

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)
DOI 10.33048/semi.2022.19.xxx

УДК 512.54, 510.53
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.

© 2022 ROMAN'KOV V.A.

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 [18] the author announced a negative solution to this problem for a free nilpotent group $N_{k,c}$ of nilpotency class c at least two of sufficiently large rank k . This result will appear in [20]. This gives an answer to the well-known question of M. Lohrey and B. Steinberg ([5], 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 with respect to M .

In [2] the authors prove that the somewhat more general the subsemigroup membership problem is decidable for the Heisenberg group $\mathbb{H} = H(3, \mathbb{Z})$ consisting of upper triangular integer matrices with units along the diagonal. In other words, the Heisenberg group is a free nilpotent group of rank two and class two. Earlier in [4] 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 [18] mentioned above and the recently published paper [19], in which sufficient conditions for the solvability 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 [20]. Our objective in this paper is to prove the undecidability of the submonoid membership problem for a sufficiently large finite direct power $\tilde{\mathbb{H}} = \mathbb{H}^n$ of the Heisenberg group \mathbb{H} . Just as in [20], we prove that, given any Diophantine equation P , one can effectively construct an element g and a finitely generated submonoid M of the group $\tilde{\mathbb{H}}$ such that g belongs to 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 $\tilde{\mathbb{H}}$ with respect to M .

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

Note that a special case of the submonoid membership problem 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 [6] 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. See surveys [11], [12], [17]. The exceptions are the problem of endomorphic reducibility and a number of problems related to equations and identities in groups. See [14], [15], [16], [3], [13] on this subject.

The submonoid membership problem is the most important fragment of the more general rational subset membership problem. See survey [5].

The submonoid membership 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 ζ_1, \dots, ζ_t be an arbitrary set of commuting variables. A polynomial $D(\zeta_1, \dots, \zeta_t)$ with integer coefficients in these variables is called *Diophantine*.

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

$$(1) \quad D(\zeta_1, \dots, \zeta_t) = v, \quad v \in \mathbb{Z},$$

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

2.1. Skolem systems. In the monograph [21], T. Skolem showed that any Diophantine equation is equivalent to a system of equations in a larger number of variables of three types: $\zeta\zeta' - \zeta'' = 0$, $\zeta + \zeta' - \zeta'' = 0$ and $\zeta - \zeta' = 0$, as well as one equation of the form $\zeta - v = 0$ ($v \in \mathbb{Z}$), where each variable ζ, ζ', ζ'' either occurs in the notation of the original polynomial $D(\zeta_1, \dots, \zeta_t)$, 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 $\zeta = v$, respectively.

2.1.1. Algorithm for obtaining the Skolem system. We will show how to write the Skolem system using an equation of the form (1). We assume that either all the coefficients of the polynomial $D(\zeta_1, \dots, \zeta_t)$ 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 .

Let us take one of the non-linear monomials on the left side of the considered equation. Let $\zeta\zeta'$ be the product of its two factors. Let us 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 on to the next monomial, and so on. As a result, the left 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 $\zeta = v$, which we will also include in the system. If terms of different signs

were present, then by transforming all the terms on the left 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. *Solvability of an arbitrary Diophantine equation (1) is equivalent to the solvability 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

$$(2) \quad D_1(\zeta'_1, \zeta''_1, \dots, \zeta'_t, \zeta''_t) = 0.$$

Obviously, the solvability of the equation (1) in integers implies the solvability 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 subsection 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 $\zeta = |v|$. \square

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' and making appropriate substitutions of the form ζ_i for ζ' , we achieve that each variable will appear in these equations exactly once. Equations of the form $\zeta' = \zeta_i$ will be added to the S_v system. Next, we renumber the variables in such a way that all e equations of the indicated form take the form

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

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

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

Next, we write the third system, consisting of equations related to the equality of variables. Let us write all equalities of the form $\zeta_i = \zeta_j$, for pairs with different indices $i, j \leq e+d$, which follow from the set of all equalities. Moreover, it suffices to write down a subsystem in which each variable occurs exactly once. Let's renumber all the equations of this subsystem by assigning them the numbers $e+d+1, \dots, e+d+q$, respectively. We have the system of equations

$$(5) \quad P_k \sim \zeta_{i(k)} = \zeta_{j(k)}, i(k) \neq j(k), i(k), j(k) \leq 3(e+d), k = e+d+1, \dots, e+d+q.$$

