SⓔMR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

ФГАОУ ВО "Сибирский федеральный университет", СФУ и Институт математики
им. С.Л.Соболева СО РАН, Омский филиал
Federal State Autonomous Educational Institution of Higher Education "Siberian
Federal University" and Sobolev Institute of Mathematics SB RAS, Omsk Branch

Том 19, стр. 144–144 (2022) УДК 512.54, 510.53
DOI 10.33048/semi.2022.19.xxx MSC 20F10

UNDECIDABILITY OF THE SUBMONOID MEMBERSHIP PROBLEM FOR A SUFFICIENTLY LARGE FINITE DIRECT POWER OF THE HEISENBERG GROUP

V.A. ROMAN'KOV

Abstract. The submonoid membership problem for a finitely generated group G is the decision problem, where for a given finitely generated submonoid M of G and a group element g it is asked whether $g \in M$. In this paper, we prove that for a sufficiently large direct power $\mathbb{H}^n$ of the Heisenberg group $\mathbb{H}$, there exists a finitely generated submonoid M whose membership problem is algorithmically unsolvable. Thus, an answer is given to the question of M. Lohrey and B. Steinberg about the existence of a finitely generated nilpotent group with an unsolvable submonoid membership problem. It also answers the question of T. Colcombet, J. Ouaknine, P. Semukhin and J. Worrell about the existence of such a group in the class of direct powers of the Heisenberg group. This result implies the existence of a similar submonoid in any free nilpotent group $N_{k,c}$ of sufficiently large rank k of the class $c \geq 2$. The proofs are based on the undecidability of Hilbert's 10th problem and interpretation of Diophantine equations in nilpotent groups.

Roman'kov, V.A., Undecidability of the submonoid membership problem for a sufficiently large finite direct power of the Heisenberg group.

The research was supported with a grant from the Russian Science Foundation (project No. 19-71-10017).

Received on ?, ??, 2022, published on ? ?? 2022.

Keywords: nilpotent group, Heisenberg group, direct product, submonoid membership problem, rational set, decidability, Hilbert's 10th problem, interpretability of Diophantine equations in groups.

1. Introduction

The submonoid membership problem for finitely generated nilpotent groups, which has attracted the attention of a number of researchers in recent years, is considered. Recall that this is the problem of the existence of an algorithm that determines, given an arbitrary element g and a finitely generated submonoid M of a group G, whether g belongs to M. Note that in [13] the author announced a negative solution to this problem for a free nilpotent group $N_{k,c}$ of nilpotency class $c \geq 2$ of sufficiently large rank k. This result will appear in [15]. This gives an answer to the well-known question of M. Lohrey and B. Steinberg ([4], Open problem 24) about the existence of a finitely generated nilpotent group with an unsolvable submonoid membership problem. Moreover, the existence in $N_{k,c}$ of a finitely generated submonoid M with the unsolvable membership problem was established. The proof shows how, from an arbitrary Diophantine equation P, an element g and a finitely generated submonoid M of the group $N_{k,c}$ are effectively constructed such that g belongs to M if and only if the equation P is solvable in integers. Then the undecidability of Hilbert's 10th problem allows us to obtain from this result the undecidability of the membership problem for $N_{k.c}$ with respect to M.

In [2] the authors prove that the somewhat more general the subsemigroup membership problem is solvable for the Heisenberg group $\mathbb{H} = H(3, \mathbb{Z})$ consisting of upper triangular integer matrices with units along the diagonal. In other words, $\mathbb{H}$ is the free nilpotent group $N_{2,2}$. Earlier in [3] it was shown how to solve the problem of belonging of the identity matrix to finitely generated subsemigroups in $\mathbb{H}$. In [2], the question was raised about the decidability of the submonoid membership problem for a direct power of the Heisenberg group.

This paper is a continuation of our previous papers: the paper [13] mentioned above and the recently published paper [14], in which sufficient conditions for the decidability of the submonoid membership problem for a free nilpotent group of the class 2 with respect to a given submonoid M were presented, as well as the upcoming paper [15]. Our objective in this paper is to prove the undecidability of the submonoid membership problem for a sufficiently large finite direct power $\widetilde{\mathbb{H}} = \mathbb{H}^n$ of the Heisenberg group $\mathbb{H}$. Just as in [15], we prove that, given any Diophantine equation P, one can effectively construct an element g and a finitely generated submonoid $\widetilde{M}$ of the group $\widetilde{\mathbb{H}}$ such that g belongs to $\widetilde{M}$ if and only if the equation P is solvable in integers. Again, the undecidability of Hilbert's 10th problem allows us to obtain from this result the undecidability of the membership problem for $\widetilde{\mathbb{H}}$ with respect to $\widetilde{M}$.

This result also easily implies the existence of a submonoid M of a free nilpotent group $N_{k,c}$ of sufficiently large rank k of any class $c \geq 2$ with the unsolvable problem of belonging to M.

Note that a special case of the submonoid membership problem for G is the classical membership problem, which came from M. Dehn, where M is a finitely generated subgroup. In a different terminology, it is called the *generalized word problem.* A.I. Maltsev [5] showed that this problem is decidable for any finitely generated nilpotent group. It is worth noting that in the class of finitely generated nilpotent groups, almost all basic algorithmic problems (word, conjugacy, isomorphism, etc.) are solved positively. The exceptions are the problem of endomorphic reducibility and a number of problems related to equations and identities in groups. See surveys [10] – [12] on this subject.

The submonoid membership problem is the most important fragment of the more general rational subset membership problem. See survey [4].

This problem for a non-commutative 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 appears on a non-commutative platform. A new line of research has emerged and is being developed – noncommutative discrete optimization. The chapter "Discrete optimization in groups" in the book [1] is devoted to this direction. In this case, special attention is paid to the class of finitely generated nilpotent groups, which is closest to the class of abelian groups.

