two lemmas.

Lemma 1. *Let V be a finite-dimensional vector space over $\mathbb{Q}$ with the basis $E_r = \{e_1, \dots, e_r\}$. Let B be a finite set of vectors whose fixed coordinate, for certainty, the last one, is non-negative. Suppose that B_0 are all vectors in B with a zero selected coordinate, and $B_{>0}$ with a positive one. Then we can move to a new basis $E_r' = \{e_1', \dots, e_r'\}$, for which $e_1' = e_1, \dots, e_{r-1}' = e_{r-1}$ and $e_r' = e_r - \sum_{i=1}^{r-1} \gamma_i e_i$, $\gamma_i > 0$, in which vectors from B_0 retain their coordinates, and all coordinates of vectors from $B_{>0}$ are strictly positive.*

Proof.

The statement concerning B_0 is trivial.

Suppose that $B_{>0} = \{b_1, \dots, b_k\}$, $b_i = (\alpha_{i,1}, \dots, \alpha_{i,r})$, $i = 1, \dots, k$. In the basis E_r', the vector $b_i \in B_{>0}$ has the following form:

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

By assumption, $\alpha_{i,r} > 0$. We choose γ_i for every $i = 1, \dots, k$ so that the inequalities $\alpha_{i,j} + \gamma_i \alpha_{i,r} > 0$ are fulfilled. Then the statement concerning $B_{>0}$ will be true. $\square$

Corollary 1. *Let B be a finite set of vectors of the space $\mathbb{Q}^r$ with a fixed basis E_r for which the fixed coordinate, say the last one, is positive. Then the basis transition* *described in Lemma 1 allows to obtain the basis E'_r, where all coordinates of vectors from B are strictly positive.*

Proof. The statement directly follows from Lemma 1. We only need to note that in its notation, $B = B_{>0}$. $\square$

Lemma 2. *Suppose that the system of equalities and inequalities*

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

where $\alpha_{i,j} \in \mathbb{Q}, \lambda \in \mathbb{R}$, has a solution in real numbers. Then it has a solution in rational numbers

Proof. Let $E_r = \{e_1, \ldots, e_r\}$ be the basis of the space $\mathbb{Q}^r$, which is also the basis of its natural completion $\mathbb{R}^r$. The coefficient vectors $b_i = (\alpha_{i,1}, \ldots, \alpha_{i,r}), i = 1, \ldots, k+l$, from (1) are considered as elements of the space $\mathbb{Q}^r$.

Let $v = (v_1, \ldots, v_r) \in \mathbb{R}^r$ be a solution of the system (1). After substituting x with v in equations and inequalities of the system (1), we obtain a set of equalities, which we write using the language of dot products:

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

where $\delta_j > 0, j = 1, \ldots, l$. We put $\delta = \min\{\delta_j : j = 1, \ldots, l\}$.

Suppose that $\alpha = \max\{|\alpha_{i,j}| : i = k+1, \ldots, k+l; j = 1, \ldots, r\}$. We take $\varepsilon > 0$ such that

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

If some vector $v' = (v'_1, \ldots, v'_r) \in \mathbb{Q}^r$ satisfies all equations of the system (1) and at the same time the inequalities $|v_i - v'_i| \leq \varepsilon$ are fulfilled, then v' is the required solution of the system (1). We move to the proof of existence of such vector.

Let $V = \mathrm{Lin}_{\mathbb{Q}}(\alpha_{1-k})$ be a subspace in $\mathbb{Q}^r$, generated by the vectors $\alpha_1, \ldots, \alpha_k$. Let $m = \dim(V)$ be its dimension. Then the orthogonal completion $V_{\mathbb{Q}}^{\perp}$ in $\mathbb{Q}^r$ has dimension $r - m$. We write its basis $\tilde{E}_{r-m} = \{\tilde{e}_1, \ldots, \tilde{e}_{r-m}\}$ through the basis E_r (if in the system (1) there are no equalities, then $\tilde{E}_r = E_r$):

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

The basis $\tilde{E}_{r-m}$ is also the basis of the orthogonal completion $V_{\mathbb{R}}^{\perp}$ in $\mathbb{R}^r$.

We have the decomposition

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

From equalities (4) and (5), we obtain the equalities

$$\begin{cases} v_1 = \sum_{i=1}^{r-m} \tilde{v}_i \gamma_{i,1} \\ \dots \\ v_r = \sum_{i=1}^{r-m} \tilde{v}_i \gamma_{i,r} \end{cases}. \tag{6}$$

Suppose that $\gamma = \max\{|\gamma_{i,j}| : i = 1, \dots, r-m; j = 1, \dots, r\}$. We take $\varepsilon' > 0$ such that