It remains to write a special equation

$$(6) \quad \zeta_t = |v|.$$

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, $\zeta_1, \dots, \zeta_{3e}, \zeta_{3e+1}, \dots, \zeta_{3(e+d)}$ 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 $\alpha, \beta \in \mathbb{Z}$, $b^\beta a^\alpha = a^\alpha b^\beta c^{\alpha\beta}$.

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*

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

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,

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

□

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

$$\left| \mathbb{H}: b = \begin{array}{ccc} g_1^\zeta & b & g_2^\zeta \\ (ac)^\zeta & b & a^{-\zeta} \end{array} \right|.$$

Table 1.

In the following lemmas, \mathbb{H}^k 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 ($i = 1, \dots, k$) as a_i, b_i, c_i respectively.

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 $b_{1 \rightarrow 3}$ in terms of the generators of M has the form*

$$(9) \quad b_{1 \rightarrow 3} = g_1^\zeta g_2^{\zeta'} g_3^{\zeta''} f_1 g_4^\zeta g_5^{\zeta'} g_6^{\zeta''}$$

provided that $\zeta + \zeta' = \zeta''$. 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 side and g_j ($j = 4, 5, 6$) on the right side of the factor f_1 . For null value of ζ, ζ' or ζ'' , you can also assume that the corresponding generator is located as indicated.

Proof. 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. Then the equality $\zeta + \zeta' = \zeta''$ is necessary and sufficient for the indicated occurrence of the element b in the submonoid M . \square

Let $\mathbb{H}^4 = \mathbb{H}(1) \times \dots \times \mathbb{H}(4)$. The scheme of the exact location of the components of the generators of the submonoid M when expressing the element $b_{1 \rightarrow 3}$ is as follows (empty positions correspond to trivial elements).

	$b_{1 \rightarrow 3} =$	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 $b_{1 \rightarrow 6} = b_1 \cdot \dots \cdot b_6$ in terms of the generators of M has the form*

$$(10) \quad b_{1 \rightarrow 6} = g_1^\zeta g_2^{\zeta'} f_1 g_3^\zeta g_4^{\zeta'} f_2 g_5^\zeta g_6^{\zeta'} f_3 g_7^\zeta g_8^{\zeta'}$$

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 side and g_3, g_4 on the right side of f_1 , g_3, g_4 on the left side and g_5, g_6 on the right side of f_2 , g_5, g_6 on the left side and g_7, g_8 on the right side of f_3 . For null value of ζ or ζ' , you can also assume that the corresponding generator is located as indicated.

Proof. 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 degrees, say ζ and ζ' , respectively. The location of the factors g_i th with respect to f_j th follows from Lemma 2. \square

Let $\mathbb{H}^6 = \mathbb{H}(1) \times \dots \times \mathbb{H}(6)$. The scheme of the exact location of the components of the generators of the submonoid M when expressing the element $b_{1 \rightarrow 6}$ is as

follows (empty positions correspond to trivial elements).

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

Table 3.

Lemma 5. Consider a group \mathbb{H}^8 in which the first 6 components form the group \mathbb{H}^6 from Lemma 4. Let M be a submonoid of \mathbb{H}^8 generated by $g_1 = a_1 c_1 a_7, g_2 = a_2 c_2, g_3 = a_1^{-1} a_3 c_3, g_4 = a_2^{-1} a_4 c_4 b_7, f_1 = b_1 b_2, f_2 = b_3 b_4, g_5 = a_3^{-1} a_5 c_5 a_7^{-1}, g_6 = a_4^{-1} a_6 c_6, f_3, g_7 = a_5^{-1}, g_8 = a_6^{-1} b_7^{-1}$ and $g_9 = a_8 c_6 c_7^{-1}, f_4 = b_8, g_{10} = a_8^{-1}$. Then the representation of $b_{1 \rightarrow 6} b_8$ in terms of the generators of M has the form

$$(11) \quad b_{1 \rightarrow 6} b_8 = g_1^\zeta g_2^{\zeta'} f_1 g_3^\zeta g_4^{\zeta'} f_2 g_5^\zeta g_6^{\zeta'} f_3 g_7^\zeta g_8^{\zeta'} g_9^{\zeta''} f_4 g_{10}^{\zeta''}.$$