2. Diophantine equations and Skolem systems

Let $\zeta_1, \ldots, \zeta_t$ be an arbitrary set of commuting variables. A polynomial $D(\zeta_1, \ldots, \zeta_t)$ with integer coefficients in these variables is called *Diophantine.*

In this paper, we will write an arbitrary Diophantine equation in the form

$$D(\zeta_1, \ldots, \zeta_t) = \upsilon, \ \upsilon \in \mathbb{Z}, \tag{1}$$

where the polynomial from the left-hand side has zero constant term.

2.1. Skolem systems.

In the monograph [16], T. Skolem showed that any Diophantine equation is equivalent to a system of equations in a larger number of variables of three types: $\zeta\zeta' - \zeta'' = 0, \zeta + \zeta' - \zeta'' = 0, \zeta - \zeta' = 0$, and one equation of the form $\zeta - \upsilon = 0\,(\upsilon \in \mathbb{Z})$, where each variable ζ, ζ', ζ'' either occurs in the notation of the original polynomial $D(\zeta_1, \ldots, \zeta_t)$, or is introduced additionally. Such a system is called the *Skolem system.* In what follows, we also write the equations of the Skolem system in the form $\zeta\zeta' = \zeta'',\ \zeta + \zeta' = \zeta'',\ \zeta = \zeta',$ and $\zeta = \upsilon,$ respectively.

2.1.1. *Algorithm for obtaining the Skolem system.* We show how to write the Skolem system equivalent to an equation of the form (1). We assume that either all the coefficients of the polynomial $D(\zeta_1, \ldots, \zeta_t)$ are positive, or there are coefficients of different signs among them. If initially all these coefficients are negative, then we pass to the equation obtained by multiplying both parts of (1) by -1.

We take one of the non-linear monomials on the left-hand side of the considered equation. Let $\zeta\zeta'$ be the product of its two factors. We introduce a new variable ζ'' and write a new equation $\zeta\zeta' = \zeta''$ into the system, simultaneously replacing the product $\zeta\zeta'$ in the monomials by ζ''. The degree of the monomial under consideration will decrease by one. If it has become linear, go to the next monomial. If not, then we continue to act similarly with the given monomial until it becomes linear.

Then we move to the next monomial, and so on. As a result, the left-hand side of the equation will be represented as an algebraic sum of variables. Next, we introduce new variables, replacing $\zeta + \zeta'$ in this sum by ζ'' (similarly, $-\zeta - \zeta'$ is replaced by $-\zeta''$), adding the equation $\zeta + \zeta' = \zeta''$ to the system. We continue this process. If all coefficients in the algebraic sum are equal to 1, then the last equation will be of the form $\zeta = \upsilon$, which we will also include in the system. If terms of different signs were present, then by transforming all the terms on the left-hand side, we arrive at an equation of the form $\zeta - \zeta' = v$. Then we set $\zeta = \zeta' + \zeta''$ and $\zeta'' = v$.

2.1.2. *Nonnegative Diophantine equations and Skolem systems.* A Diophantine equation that is considered solvable if it has a solution in nonnegative integers is called *nonnegative*. Similarly, a Skolem system for which decidability means the existence of a solution in nonnegative integers is called *nonnegative*.

Lemma 1. *Decidability of an arbitrary Diophantine equation (1) is equivalent to the decidability of some nonnegative Diophantine equation in* $2t$ *variables effectively constructed from this equation. The resulting equation is equivalent to the nonnegative Skolem system* S_v.

Proof. We write each variable ζ_i as the difference of the new variables $\zeta_i' - \zeta_i''$. Substituting these differences for the variables of the equation (1), we obtain the nonnegative Diophantine equation

$$D_1(\zeta_1', \zeta_1'', \dots, \zeta_t', \zeta_t'') = 0. \tag{2}$$

Obviously, the decidability of the equation (1) in integers implies the decidability of the equation (2) in nonnegative integers, and vice versa.

Based on the nonnegative equation obtained in this way, we build the Skolem system, as described in the 2.1.1. All substitutions of the form $\zeta\zeta' = \zeta''$ and $\zeta + \zeta' = \zeta''$ lead to nonnegative variables of the Skolem system. An exception is possible only at the final replacement, when it is necessary to transform the equation of the form $\zeta - \zeta' = v$ for $v < 0$. Then we set $\zeta' = \zeta + \zeta''$ and $\zeta'' = -v$. In all cases the last equation has the form $\zeta = |v|$. □

Consider the obtained nonnegative Skolem system S_v. For what follows, we need the renumbering of variables, the introduction of new variables, and the ordering of the equations of the S_v system. For simplicity, the notation S_v does not change in this process.

Assume that S_v contains e equations of the form $\zeta_i\zeta_j = \zeta_l$. Introducing new variables ζ_s and making appropriate substitutions of the form ζ_i for ζ_s, we achieve that each variable will appear in these equations exactly once. Equations of the form $\zeta_s = \zeta_i$ for the new ζ_s we add to the system S_v. Next, we renumber the variables in such a way that all e equations take the form

$$\begin{gathered} \zeta_1\zeta_2 = \zeta_3, \\ \dots \\ \zeta_{3(e-1)+1}\zeta_{3(e-1)+2} = \zeta_{3e}. \end{gathered} \tag{3}$$