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

where the parameter ε is the one featured in the inequality (3). We choose the values $\tilde{v}'_i \in \mathbb{Q}$ such that $|\tilde{v}_i - \tilde{v}'_i| \leq \varepsilon'$. We define the set $v' = (v'_1, \dots, v'_r) \in \mathbb{Q}^r$, where $v'_i = \sum_{j=1}^{r-m} \tilde{v}'_j \gamma_{i,j}$, $i = 1, \dots, r$. The inequality (7) yields

$$|v_i - v'_i| \leq \varepsilon.$$

Then v' is the solution of the system (1). □

Definition 2. *A subset $B = \{b_1, \dots, b_s\}$ of the group A_r or the group $A_r^{\mathbb{Q}}$ is said to be positively independent, if the equality $\sum_{i=1}^{s} \alpha_i b_i = 0$ for $\alpha_i \in \mathbb{Q}, \alpha_i \geq 0, i = 1, \dots, s$, yields the equalities $\alpha_i = 0, i = 1, \dots, s$.*

Otherwise, B is said to be positively dependent.

The following theorem is proved in [57]. Unfortunately, there is a significant gap in its proof. Therefore, we provide a new proof that eliminates the mentioned gap and other inaccuracies.

Theorem 1. *A subset of elements $B = \{b_1, \dots, b_s\}$ of the group $A_r^{\mathbb{Q}} \simeq \mathbb{Q}^r$ is potentially positive if and only if B is positively independent. Moreover, for every positively independent subset B there exists a basis of the space $\mathbb{Q}^r$, where all coordinates of vectors from B are strictly positive.*

Proof. Obviously, every positively dependent subset B is not potentially positive.

Let B be a positively independent set written in the basis $E_r = \{e_1, \dots, e_r\}$ of the space $\mathbb{Q}^r$: $b_i = (\alpha_{i,1}, \dots, \alpha_{i,r})$, $i = 1, \dots, s$. As before, we assume that E_r is the basis of the space $\mathbb{R}^r$. We use induction by r. The statement is obvious when $r = 1$ and s is arbitrary, since every system containing at least two oppositely directed vectors is positively linearly dependent, and a system of vectors with same directions is either positive or becomes such when substituting the basis vector with the opposite one. Suppose that the statement of the theorem is true for every space $\mathbb{Q}^n$ of dimension $n < r$.

Consider the cone

$$C = C(b_1, ..., b_s) = \{\sum_{i=1}^{s} \alpha_i b_i, \alpha_i \in \mathbb{Q}, \alpha_i \geq 0, i = 1, \dots, s\},$$

generated by the vectors from B. The subsets $C, -C, C \setminus \{0\}, -C \setminus \{0\}$ are convex. In the considered case, the subsets $C \setminus \{0\}, -C \setminus \{0\}$ do not intersect. We assume the space $\mathbb{Q}^r$ for every n to be naturally embedded into the euclidean space $\mathbb{R}^r$. We denote by $C^{\mathbb{R}}$ the convex hull of the cone C in $\mathbb{R}^r$. Obviously, the sets $C^{\mathbb{R}} \setminus \{0\}$ and $-C^{\mathbb{R}} \setminus \{0\}$ do not intersect as well.

We use the following version of Minkowski's theorem on hyperplane separation convex sets (see, for example, the study [11], p. 46). Let U and W be non-intersecting convex subsets of the space $\mathbb{R}^n$. Then there exists a nonzero vector v and a real number λ such that $\langle x, v\rangle \geq \lambda$ for every $x \in U$ and $\langle y, v\rangle \leq \lambda$ for every $y \in W$; that is, the hyperplane $\langle \cdot, v\rangle = \lambda$, for which v is the normal vector, separates U and W.

Therefore, there exists a hyperplane $H^{\mathbb{R}}$ of the space $\mathbb{R}^r$ separates $U = C^{\mathbb{R}} \setminus \{0\}$ and $W = -C^{\mathbb{R}} \setminus \{0\}$. All vectors from B split into two subsets: B_0 contains the vectors belonging to H, and $B_{>0}$ contains the ones that do not belong to H.

Suppose that $B_0 = \{b_1, \dots, b_k\}$, $B_{>0} = \{b_{k+1}, \dots, b_{k+l}, k + l = s\}$. Then v is the solution of the system (1).

By Lemma 2, the system (1) has the solution $v' \in \mathbb{Q}^r$. We define the hyperplane H' of the space $\mathbb{Q}^r$ with the normal v'. We choose in H' the basis

$$E'_{r-1} = \{e'_1, \dots, e'_{r-1}\},$$

where the vectors $b_1, \dots, b_k$ have strictly positive coordinates. We extend E'_{r-1} to the basis E'_r of the entire space $\mathbb{Q}^r$ with the vector $e'_r = v'$. Note that the last coordinates of vectors from $B = B_{>0}$ in this basis are strictly positive. Then by Corollary 1, there exists a basis E''_r of the space $\mathbb{Q}^r$, in which all the coordinates of every vector from $B_{>0}$ are strictly positive.