The last three generators commute with each of the first 10 generators. For given positive ζ, ζ', ζ'' the equality $\zeta \cdot \zeta' = \zeta''$ is necessary and sufficient for the indicated occurrence of the element $b_{1 \rightarrow 6} b_8$ in the submonoid M . For null value of ζ, ζ' or ζ'' , you can also assume that the corresponding generator is located as indicated.

Proof. It is clear that the configuration of the factors in (10) is preserved for their counterparts in (11). Thus, the 7th component of the product of these analogs in (11) is equal to $c_1^{\zeta_1 \zeta_2}$. This value must cancel out due to the $c_1^{-\zeta_3}$ multiplier present in the g_9 exponent in the representation (11). \square

Let $\mathbb{H}^8 = \mathbb{H}(1) \times \dots \times \mathbb{H}(8)$. The scheme of the exact location of the components of the generators of the submonoid M when expressing the element $b_{1 \rightarrow 6} b_8$ is as follows (empty positions correspond to trivial elements).

$$\mathbb{H}^8 : b_{1 \rightarrow 6} b_8 =$$

$$\left| \begin{array}{l} b_{1 \rightarrow 6} b_8 = \\ \mathbb{H}(1) : b_1 = \\ \mathbb{H}(2) : b_2 = \\ \mathbb{H}(3) : b_3 = \\ \mathbb{H}(4) : b_4 = \\ \mathbb{H}(5) : b_5 = \\ \mathbb{H}(6) : b_6 = \\ \mathbb{H}(7) : 1 = \\ \mathbb{H}(8) : b_8 = \end{array} \begin{array}{cccccccc} g_1^\zeta g_2^{\zeta'} & f_1 & g_3^\zeta g_4^{\zeta'} & f_2 & g_5^\zeta g_6^{\zeta'} & f_3 & g_7^\zeta g_8^{\zeta'} & g_9^{\zeta''} & f_4 & g_{10}^{\zeta''} \\ a_1^\zeta c_1^{\zeta'} & b_1 & a_1^{-\zeta} & & & & & & & \\ a_2^{\zeta'} c_2^{\zeta'} & b_2 & a_2^{-\zeta'} & & & & & & & \\ a_3^\zeta c_3^\zeta & & b_3 & a_3^{-\zeta} & & & & & & \\ a_4^{\zeta'} c_4^{\zeta'} & & b_4 & a_4^{-\zeta'} & & & & & & \\ & & & a_5^\zeta c_5^\zeta & b_5 & a_5^{-\zeta} & & & & \\ & & & a_6^{\zeta'} c_6^{\zeta'} & b_6 & a_6^{-\zeta'} & & & & \\ & & & a_7^{\zeta'} & & a_7^{-\zeta} & b_7^{-\zeta'} & c_7^{\zeta''} & & \\ & & & & & & & a_8^{\zeta''} c_8^{\zeta''} & b_8 & a_8^{-\zeta''} \end{array} \right|$$

Table 4.

4. CHOOSING A DIRECT POWER OF THE HEISENBERG GROUP AND
CONSTRUCTING A SUBMONOID IN IT FOR WHICH THE MEMBERSHIP PROBLEM
IS EQUIVALENT TO THE SOLVABILITY OF THE GIVEN DIOPHANTINE EQUATION

First, a Diophantine equation (1) is taken. Then the equivalent nonnegative Skolem system $S(v)$ 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_v we associate the group $\tilde{\mathbb{H}} = \mathbb{H}^{8e+4d+q+1}$. We construct a submonoid $M = M$ of the group $\tilde{\mathbb{H}}$ by defining its generating elements g_i for $i = 1, \dots, 10e, 10e + 1, \dots, 10e + 6d$ and f_j for $j = 1, \dots, 4e, 4e + 1, \dots, 4e + d$ in accordance with the lemmas 3 and 5. The form of these generators are defined below.