Let the system S_v contains d equations of the form $\zeta_i + \zeta_j = \zeta_l$. Similarly to the case just considered, we will ensure that among the variables of the considered set of equations there will be no variables of the previous subsystem, and each variable in their entries will appear in these equations exactly once. Next, we renumber the variables of this subsystem in such a way that all d equations of the indicated form will include only the variables $\zeta_{3e+1}, \dots, \zeta_{3(e+d)}$, and the subsystem itself will take the form

$$\begin{gathered} \zeta_{3e+1} + \zeta_{3e+2} = \zeta_{3(e+1)}, \\ \dots \\ \zeta_{3(e+d-1)+1} + \zeta_{3(e+d-1)+2} = \zeta_{3(e+d)}. \end{gathered} \tag{4}$$

Next, we write the third system, consisting of equations related to the equalites of variables. We write all equalities of the form $\zeta_i = \zeta_j$, for pairs with different indices $1 \leq i, j \leq 3(e+d)$, which follow from the set of all equalities. It suffices to fix one representative ζ in each class of equal variables and write down all equations of the form $\zeta = \zeta'$ for the remaining variables ζ' from this class. Then we renumber all the equations of this subsystem by assigning them the numbers $e+d+1, \ldots, e+d+q$, respectively. We have the system of equations

(5)

$$P_k \sim \zeta_{i(k)} = \zeta_{j(k)}, \; i(k) \neq j(k), 1 \leq i(k), j(k) \leq 3(e+d), k = e+d+1, \ldots, e+d+q.$$

It remains to write a special equation

$$\zeta_t = |v|. \tag{6}$$

Except for the trivial equation (1) of the form $\zeta_1 = v \, (t = 1)$, the variable ζ_t is present in the system (5). Hence, $\zeta_1, \ldots, \zeta_{3e}, \zeta_{3e+1}, \ldots, \zeta_{3(e+d)}$ are all variables of the system S_v. It is obvious that the system S_v is equivalent to the new system thus replaced.

3. Auxiliary assertions

Now we prove a number of auxiliary assertions. The commutator $[g, f]$ of two elements g and f of a group G is defined as $g^{-1}f^{-1}gf$. Then $gf = fg[g, f]$.

Recall that the group $\mathbb{H}$ is generated by the transvections $a = t_{12}$ and $b = t_{23}$, and its center is the infinite cyclic group generated by their commutator $c = [b, a] = t_{13}^{-1}$. Then for any $\alpha, \beta \in \mathbb{Z}$, $b^\beta a^\alpha = a^\alpha b^\beta c^{\alpha\beta}$. Further in the paper, $\mathbb{H}^k = \prod_{i=1}^k \mathbb{H}(i)$ denotes the direct product of k copies of the group $\mathbb{H}$. Denote the transvections $t_{12}, t_{23}, t_{13}^{-1}$ in the i-th copy $(i = 1, \ldots, k)$ as a_i, b_i, c_i respectively. In what follows, $b_{i \to j} \; (i < j)$ means $b_i \cdot \ldots \cdot b_j$.

Lemma 2. *Let M be a submonoid of $\mathbb{H}$ generated by $g_1 = ac, b$ and $g_2 = a^{-1}$. Then any representation of b in terms of the generators of M has the form*

$$b = g_1^\zeta b g_2^\zeta, \zeta \in \mathbb{N} \cup \{0\}. \tag{7}$$

Proof. Obviously, the generator b of the submonoid M appears exactly once among the factors of the right-hand side (7), and the total exponents of the occurrences of the other two generators g_1 and g_2 are equal. Then the cancellation of the degree c^ζ occurs only for the indicated arrangement of the generators of the submonoid on the right-hand side (7).

The cancellation occurs during the commutator collecting process, which consists in the transition of g_2^ζ through b. Namely,

$$g_1^\zeta b g_2^\zeta = (a^\zeta c^\zeta) a^{-\zeta} b [b, a^{-\zeta}] = b. \tag{8}$$

□

The scheme of the exact location of the generators of the submonoid M when expressing the element b is as follows.

$$\left| \begin{array}{ccccc} & & g_1^\zeta & b & g_2^\zeta \\ \mathbb{H}: & b = & a^\zeta c^\zeta & b & a^{-\zeta} \end{array} \right| .$$

Table 1.

The following lemma allows us to interpret equations of the form $\zeta + \zeta' = \zeta''$ in the group $\mathbb{H}^4$.

Lemma 3. *Let M be a submonoid of $\mathbb{H}^4$ generated by $g_1 = a_1c_1c_4, g_2 = a_2c_2c_4, g_3 = a_3c_3c_4^{-1}, g_4 = a_1^{-1}, g_5 = a_2^{-1}, g_6 = a_3^{-1}$, and $f_1 = b_1b_2b_3$. Then the representation of $\dot{b} = b_{1\to 3}$ in terms of the generators of M has the form*

$$\dot{b} = g_1^{\zeta} g_2^{\zeta'} g_3^{\zeta''} f_1 g_4^{\zeta} g_5^{\zeta'} g_6^{\zeta''} \tag{9}$$

Such a representation for nonnegative integers ζ, ζ', ζ'' exists if and only if $\zeta + \zeta' = \zeta''$.

Proof. We note that for given positive ζ, ζ', ζ'', the form (9) is uniquely determined up to a permutation of the factors g_i $(i = 1, 2, 3)$ on the left-hand side and g_j $(j = 4, 5, 6)$ on the right-hand side of the factor f_1. For null value of ζ, ζ' or ζ'', we assume that the corresponding generator is located as indicated.

Obviously, the generator f_1 of the submonoid M occurs exactly once among the factors of the right-hand side of (9), and the total exponents of occurrences of any pair of generators g_i and g_{i+3} for $i = 1, 2, 3$ are the same, say ζ, ζ' and ζ'', respectively. The location of the factors g_i and g_{i+3} for $i = 1, 2, 3$ with respect to f_1 follows from Lemma 2. The representation (9) for nonnegative integers ζ, ζ', ζ'' exists if and only if $\zeta + \zeta' = \zeta''$. If the equality (9) holds, then the component in $\mathbb{H}(4)$ must be $c_4^{\zeta+\zeta'=\zeta''} = 1$, hence $\zeta + \zeta' = \zeta''$. If the equality $\zeta + \zeta' = \zeta''$ is true, then (9) is checked directly.