It remains to note that the first coordinates of all vectors from B in the basis E''_r are now strictly positive. By Corollary 1, there exists a basis E'''_r of the space $\mathbb{Q}^r$, where all the coordinates of vectors from B are strictly positive. □

The following theorem is established in [58], where its proof is based on work [57], which has a gap.

Theorem 2. *A subset of non-trivial elements $B = \{b_1, \dots, b_s\}$ of the group $A_r = \mathbb{Z}^r$ is potentially positive if and only if it is positively independent. For every positively independent subset B, there exists a basis of the space $\mathbb{Q}^r$, in which all coordinates of vectors from B are strictly positive.*

Proof. Obviously, the positively dependent subset B is not potentially positive.

Let $B = \{b_i = (\beta_{i,1}, \dots, \beta_{i,r}), i = 1, \dots, s\}$ be a subset of positively independent vectors of the group $\mathbb{Z}^r \subseteq \mathbb{Q}^r$. By Theorem 1, there exists a matrix $T \in \mathrm{GL}_r(\mathbb{Q})$ such that $c_i = b_i T = (\gamma_{i,1}, \dots, \gamma_{i,r})$ is a vector with strictly positive coordinates for every $i = 1, \dots, s$.

Suppose that $T = \nu^{-1} T_1$, where $\nu \in \mathbb{N}$ and $T_1 \in \mathrm{M}_r(\mathbb{Z})$. Let

$$t_1 = (\tau_{1,1}, \dots, \tau_{r,1})^{\mathtt{t}}$$

be the first column of the matrix T_1 ($\mathtt{t}$ denotes the transpose).

Let $\delta = \gcd(\tau_{1,1}, \dots, \tau_{r,1})$. Then the column $\tilde{t}_1 = \delta^{-1} t_1$ is primitive, that is, all its coordinates are coprime as a whole, and for every i, we have $b_i \tilde{t}_1 = \lambda_i > 0$.

It is well known (see, for example, [34], Theorem II.I, page 13), that every integer primitive column, in our case $\tilde{t}_1$, can be complemented to the integer invertible matrix $\widetilde{T} \in \mathrm{GL}_r(\mathbb{Z})$.

Suppose that $b_1 \widetilde{T} = (\mu_{1,1}, \dots, \mu_{1,r})$. If for some j, the inequality $\mu_{1,j} \leq 0$ is fulfilled, we change the matrix $\widetilde{T}$, adding to the j-th column the 1-th column, multiplied by a sufficiently large natural number δ_j, for which $\delta_j \mu_{1,1} + \mu_{1,j} > 0$. Such operation is performed for all coordinates of the vector b_1 which are not strictly positive. We obtain for the new matrix $\widetilde{T}$ the vector $b_1\widetilde{T}$ with strictly positive coordinates.

Since for every $i = 2, \ldots, r$ the first coordinate of the vector $b_i\widetilde{T}$ is positive, similar operations can be applied to achieve strong positivity of coordinates of all vectors $b_i\widetilde{T}$ for the altered matrix $\widetilde{T}$. After all changes, we obtain the matrix which we denote by T'. Obviously, $T' \in \mathrm{GL}_r(\mathbb{Z})$. Moreover, the vectors b_iT' have strictly positive coordinates for all $i = 1, ..., s$. That means that the vectors $b_1, ..., b_s$ are brought to a strictly positive form. □

Let $N_r = N_{r,2}, r \geq 2$, be a free nilpotent group with the basis $\{x_1, ..., x_r\}$ and $A_r = N_r/N_r'$ be a free abelian group with the basis $\{a_1, \ldots, a_r\}$, where $a_i = \bar{x}_i = x_iN_r'$. Here for every element $g \in N_r$ by $\bar{g}$ we denote an image g with respect to the standard homomorphism $N_r \to A_r$. We use a similar notation $\bar{U}$ for the subsets $U \subseteq N_r$.

The following theorem for the case $r = 2$ (that is, for the Heisenberg group) is proved in [59].

Theorem 3. *A subset of non-trivial elements $U = \{u_1, ..., u_s\}$ of the group N_r is potentially positive if and only if the subset $\bar{U} = \{\bar{u}_1, ..., \bar{u}_s\}$ is positively independent in A_r.*

Proof. Obviously, if $\bar{U}$ is positively dependent in A_r, then by Theorem 2 this subset is not potentially positive in A_r. Then U is not potentially positive in N_r.

Let the subset $\bar{U}$ be positively independent in A_r. Since every automorphism of the group A_r is induced by an automorphism of the group N_r (see, for example, the review [44] or the study [48]), then by Theorem 2 we can assume that $\bar{U}$ is strictly positive in A_r. Then every element $u_i \in U$ is written in the form

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

We order the commutators of elements of the basis of the group N_r in the following way: we set $[x_i, x_j] > [x_p, x_q]$, if $i > p$, or $i = p$ and $j > q$. Note that the representation in which the commutators are written according to the ordering is unique.

To find the positive representation of the subset U, we exclude from formula (8) the powers of commutators. Moreover, the powers of elements of the basis are encountered a number of times. We act as follows. We choose a natural number $\tau_{2,1} > \max\{|\mu_{i,2,1}| : i = 1, \ldots, s\}$ and define the automorphism $\varphi_{2,1} : x_1 \mapsto x_2^{\tau_{2,1}} x_1 x_2^{\tau_{2,1}}, x_i \mapsto x_i$ for $i \geq 2$.

Then for $i = 1, \ldots, s$ the equality of the following form is true:

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

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

For every expression $\varphi_{2,1}(u_i)$, we substitute exactly one of subwords of the form $x_2^{\tau_{2,1}} x_1 x_2^{\tau_{2,1}}$ with $x_2^{\tau_{2,1}+\mu_{i,2,1}} x_1 x_2^{\tau_{2,1}-\mu_{i,2,1}} [x_2, x_1]^{-\mu_{i,2,1}}$. The powers of the commutator $[x_2, x_1]$ are reduced. The powers of the basis elements remain positive.

Similarly, applying consistently the automorphisms

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

where

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

for $k \neq i$ for significantly large corresponding values $\tau_{i,j}$, step by step we delete the changing powers of the commutators

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

from the right-hand sides of the obtained equalities

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

Note that at each following step, only the powers of the commutators of higher order than the one of the deleted commutator are changed. The commutators deleted before do not reappear. After performing all of such transformations, as a result we obtain a positive word. □

Remark 1. *Checking whether the condition of potential positivity of a finite set of vectors of the group A_r is satisfied can be performed algorithmically. To do this, all the bases of the group and all possible nonzero sets of non-negative coefficients are ordered for the vectors under study. Then the processes of rewriting the tested vectors in the bases and calculating positive linear combinations with successive sets of coefficients are performed sequentially. At the final step, we either obtain the positive expression of the vectors, or their positive dependence, that shows, according to Theorem 2, that they are not potentially positive.*

4. Preliminary considerations

Let $N_r = N_{r,2}$ be a free nilpotent group of rank r of nilpotency class 2 with the basis $X_r = \{x_1, \dots, x_r\}$, $A_r = N_r/N_r'$ be a free abelian group of rank r. Every basis of the group N_r induces the basis of the group A_r. The converse is also true: a preimage of every basis of the group A_r is basis of N_r. Therefore, every automorphism of A_r is induced by an automorphism of the group N_r. The derived subgroup N_r' is a free abelian central subgroup of N_r, for whose basis we can take the set $\{[x_i, x_j] : i > j; i, j = 1, \dots, r\}$ In every finitely generated nilpotent group, in particular, in the group N_r, the word problem is solvable. Also, the membership problem is solvable, moreover, we can effectively write an element of the subgroup as a group word over its generating elements. For these and other facts, see, for example, [19], [20]. In what follows, they are almost always used without reference.

Let M be a finitely generated submonoid of the group N_r, defined by a finite set of non-trivial generating elements $Y \cup U$, where Y is a subset of elements with non-trivial images in A_r, and U is a subset of elements from N_r'. Among all elements from Y, we choose the maximal subset with respect to inclusion $G = \{g_1, \dots, g_k\}$, whose image in A_r is positively independent. We put $F = Y \setminus G = \{f_1, \dots, f_l\}$.

By Theorem 2, we assume that the basis X_r of the group N_r is chosen in a way that in the induced basis $\bar{X}_r$ of the group A_r, the images of elements from G are strictly positive. Since $\bar{G}$ is the maximal positively independent subset, every subset of the form $\bar{G} \cup \{\bar{f}_j\}$ for $j = 1, \dots, l$ is positively dependent. This means the existence of non-negative integers $\alpha_{i.j}, i = 1, \dots, k, \beta_j \neq 0$ such that

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

Hence, every element $\bar{f}_j$ is strictly negative, that is, all coefficients with respect to the basis E_r are strictly less than zero.

We put $M_1 = \mathrm{mon}(\bar{G})$, $M_2 = \mathrm{mon}(\bar{F})$. The submonoid $\bar{M}_G = \mathrm{mon}(\bar{G})$ consists of positive elements, and $\bar{M}_F = \mathrm{mon}(\bar{F})$ of negative ones.

In the following discussion, the basis of the group N_r may change and the generating elements of the monoid M from G and F may not retain these properties, so we will refer to them as originally positive or negative elements.

If $G = \emptyset$, then $F = \emptyset$. In this case, the membership problem for the submonoid $M \leq N_2'$ is solvable by the Eilenberg—Schutzenberger theorem provided in Section 2. Therefore, we assume that $G \neq \emptyset$.

We assume that β_j is the minimal number for which $\bar{f}_j^{-\beta_j} \in \bar{M}_G$, $j = 1, \dots, l$. Suppose that $\beta = \mathrm{lcm}(\beta_j : j = 1, \dots, l)$. Then for every element $\bar{f} \in \bar{M}_F$, the element $\bar{f}^{-\beta}$ belongs to $\bar{M}_G$. That is, the element inverse to $\bar{f}^{\beta}$ belongs to $\bar{M}_G$.