□

The scheme of the exact location of the components of the generators of the submonoid M when expressing the element $\dot{b}$ is as follows (empty positions correspond to trivial elements).

	$\dot{b} =$	g_1^{ζ}	$g_2^{\zeta'}$	$g_3^{\zeta''}$	f_1	g_4^{ζ}	$g_5^{\zeta'}$	$g_6^{\zeta''}$
$\mathbb{H}(1):$	$b_1 =$	$a_1^{\zeta}c_1^{\zeta}$			b_1	$a_1^{-\zeta}$		
$\mathbb{H}(2):$	$b_2 =$		$a_2^{\zeta'}c_2^{\zeta'}$		b_2		$a_2^{-\zeta'}$	
$\mathbb{H}(3):$	$b_3 =$			$a_3^{\zeta''}c_3^{\zeta''}$	b_3			$a_3^{-\zeta''}$
$\mathbb{H}(4):$	$1 =$	c_4^{ζ}	$c_4^{\zeta'}$	$c_4^{-\zeta''}$				

Table 2.

Lemma 4. *Let M' be a submonoid of $\mathbb{H}^6$ generated by $g'_1 = a_1c_1, g'_2 = a_2c_2, g'_3 = a_1^{-1}a_3c_3, g'_4 = a_2^{-1}a_4c_4, f'_1 = b_1b_2, f'_2 = b_3b_4, g'_5 = a_3^{-1}a_5c_5, g'_6 = a_4^{-1}a_6c_6, f'_3 = b_5b_6, g'_7 = a_5^{-1}, g'_8 = a_6^{-1}$. Then the representation of b_{1-6} in terms of the generators of M' has the form*

$$b_{1\to 6} = (g'_1)^{\zeta}(g'_2)^{\zeta'} f'_1 (g'_3)^{\zeta}(g'_4)^{\zeta'} f'_2 (g'_5)^{\zeta}(g'_6)^{\zeta'} f'_3 (g'_7)^{\zeta}(g'_8)^{\zeta'}. \tag{10}$$

Proof. For given positive ζ, ζ' the form (10) is defined uniquely up to a permutation of the generators g'_1, g'_2 on the left-hand side and g'_3, g'_4 on the right-hand side of f'_1, g'_5, g'_6 on the left-hand side and g'_7, g'_8 on the right-hand side of f'_3. For null value of ζ or ζ', we assume that the corresponding generator is located as indicated.

The proof is similar to the proof of Lemma 3 and follows from Lemma 2. Obviously, each of the generators f'_1, f'_2, f'_3 of the submonoid M' occurs exactly once among the factors of the right-hand side of (9), and the total exponents of occurrences of any pair of generators $(g'_1, g'_3), (g'_2, g'_4), (g'_3, g'_5), (g'_4, g'_6)$ and (g'_5, g'_7), (g'_6, g'_8) are the same, respectively. Then the quadruples of generators (g'_1, g'_3, g'_5, g'_7) and (g'_2, g'_4, g'_6, g'_8) have the same exponents, say ζ and ζ', respectively. The location of the factors g'_ith with respect to f'_jth follows from Lemma 2.

□

The scheme of the exact location of the components of the generators of the submonoid M' when expressing the element $b_{1\to 6}$ is as follows (empty positions correspond to trivial elements).

	$b_{1\to6} =$	$(g_1')^{\zeta}(g_2')^{\zeta'}$	f_1'	$(g_3')^{\zeta}(g_4')^{\zeta'}$	f_2'	$(g_5')^{\zeta}(g_6')^{\zeta'}$	f_3'	$(g_7')^{\zeta}(g_8')^{\zeta'}$
$\mathbb{H}(1):$	$b_1 =$	$a_1^{\zeta}c_1^{\zeta}$	b_1	$a_1^{-\zeta}$				
$\mathbb{H}(2):$	$b_2 =$	$a_2^{\zeta'}c_2^{\zeta'}$	b_2	$a_2^{-\zeta'}$				
$\mathbb{H}(3):$	$b_3 =$			$a_3^{\zeta}c_3^{\zeta}$	b_3	$a_3^{-\zeta}$		
$\mathbb{H}(4):$	$b_4 =$			$a_4^{\zeta'}c_4^{\zeta'}$	b_4	$a_4^{-\zeta'}$		
$\mathbb{H}(5):$	$b_5 =$					$a_5^{\zeta}c_5^{\zeta}$	b_5	$a_5^{-\zeta}$
$\mathbb{H}(6):$	$b_6 =$					$a_6^{\zeta'}c_6^{\zeta'}$	b_6	$a_6^{-\zeta'}$

Table 3.