Let $\bar{H}$ denote the submonoid of the group A_r, consisting of all invertible elements of the monoid $\bar{M}$. Then $\bar{H}$ is a subgroup of the group A_r. We should emphasise that by construction every element from $\bar{H}$ has a preimage in M. Let $\widetilde{H}$ be a full preimage of the subgroup $\bar{H}$ in M. For every element $h \in \widetilde{H}$, there exists an commuting element $h^- \in \widetilde{H}$ such that $hh^- \in N_r' \cap M$, that is, $\bar{h}\bar{h}^- = 1$. The element h^- is not uniquely defined. Every preimage of the element $\bar{h}^{-1}$ in $\widetilde{H}$ may be that element.

Let $I(\bar{F})$ denote a subgroup of the group A_r, consisting of all elements of the group A_r, linearly dependent with the elements from $\bar{F}$. In other words, $I(\bar{F})$ is an isolator of the subgroup $\mathrm{gr}(\bar{F})$ in the group A_r. The subgroup $\bar{H}$ belongs to $I(\bar{F})$ and has a finite index in it. This follows from the fact that every element from $\bar{F}$ to some nonzero power gets into $\bar{H}$, and from that every subgroup from A_r is finitely generated.

5. Main result

We present a number of sufficient conditions for generating elements of the submonoid M under which the membership problem for M is algorithmically solvable. We use the concepts and notations introduced in the previous section.

Theorem 4. *The membership problem for the submonoid M in the group N_r is algorithmically solvable in the following cases:*

(1) *When the finite set of generating elements of the submonoid M consists of the set of elements G, whose images are potentially positive in A_r, and the set U of elements from N_r'. In other words, when $F = \emptyset$.*
(2) *When the isolator $I(\bar{F})$ of the subgroup generated by $\bar{F}$, coincides with A_r.*

Proof. By Theorem 2, we choose basis X_r of the group N_r such that the images of elements from G are strictly positive in A_r with respect to the induced basis $\bar{X}_r$.

Then for the element $h \in N_r$, the set of semigroup words of the form

$$g_{i_1} \dots g_{i_q}; g_{i_t} \in G$$

such that $h = g_{i_1} \dots g_{i_q} w, w \in N_r'$, is finite. For each one of them, we check the membership of w in $\mathrm{mon}(U)$. The element h belongs to M if and only if at least one such membership takes place. Statement (1) is proved.

By condition of the theorem, the isolator $I(\bar{F})$ coincides with A_r, therefore, the subgroup $\bar{H}$ has a finite index in A_r. For every basis element x_i, there exists a pair of commuting elements of the full preimage $\widetilde{H}$ of the subgroup $\bar{H}$ in M of the form

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

We denote $c_i = h_i h_i^- = c_{i,1} c_{i,2}$. The element c_i belongs to $M \cap N_r'$ and has the following unique representation:

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

We choose in this representation the power of the commutator $[x_p, x_q]$, setting

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

where $\tilde{c}_i(p,q)$ does not contain the commutator $[x_p, x_q]$ in its record.

We will show that for the fixed pair of numbers p, q; $p > q$, we can construct the new elements of the form $h_i, h_i^- \in M, i = 1, \dots, r$, with the mentioned properties for which the elements $c_{i,1}, c_{i,2}$ belong to the expressions (11), and therefore, the right-hand sides of the expressions (12) and (13) do not contain the multiplier $[x_p, x_q]$. To do that, first we obtain two elements from $M \cap N_r'$, in whose canonical decomposition by powers of commutators of the types (12) and (13), the power of $[x_p, x_q]$ for one of the elements is strictly positive and for the other is strictly negative.

We take for definiteness $p = 2, q = 1$, in other cases the reasoning is similar. For every number $\kappa \in \mathbb{N}$, we have the equality

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

where $\tilde{c}_{2,1}(\kappa) = \tilde{c}_1(2,1)^\kappa \tilde{c}_2(2,1)^\kappa$ does not contain the multiplier $[x_2, x_1]$. Then, we write the left-hand side of the equality (14) in the form $(h_2^-)^\kappa h_2^\kappa h_1^\kappa (h_1^-)^\kappa$ and calculate the following expression obtained by transposition of h_2^κ and h_1^κ:

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

The expression $\kappa^2 \alpha_1 \alpha_2 > 0$ as a function in κ grows faster than $\kappa(\gamma_{1,2,1} + \gamma_{2,2,1})$, hence, given significantly large values of κ, the power of $[x_2, x_1]$ in the equation (15) is negative. We denote it by $-\nu, \nu > 0$.