Lemma 5. *Consider the group* $\mathbb{H}^8$*. Let* M *be its submonoid generated by the elements* $g_1 = a_1c_1a_7, g_2 = a_2c_2, f_1 = b_1b_2, g_3 = a_1^{-1}a_3c_3, g_4 = a_2^{-1}a_4c_4b_7, f_2 = b_3b_4, g_5 = a_3^{-1}a_5c_5a_7^{-1}, g_6 = a_4^{-1}a_6c_6, f_3 = b_5b_6, g_7 = a_5^{-1}, g_8 = a_6^{-1}b_7^{-1}$ *(whose projections onto* $\mathbb{H}^6$ *coincide with the generators of the submonoid* M' *in the lemma 4 with the same notation, but with '), and by the elements* $g_9 = a_8c_8c_7, f_4 = b_8, g_{10} = a_8^{-1}$*. Then the representation of* $\ddot{b} = b_{1\to6}b_8$ *in terms of the generators of* M *has the form*

$$\ddot{b} = g_1^{\zeta}g_2^{\zeta'}f_1g_3^{\zeta}g_4^{\zeta'}f_2g_5^{\zeta}g_6^{\zeta'}f_3g_7^{\zeta}g_8^{\zeta'}g_9^{\zeta''}f_4g_{10}^{\zeta''}. \tag{11}$$

Such a representation for nonnegative integers ζ, ζ', ζ'' *exists if and only if* $\zeta\zeta' = \zeta''$*.*

Proof. For given positive ζ, ζ' the form (11) is defined uniquely up to a permutation of the generators g_1, g_2 on the left-hand side and g_3, g_4 on the right-hand side of f_1, g_5, g_6 on the left-hand side and g_7, g_8 on the right-hand side of f_3. We also note that the last three generators are uniquely located relative to each other, but in relation to other generators they can occupy any position, since these elements commute with other generators. For given positive ζ, ζ', ζ'' the equality $\zeta \cdot \zeta' = \zeta''$ is necessary and sufficient for the indicated occurrence of the element $\ddot{b}$ in the submonoid M. For null value of ζ, ζ' or ζ'', we assume that the corresponding generator is located as indicated. It is clear that the configuration of the factors in (10) is preserved for their counterparts in (11). Such a representation for nonnegative integers ζ, ζ', ζ'' exists if and only if $\zeta\zeta' = \zeta''$. If the equality (11) holds, then the component in $\mathbb{H}(7)$ must be $c_7^{\zeta''-\zeta\zeta'} = 1$, hence $\zeta\zeta' = \zeta''$. If the equality $\zeta\zeta' = \zeta''$ is true, then (11) is checked directly. □

The scheme of the exact location of the components of the generators of the submonoid M when expressing the element $\ddot{b}$ is as follows (empty positions correspond to trivial elements). The scheme consists of the table 4 presenting all the generators except g_9, f_4, g_{10} and table 4' presenting these three generators with components on the last two rows, corresponding $\mathbb{H}(7)$ and $\mathbb{H}(8)$ respectively, and additional to table 4 three columns. The remaining components of these elements are trivial.

$$\left|\begin{array}{rlccccccc}
 & \ddot{b} \;= g_1^{\zeta} g_2^{\zeta} & f_1 & g_3^{\zeta} g_4^{\zeta'} & f_2 & g_5^{\zeta} g_6^{\zeta'} & f_3 & g_7^{\zeta} g_8^{\zeta'} \\
\mathbb{H}(1): & b_1 = a_1^{\zeta} c_1^{\zeta} & b_1 & a_1^{-\zeta} & & & & \\
\mathbb{H}(2): & b_2 = a_2^{\zeta'} c_2^{\zeta'} & b_2 & a_2^{-\zeta'} & & & & \\
\mathbb{H}(3): & b_3 = & & a_3^{\zeta} c_3^{\zeta} & b_3 & a_3^{-\zeta} & & \\
\mathbb{H}(4): & b_4 = & & a_4^{\zeta'} c_4^{\zeta'} & b_4 & a_4^{-\zeta'} & & \\
\mathbb{H}(5): & b_5 = & & & & a_5^{\zeta} c_5^{\zeta} & b_5 & a_5^{-\zeta} \\
\mathbb{H}(6): & b_6 = & & & & a_6^{\zeta'} c_6^{\zeta'} & b_6 & a_6^{-\zeta'} \\
\mathbb{H}(7): & 1 \;=\; a_7^{\zeta} & & b_7^{\zeta'} & & a_7^{-\zeta} & & b_7^{-\zeta'} \\
\mathbb{H}(8): & b_8 = & & & & & &
\end{array}\right|$$

Table 4.

$$\left|\begin{array}{lccc}
 & g_9^{\zeta''} & f_4 & g_{10}^{\zeta''} \\
\mathbb{H}(7): & c_7^{\zeta''} & & \\
\mathbb{H}(8): & a_8^{\zeta''} c_8^{\zeta''} & b_8 & a_8^{-\zeta''}
\end{array}\right|$$

Table 4'.

4. Main results

Theorem 1. *For any Diophantine equation (1) there exists a direct power $\widetilde{\mathbb{H}} = \mathbb{H}^n$ of the Heisenberg group $\mathbb{H}$, a finitely generated submonoid $\widetilde{M}$ in it and an element $g(\upsilon) \in \widetilde{\mathbb{H}}$ such that the equation (1) is solvable in integers if and only if $g(\upsilon)$ belongs to $\widetilde{M}$. The parameter n, the element $g(\upsilon)$, and the finite set of generators of the submonoid $\widetilde{M}$ are effectively determined. The submonoid $\widetilde{M}$ depends only on the Diophantine polynomial D on the left-hand side (1).*

Proof. Further in the proof, the considered powers of the group $\mathbb{H}$ are considered to be subgroups of the group $\widetilde{\mathbb{H}}$ with corresponding indices. Speaking of adding components to the elements of the group $\widetilde{\mathbb{H}}$, we have in mind non-trivial components. Components not explicitly defined are considered trivial.