Writing the expression from the left-hand side of the equality (14) in the form $h_2^\kappa (h_2^-)^\kappa h_1^\kappa (h_1^-)^\kappa$, we calculate the following expression:

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

Same as above, we show that given sufficiently large values of κ, the power of the commutator $[x_2, x_1]$ is positive. We denote it by μ. With that, of course, we assume that κ is chosen large enough to fulfill both conditions for μ and ν.

Hence, the submonoid M contains two elements $d(\mu), d(\nu) \in N_r'$, in whose canonical expression, the commutator $[x_2, x_1]$ has powers $\mu > 0$ and $-\nu\,(\nu > 0)$, respectively.

We take the element $h_i = x_i^{\alpha_i} [x_2, x_1]^{\rho_i} \tilde{c}_i$, where $\tilde{c}_i$ does not contain in the canonical expression the commutator $[x_2, x_1]$. We consider its power $h_i^{\mu\nu}$. If $\rho_i = 0$, we leave this power unaltered. If $\rho_i > 0$, we multiply this power by $d(\nu)^{\mu\rho_i}$. As a result, we obtain an element differing from $x_i^{\alpha_i\mu\nu}$ by the multiplier from N'_r, which does not contain $[x_2, x_1]$ in the canonical expression. If $\rho_i < 0$, we multiply this power by $d(\mu)^{\nu\rho_i}$, also excluding $[x_2, x_1]$. We perform the similar operations for the element h_i^-. For further calculations, we use the obtained pair of elements instead of the pair h_i, h_i^-.

We perform such transformations for every $i = 1, \dots, r$. As a result, we obtain a new set of elements (to simplify the record, we keep their original notation) $h_i, h_i^-, i = 1, \dots, r$, $h_i = x_i^{\beta_i} c_{i,1}, h_i^- = x_i^{-\beta_i} c_{i,2}$, for which the canonical expressions of the elements $c_{i,1}, c_{i,2} \in N'_r$ do not contain the powers of the commutator $[x_2, x_1]$. Acting similarly with the obtained elements, we consistently exclude from the record the powers of other commutators in a similar way.

As a result, we obtain the pairs of mutually inverse elements of the monoid M of the form $x_i^{\pm\xi_i}, \xi_i > 0$. Therefore, the commutators $[x_i^{\xi_i}, x_j^{\xi_j}] = [x_i, x_j]^{\xi_i\xi_j}$ and the inverse ones belongs to the monoid M. The subgroup $T \leq M$, generated by these commutators has a finite index in N_r. An arbitrary element belongs to M if and only if its image belong to the image M in the quotient group N_r/T. This quotient group is almost an abelian one. Indeed, if the exponent of the quotient group N_r/T equals t, then the power N_r^t is abelian. The results by Eilenberg—Schutzenberger and Grunschlag, provided in Section 2, yield that in N_r/T the membership problem for finitely generated submonoid is solvable. Therefore, the membership problem for M is solvable in N_r. Since the submonoid M is arbitrary, the statement (2) of the theorem is proved. □

Note that the submonoid membership problem for a finitely generated nilpotent group is reduced to the similar problem for the corresponding free nilpotent group.

Remark 2. *Let $N = N_{r,l}/R$ be a finitely generated nilpotent group,*

$$M = mon(m_1, \dots, m_k)$$

be its submonoid. We take the set $\{\tilde{m}_1, \dots, \tilde{m}_k\}$ of preimages of generating elements of the monoid M in the group $N_{r,l}$. The normal subgroup R of the group $N_{r,l}$ is finitely generated, therefore, $R = gr(r_1, \dots, r_t)$ for some elements $r_i \in N_{r,l}$. The submonoid $\tilde{M} = (\tilde{m}_1, \dots, \tilde{m}_k, r_1^{\pm 1}, \dots, r_t^{\pm 1})$ is a complete preimage M in $N_{r,l}$. The membership problem for M for the group N is obviously equivalent to the membership problem for $\tilde{M}$ for the group $N_{r,l}$.

This means that the sufficient conditions for the solvability of the submonoid membership problem obtained in Theorem 4, can be applied to an arbitrary finitely generated nilpotent group of class two.

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. Zbl 0065.00901

[2] S.I. Adian, *Unsolvability of some algorithmic problems in the theory of groups*, Tr. Mosk. Mat. Obshch., **6** (1957), 231–298. Zbl 0080.24101

[3] S.I. Adian, V.G. Durnev, *Decision problems for groups and semigroups*, Russ. Math. Surv., **55**:2 (2000), 207–296. Zbl 0958.20029

[4] V. Diekert, O. Kharlampovich, M. Lohrey, A. Myasnikov, *Algorithmic problems in group theory (Dagstuhl Seminar 19131)*, Dagstuhl Reports, **9**:3 (2019), 83пїS110.

[5] F. Bassino, I. Kapovich, M. Lohrey, A. Miasnikov, C. Nicaud, A. Nikolaev, I. Rivin, V. 7205680, A. Ushakov, P. Weil, *Complexity and randomness in group theory. GAGTA book 1*, de Gruyter, Berlin, 2020. Zbl 7205680

[6] G. Baumslag, F.B. Cannonito, D.J.S. Robinson, *The algorithmic theory of finitely generated metabelian groups,* Trans. Am. Math. Soc., **344**:2 (1994), 629–648. Zbl 0821.20019

[7] G. Baumslag, F.B. Cannonito, D.J.S. Robinson, D. Segal, *The algorithmic theory of polycyclic-by-finite groups,* J. Algebra, **141**:1 (1991), 118–149. Zbl 0774.20019

[8] G. Baumslag, D. Gildenhuys, R. Strebel, *Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. I,* J. Pure Appl. Algebra, **39** (1986), 53–94. Zbl 0577.20021

[9] G. Baumslag, D. Gildenhuys, R. Strebel, *Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras. II,* J. Algebra, **97** (1985), 278–285. Zbl 0579.20031

[10] M. Benois, *Parties rationnelles du groupe libre*, C. R. Acad. Sci. Paris, Sér. A, **269** (1969), 1188–1190. Zbl 0214.03903

[11] S.P. Boyd, L. Vandenberghe, *Convex optimization*, Cambridge University Press, Cambridge, 2004. Zbl 1058.90049

[12] T. Colcombet, J. Ouaknine, P. Semukhin, J. Worrell, *On reachability problems for low dimensional matrix semigroups* In: C. Baier (ed.) et al., *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, LIPIcs, **132**, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, 2019, 44:1–44:15.

[13] S. Eilenberg, M.P. Schützenberger, *Rational sets in commutative monoids*, J. Algebra, **13**, (1969), 173–191. Zbl 0206.02703

[14] E. Formanek, *Conjugacy separability in polycyclic groups*, J. Algebra, **42**:1, (1976), 1–10. Zbl 0345.20031

[15] R.H. Gilman, *Formal languages and infinite groups*, In Baumslag, Gilbert (ed.) et al., *Geometric and computational perspectives on infinite groups. Proceedings of a joint DIMACS/Geometry Center workshop, January 3-14, 1994 at the University of Minnesota, Minneapolis, MN, USA and March 17-20, 1994 at DIMACS, Princeton, NJ, USA*, DIMACS, Ser. Discrete Math. Theor. Comput. Sci., **25**, AMS, Providence, 1996, 27–51. Zbl 0851.20030

[16] F. Grunewald, D. Segal, *The solubility of certain decision problems in arithmetic and algebra*, Bull. Am. Math. Soc., New Ser., **1**:6 (1979), 915–918. Zbl 0431.20029

[17] F. Grunewald, D. Segal, *Some general algorithms. I: Arithmetic groups*; *Some general algorithms. II: Nilpotent groups*, Ann. Math. (2), **112**:3 (1980), 531–583; 585–617. Zbl 0457.20047; Zbl 0457.20048

[18] Z. Grunschlag, *Algorithms in geometric group theory*, PhD thesis, University of California at Berkley, 1999.

[19] P. Hall, *Nilpotent groups. Notes of lectures given at the Canadian Mathematical Congress, summer seminar, University of Alberta, Edmonton, 12-30 August, 1957*, Queen Mary College (University of London), London, 1969. Zbl 0211.34201

[20] M. Hall jun., *The theory of groups*, The Macmillan Company, New York, 1959. Zbl 0084.02202

[21] O.G. Harlampovich, *A finitely presented solvable group with undecidable word problem,* Math. USSR-Izvestiya, **19**:1 (1982), 151–169. MR0631441

[22] R. Lipton, Y. Zalstein, *Word problems solvable in logspace*, J. Assoc. Comput. Math., **24** (1977), 522–526. Zbl 0359.68049

[23] M. Lohrey, *The rational subset membership problem for groups: a survey*, In Campbell, C.M. (ed.) et al., *Groups St Andrews 2013. Selected papers of the conference, St. Andrews, UK, August 3nïS11, 2013*, London Mathematical Society Lecture Note Series, **422**, Cambridge University Press, 2015, 368–389, Zbl 1346.20043

[24] M. Lohrey, B. Steinberg, *Tilings and submonoids of metabelian groups*, Theory Comput. Syst., **48**:2 (2011), 411–427. Zbl 1229.20025

[25] J. Macdonald, A. Myasnikov, A. Nikolaev, S. Vassileva, *Logspace and compressed-word computations in nilpotent groups*, arXiv: 1503.03888v3

[26] J. Macdonald, A. Miasnikov, D. Ovchinnikov, *Low-complexity computations for nilpotent subgroup problems*, Int. J. Algebra Comput., **29**:4 (2019), 639–661. Zbl 7079848

[27] Y. Matijasevic, J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arith., **27** (1975), 521–553. Zbl 0279.10019

[28] Ch.F. III Miller, *Decision problems in algebraic classes of groups (a survey)*, Studies Logic Foundations Math., **71** (1973), 507–523. Zbl 0288.20052