First, a Diophantine equation (1) is taken. Then the equivalent nonnegative Skolem system S_υ is constructed from this equation. The variables and equations of this system are ordered and written as specified in (3–6). To the resulting system S_υ we associate the group $\widetilde{\mathbb{H}} = \mathbb{H}^n$ for $n = 8e + 4d + q + 1$. The first $8e$ factors of this group are sequentially divided into e blocks of 8 factors each: $B_1, \ldots, B_e$, where $B_i = \mathbb{H}(8(i-1)+1) \times \ldots \times \mathbb{H}(8(i-1)+8)$, $i = 1, \ldots, e$. Each block in accordance with the lemma 5 corresponds to equation with the same system number in (3). The following d blocks of 4 factors each are $B_{e+1}, \ldots, B_{e+d}$, where $B_{e+i} = \mathbb{H}(8e+4(i-1)+1) \times \ldots \times \mathbb{H}(8e+4(i-1)+4)$, $i = 1, \ldots, d$. Each block B_{e+i} in accordance with the lemma 3 corresponds to equation with the system number i in (4). Remaining $q+1$ factors are not divided into blocks. The next q factors $\mathbb{H}(k)$, $k = 8e+4d+1, \ldots, 8e+4d+q$ correspond sequentially to the equations of system (5). The last factor $\mathbb{H}(8e+4d+q+1)$ corresponds to the equation (6).

We construct a submonoid $\widetilde{M}$ of the group $\widetilde{\mathbb{H}}$ by defining its generating elements in accordance with lemmas 3 and 5 modified by adding multipliers to some of them from the factors $\mathbb{H}(8e+4d+k)$ for $k = 1, \ldots q$, taking into account the equation (6), that corresponds to the last factor $\mathbb{H}(8e+4d+q+1)$.

Construction of submonoid generators associated with the systems (3) and (4). Consider first the equations of system (3). The blocks $B_1, \dots, B_e$ correspond sequentially to these equations. Each of them is isomorphic to the group $\mathbb{H}^8$. Let $\mu_i : \mathbb{H}^8 \to B_i$ for $i = 1, \dots, e$ be an isomorphism such that the generators a_j, b_j each of the factors $\mathbb{H}(j)$ are mapped to $a_{8(i-1)+j}, b_{8(i-1)+j}$ $(j = 1, \dots, 8)$ respectively.

Let M be a submonoid of the group $\mathbb{H}^8$ defined in the lemma 5 by the set of generators $C = \{g_1, \dots, f_1, \dots, g_{10}\}$. Then $M_i = \mu_i(M)$ is the submonoid of B_i generated by the set $C_i = \mu_i(C)$. For B_i we define $b(i) = \mu_i(\ddot{b})$ $(i = 1, \dots, e)$. Then for each $B_i, i = 1, \dots, e$, the natural analog of the statement of the lemma 5 is valid with the submonoid M and element $\ddot{b}$ replaced by M_i and $b(i)$ respectively. An analogue of the expression (11) is also true for exponents ζ, ζ', ζ'' replaced by $\zeta_{3(i-1)+1}, \zeta_{3(i-1)+2}, \zeta_{3(i-1)+3}$ respectively. An analogue of the assertion about the uniqueness of such a representation made in the proof of lemma 5 is also true.

We compose the group

$$B(1) = \prod_{i=1}^{e} B_i \simeq \mathbb{H}^{8e}. \tag{12}$$

We put $M(1) = \prod_{i=1}^{e} M_i$. The so-defined submonoid is a projection of the submonoid $\widetilde{M}$ under construction into the group $B(1)$. It is generated by the set $\bar{C} = \cup_{i=1}^{e} C_i$.

It follows from lemma 5 that an element $\bar{b}(1) = \prod_{i=1}^{e} b(i)$ belongs to the submonoid $M(1)$ of the group $B(1)$ if and only if the variables ζ_i, $i = 1, \dots, 3e$, are a solution to the system (3).

Consider now the equations of the system (4). The blocks $B_{e+1}, \dots, B_{e+d}$ correspond sequentially to these equations. Each of them is isomorphic to the group $\mathbb{H}^4$. Let $\nu_{e+i} : \mathbb{H}^4 \to B_{e+i}$ for $i = 1, \dots, d$ be an isomorphism in which the generators a_j, b_j of the factor $\mathbb{H}(j)$ map to $a_{8e+4(i-1)+j}, b_{8e+4(i-1)+j}$ respectively $(j = 1, \dots, 4)$.

Let M be a submonoid of the group $\mathbb{H}^4$ defined in the lemma 3 by the set of generators $D = \{g_1, \dots, f_1, \dots, g_6\}$. Then $M_{e+i} = \nu_{e+i}(M)$ is the submonoid of B_{e+i} generated by the set $D_{e+i} = \nu_{e+i}(D)$. For B_{e+i} we define $b(e+i) = \nu_{e+i}(\dot{b})$ $(i = 1, \dots, d)$. Then for each B_{e+i} the natural analog of the statement of the lemma 3 is valid with the submonoid M and element $\dot{b}$ replaced by M_{e+i} and $b(e+i)$ respectively. An analogue of the expression (9) is also true for exponents ζ, ζ', ζ'' replaced by $\zeta_{3e+3(i-1)+1}, \zeta_{3e+3(i-1)+2}, \zeta_{3(i-1)+3}$ respectively. An analogue of the assertion about the uniqueness of such a representation made in the proof of lemma 3 is also true.

Now we define

$$B(2) = \prod_{i=1}^{d} B_{e+i} \simeq \mathbb{H}^{4d}. \tag{13}$$

We put $M(2) = \prod_{i=1}^{d} M_{e+i}$. The so-defined submonoid is a projection of the submonoid $\widetilde{M}$ under construction into the group $B(2)$. It is generated by the set $\bar{D} = \cup_{i=1}^{d} D_{e+i}$.

It follows from lemma 3 that an element $\bar{b}(2) = \prod_{i=1}^{d} b(e+i)$ belongs to the submonoid $M(2)$ of the group $B(2)$ if and only if the variables ζ_{3e+i}, $i = 1, \dots, 3e + 3d$, are a solution to the system (4).

We regard the groups $B(1)$ and $B(2)$ as naturally embedded in the group $\mathbb{H}^{8e+4d}$.

We put $B(1,2) = B(1) \cdot B(2)$ and define $M(1,2) = M(1) \cdot M(2)$. We also put $\bar{b}(1,2) = \bar{b}(1)\bar{b}(2)$. It follows from the above considerations that the element $\bar{b}(1,2)$ belongs to $M(1,2)$ if and only if the combined system of equations (3) and (4) is solvable in nonnegative integers $\zeta_1, \ldots, \zeta_{3(e+d)}$.

The submonoid $M(1,2)$ is generated by the set $\bar{C} \cup \bar{D}$. It is easy to calculate that this set consists of $14e + 7d$ elements. Rename and number these elements as $h_1, \ldots, h_{14e+7d}$. The set of generating elements $\tilde{h}_1, \ldots, \tilde{h}_{14e+7d}$ of the submonoid $\widetilde{M}$ has the same cardinality. Each element $\tilde{h}_i$ has a projection h_i to the group $B(1,2)$.

Construction of generators of the submonoid $\widetilde{M}$ associated with the system S_v. We define an element

$$g(v) = \bar{b}(1,2)c_{8e+4d+q+1}^{|v|} \in \widetilde{\mathbb{H}}. \tag{14}$$

Since all variables of the systems (3) and (4) are pairwise distinct, both of them are decidable together. It remains to take into account the equalities between these variables in the system (5) and the system (6). So, we consider the system S_v of equations, which is the union of all four systems: (3) – (6). We proceed to the completion of the construction of the submonoid $\widetilde{M}$, whose membership problem is equivalent to the decidability of the system S_v in nonnegative integers. Namely, we will prove that $g(v)$ belongs to $\widetilde{M}$ if and only if the system S_v has a solution in the nonnegative integers.

We include components in the factors $\mathbb{H}(i)$ for $i = e + d + 1, \ldots, e + d + q + 1$ into some of the elements of $\tilde{h}_i$ during construction. We do this as follows.

For any equation P_{e+d+k} $(k = 1, \ldots, q)$ of the form $\zeta_{i(k)} = \zeta_{j(k)}$ from (5) we find among the generating elements of the submonoid $M(1,2)$ such one h_l whose exponent in the equation corresponding to the equation (9) or to the equation (11) is equal to $\zeta_{i(k)}$. Add the element $c_{8e+4d+k}$ to $\tilde{h}_l$ in its the factor $\mathbb{H}(8e + 4d + k)$. Then we similarly find element h_p with the exponent $\zeta_{j(k)}$ and add the element $c_{8e+4d+k}^{-1}$ to $\tilde{h}_p$ in the same factor. We add no nontrivial components to the other generators $\tilde{h}_i$ in this factor. This component will be trivial for any expression of the element $g(v)$ if and only if $\zeta_{i(k)} = \zeta_{j(k)}$.

Then for equation (6), we similarly find the one of the generating elements h_r of the submonoid $M(1,2)$ whose exponent is equal to ζ_t and add the element $c_{8e+4d+q+1}$ to the $8e + 4d + q + 1$th component of $\tilde{h}_r$. Note, that this component is equal to $c_{8e+4d+q+1}^{\zeta_t}$ for any expression of the element $g(v)$ if and only if $\zeta_{i(k)} = \zeta_{j(k)}$.

The process of constructing the generators of the submonoid $\widetilde{M}$ of the group $\widetilde{\mathbb{H}}$ is completed.

We give a formal proof that $g(v)$ belongs to $\widetilde{M}$ if and only if the system S_v has a solution in nonnegative integers.

Let us assume that the system S_v has a solution in non-negative integers $\zeta_1, \ldots, \zeta_t$. Then the equations (3) and (4) become equalities. By lemmas 3 and 5 and their analogues for the groups B_i $(i = 1, \ldots, e + d)$ form the expression $b(1,2)$ in terms of the elements $h_1, \ldots, h_{14e+7d}$. Then the analogous expression for the elements $\tilde{h}_1, \ldots, \tilde{h}_{14e+7d}$ is equal to the element g_v because the components of this expression with numbers $8e + 4d + k$ $(k = 1, \ldots, q)$ are trivial due to equations (5) and the last component is $c^{|v|}$. Thus $g_v \in \widetilde{M}$.

Suppose now that the element $g(v)$ belongs $\widetilde{M}$. Then for every its expression of the form

$$g(\upsilon) = g(\tilde{h}_1, \ldots, \tilde{h}_{14e+7d}) \tag{15}$$

through the generators of $\widetilde{M}$ the equalities (3) and (4) hold by lemmas 3 and 5. The components with numbers $8e + 4d + k$ $(k = 1, \ldots, q)$ must be trivial, which corresponds to the fulfillment of the equalities (5). The $(8e+4d+q+1)$th component must be equal to $c_{8e+4d+q+1}^{|\upsilon|}$, which means that (6) satisfied. Consequently, the exponents $\zeta_1, \ldots, \zeta_{3(e+d)}$, with which the generators of the submonoid $\widetilde{M}$ enter the representation of the element $g(\upsilon)$, are the solution of the system S_υ.

□

Recall that Hilbert's 10th problem is the question of the existence of an algorithm that, given a Diophantine equation determines whether it has an integer solution. Yu.V. Matiyasevich (see [6]–[9]) proved that such an algorithm does not exist. In addition, he established that there exists a Diophantine polynomial $D_0(\zeta_1, \ldots, \zeta_t)$ with a zero constant term such that there is no algorithm that determines the decidability of equations of the form

$$D_0(\zeta_1, \ldots, \zeta_t) = \upsilon,\ \upsilon \in \mathbb{Z}. \tag{16}$$

From the undecidability of Hilbert's 10th problem and Theorem 1, it follows that the submonoid membership problem in the class of finite direct powers of the Heisenberg group is undecidable.