[29] A. Myasnikov, V. Roman'kov, *On rationality of verbal subsets in a group*, Theory Comput. Syst., **52**:4 (2013), 587–598. Zbl 1276.68113

[30] A. Myasnikov, V. Shpilrain, A. Ushakov, *Group-based cryptography*, Advanced Courses in Mathematics пїS CRM Barcelona, Birkhäuser, Basel, 2008. Zbl 1248.94004

[31] A. Myasnikov, V. Shpilrain, A. Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, Mathematical Surveys and Monographs, **177**, Amer. Math. Soc., Providence, 2011. Zbl 1248.94006

[32] M.Yu. Nedbay, *The rational subset membership problem for finitely generated abelian groups*, Vestnik Omskogo universiteta, **1999**:3 (1999), 37–41.

[33] M.Yu. Nedbay, *The rational subset membership problem for free products of groups*, Vestnik Omskogo universiteta, **2000**:2 (2000), 17–18.

[34] M. Newman, *Integral matrices*, Pure and Applied Mathematics, **45**, Academic Press, New York-London, 1972. Zbl 0254.15009

[35] G.A. Noskov, *Conjugacy problem in metabelian groups,* Math. Notes, **31**:4 (1982), 252–258. Zbl 0506.20013

[36] G.A. Noskov, V.N. Remeslennikov, V.A. RomanпїSkov, *Infinite groups*, J. Sov. Math., **18**:5 (1982), 669–735. Zbl 0479.20001

[37] P.S. Novikov, *On the algorithmic unsolbability of the word problem*, Dokl. Akad. Nauk SSSR, n. Ser., Zbl **85**:4 (1952), 709–712. Zbl 0047.24901

[38] P.S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Tr. Mat. Inst. Steklova, **44**, Acad. Sci. USSR, Moscow, 1955. Zbl 0068.01301

[39] M.O. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. Math. (2), **67** (1958), 172–194. Zbl 0079.24802

[40] V.N. Remeslennikov, *Conjugacy in polycyclic groups*, Algebra Logic, **8** (1971), 404–411. Zbl 0291.20037

[41] V.N. Remeslennikov, V.A. RomanпїSkov, *Model-theoretic and algorithmic questions in group theory*, J. Sov. Math., **31**:3 (1985), 2887–2939. Zbl 0573.20031

[42] N.S. Romanovskii, *Some algorithmic problems for solvable groups*, Algebra Logika, **13**:1 (1974), 26–34. Zbl 0292.20026

[43] N.S. Romanovskii, *The occurrence problem for extensions of abelian groups by nilpotent groups,* Sib. Math. J., **21** (1980), 273–276. Zbl 0469.20019

[44] V.A. Roman'kov, *Automorphisms of groups*, Acta Appl. Math., **29**:3 (1992), 241–280. Zbl 0772.20016

[45] 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.

[46] V.A. Roman'kov, *Rational subsets in groups*, Omsk State Univrersity, Omsk, 2014.

[47] V.A. Roman'kov, *On algorithmic problems in group theory*, Vestnik Omskogo universiteta, **2017**:2(84) (2017), 18–27.

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

[49] 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*, Glasg. Math. J., **60**:1 (2018), 209–218. Zbl 1427.20041

[50] V.A. Roman'kov, *Algebraic cryptology*, OmSU, Omsk, 2020.

[51] V.A. Roman'kov, *Two problems for solvable and nilpotent groups.* Algebra Logic, **59**:6 (2021), 483–492. Zbl 7350231

[52] V.A. Roman'kov, *Algorithmic theory of solvable groups*, Prikl. Diskr. Mat., **52** (2021), 16–64. Zbl 7382418

[53] R.A. Sarkisjan, *Algorithmic questions for linear algebraic groups, I*, Math. USSR, Sb., 41:2 (1982), 149–189. Zbl 0478.20028

[54] R.A. Sarkisjan, *Algorithmic questions for linear algebraic groups, II*, Math. USSR, Sb., **41**:3 (1982), 329–359. Zbl 0478.20029

[55] D. Segal, *Decidable properties of polycyclic groups,* Proc. Lond. Math. Soc., III. Ser., **61**:3 (1990), 497–528. Zbl 0674.20020

[56] E.I. Timoshenko, *Algorithmic problems for metabelian groups,* Algebra and Logic, **12**:2 (1973), 132–137.

[57] O.A, Yurak, *On the simultaneous reduction of elements of abelian groups to positive form*, Vestnik Omskogo universiteta, **2006**:3 (2006), 18–19.

[58] O.A, Yurak, *On the simultaneous reduction of elements of abelian groups to positive form, II*, Vestnik Omskogo universiteta, **2006**:4 (2006), 7–8.

[59] O.A. Yurak, *Positive elements of the Heisenberg group*, Vestnik Omskogo universiteta, **2008**:2 (2008), 16–19.

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