The existence of an algorithmically unsolvable equation of the form (16) with a fixed left-hand side and parameter υ allows us to establish the following stronger assertion.

Theorem 2. *For sufficiently large $n \in \mathbb{N}$, the direct power $\widetilde{\mathbb{H}} = \mathbb{H}^n$ of the Heisenberg group $\mathbb{H}$ contains a finitely generated submonoid $\widetilde{M}$ with an unsolvable membership problem.*

Proof. First, an equation of the form (16), which is unsolvable in integers, is taken. Then the equivalent nonnegative Skolem system $S(\upsilon)$ is constructed from this equation. The rest of the proof completely repeats the proof of the Theorem 1. Variations of the parameter υ in the equation (16) correspond to variations of the element $g(\upsilon)$. The submonoid $\widetilde{M}$ does not change. An element $g(\upsilon)$ belongs to $\widetilde{M}$ if and only if the system S_υ is solvable in nonnegative integers. This is equivalent to saying that the equation (16) with this parameter is solvable in integers. This implies the assertion of the theorem.

□

Note that the existence of a finitely generated submonoid with an unsolvable membership problem in a finitely generated nilpotent group implies the existence of a similar submonoid in the corresponding free nilpotent group.

Proposition 1. *For $k, c \in \mathbb{N}$, let N be a k-generated nilpotent group of class c that has a finitely generated submonoid M with the undecidable membership problem. Then the free nilpotent group $N_{k,c}$ contains a finitely generated submonoid $\widetilde{M}$ with an undecidable membership problem.*

Proof. Consider the natural homomorphism $\phi : N_{k,c} \to N$. Let $\widetilde{M}$ denote the full pre-image of the submonoid M in $N_{k,c}$. An element $g \in N$ belongs to M if and only if any of its inverse images $\tilde{g}$ belongs to $\widetilde{M}$. It remains to note that the submonoid $\widetilde{M}$ is finitely generated.

Let $\widetilde{M}$ is generated by elements $\tilde{g}_1, \ldots, \tilde{g}_l$. For each of these generators g_i, take some inverse image $\tilde{g}_i$ in the group $N_{k,c}$. The group $N_{k,c}$ is Noetherian, so $\ker(\mu)$ is a finitely generated subgroup. Let $\ker(\phi) = \mathrm{gp}(f_1, \ldots, f_t)$. Then the submonoid M is generated by the elements $g_1, \ldots, g_l, f_1^{\pm 1}, \ldots, f_t^{\pm 1}$.

□

Theorem 2 and proposition 1 imply that a submonoid with an unsolvable membership problem exists in any free nilpotent group $N_{k,c}$ for $c \geq 2$ of sufficiently large rank k.

References

[1] F. Bassino, I. Kapovich, M. Lohrey, A. Miasnikov, A. Nicaud, A. Nikolaev, I. Rivin, V. Shpilrain, A. Ushakov, P. Weil, *Complexity and Randomness in Group Theory: GAGTA BOOK 1.* Walter de Gruyter, Berlin, Boston, 2020, 386 p.

[2] 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, Germany, 2019, 44:1–44:15.

[3] S.-Ki Ko, R. Niskanen, R. Niskanen, and I. Potapov, *On the identity problem for the special linear group and the Heisenberg group*, In: I. Chatzigiannakis, C. Kaklamanis, D. Marx, and D. Sannella (Eds), 45th Intern. Colloquium on Automata, Languages, and Programming (ICALP 2018), LIPIcs, **132**, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2018, 132:1–132:15.

[4] M. Lohrey, *The rational subset membership problem for groups: A survey*, In C. Campbell, M. Quick, E. Robertson, & C. Roney-Dougal (Eds.), Selected papers of the conference, St. Andrews, UK, August, 2013, London Mathematical Society Lecture Note Series, **422**, Cambridge University Press, 2015, 368–389, Zbl 1346.20043

[5] A.I. Maltsev, *Homomorphisms onto finite groups*, Ivanov Gos. Ped. Inst. Uchen. Zap., **18** (1958), 49–60.

[6] Yu. V. Matiyasevich, *The Diophantineness of enumerable set*, Soviet Mathematics, **11**:2 (1970), 354–357.

[7] Yu. V. Matiyasevich, *Diophantine representation of enumerable predicate*, Izvestiya Math., **5**:1 (1971), 1–28. Zbl 0219.02035

[8] Yu. Matiyasevich, *Some purely mathematical results inspired by mathematical logic*, In: Proc. Fifth Intern. Congr. Logic, Methodology and Philos. of Sci., London, Ont., 1995, 121–127.

[9] Y. Matijasevic, J. Robinson, *Reduction of Diophantine equation to one in 13 unknowns*, Acta Arith., **27** (1975), 521–553.

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

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

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

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

[14] V.A, Roman'kov, *Positive elements and sufficient conditions for solvability of the submonoid membership problem for nilpotent groups of class two*, Siberian Electronic Mathematical Reports, **19**:2 (2022), 387–403.

[15] V.A. Roman'kov, *Unsolvability of the submonoid membership problem for a free nilpotent group of class $l \geq 2$ of a sufficiently large rank*, Izvestiya Math. (accepted for publication).

[16] T. Skolem, *Diophantische Gleichungen*, Springer, Berlin, 1938, 130 p.

Vitalii Anatolievich Roman'kov
Federal State Autonomous Educational Institution of Higher Education "Siberian Federal University
79/10, Svobodny pr.,
Krasnoyarsk, 660041, Russia;
Sobolev Institute of Mathematics, Omsk Branch,
13, Pevtsov str.,
Omsk, 644099, Russia
Email address: `romankov48@mail.ru`