Construction of submonoid generators associated with the system (3).

Consider first the equations of system (3). For each of these e equations, we sequentially define the corresponding block $\mathbb{H}(i) = \mathbb{H}^{8e}, i = 1, \dots, e$. Consistently compose the group

$$(12) \quad \mathbb{H}^{8e} = \prod_{i=1}^e \mathbb{H}(i)$$

from the obtained blocks. We assume that the group \mathbb{H}^{8e} consists of the first $8e$ factors of the group $\tilde{\mathbb{H}}$. Let \bar{M}_1 be the projection of M into \mathbb{H}^{8e} . We define successively $14e$ projections \bar{g}_i ($i = 1, \dots, 10e$), \bar{f}_j , ($j = 1, \dots, 4e$) of the generators g_i ($i = 1, \dots, 10e$), f_j ($j = 1, \dots, 4e$) of the submonoid M into the group \mathbb{H}^{8e} with 14 generators for each block (10 generators \bar{g}_i and 4 generators \bar{f}_j). All these projections generate \bar{M}_1 , the projection of M into \mathbb{H}^{8e} . The remaining generators of M have trivial projections.

The generators of the block $\mathbb{H}(1)$ are constructed in exactly the same way as in Lemma 5. They are $\bar{g}_1, \dots, \bar{g}_{10}$ and $\bar{f}_1, \dots, \bar{f}_4$. They are considered as elements of the group \mathbb{H}^{8e} . All their other components in \mathbb{H}^{8e} are trivial. The generating elements of the remaining components are determined in the same way. The generators of the submonoid \bar{M}_1 in the block $\mathbb{H}(i)$ (for simplicity we denote $t_i = 10(i - 1)$ and $s_i = 4(i - 1)$) are:

$$(13) \quad \begin{aligned} \bar{g}_{1+t_i} &= a_{1+t_i} c_{1+t_i} a_{7+t_i}, \bar{g}_{2+t_i} = a_{2+t_i} c_{2+t_i}, \bar{g}_{3+t_i} = a_{1+t_i}^{-1} a_{3+t_i} c_{3+t_i}, \\ \bar{g}_{4+t_i} &= a_{2+t_i}^{-1} a_{4+t_i} c_{4+t_i} b_{7+t_i}, \bar{f}_{1+s_i} = b_{1+s_i} b_{2+s_i}, \\ \bar{f}_{2+s_i} &= b_{3+s_i} b_{4+s_i}, \bar{g}_{5+t_i} = a_{3+t_i}^{-1} a_{5+t_i} c_{5+t_i} a_{7+t_i}^{-1}, \bar{g}_{6+t_i} = a_{4+t_i}^{-1} a_{6+t_i} c_{6+t_i}, \\ \bar{f}_{3+s_i} &= b_{5+s_i} b_{6+s_i}, \bar{g}_{7+t_i} = a_{5+t_i}^{-1}, \bar{g}_{8+t_i} = a_{6+t_i}^{-1} b_{7+t_i}^{-1}, \\ \bar{g}_9 &= a_{8+t_i} c_{6+t_i} c_{7+t_i}^{-1}, \bar{f}_{4+s_i} = b_{8+s_i}, \bar{g}_{10+t_i} = a_{8+t_i}^{-1}. \end{aligned}$$

The analogue of the formula (11) for the block $\mathbb{H}(i)$ is the following formula:

$$(14) \quad \begin{aligned} b_{(1+8(i-1)) \rightarrow (6+8(i-1))} b_{8i} &= \bar{g}_{1+t_i}^{\zeta_{1+t_i}} \bar{g}_{2+t_i}^{\zeta_{2+t_i}}. \\ \bar{f}_{1+s_i} \bar{g}_{3+t_i}^{\zeta_{1+t_i}} \bar{g}_{4+t_i}^{\zeta_{2+t_i}} \bar{f}_{2+s_i} \bar{g}_{5+t_i}^{\zeta_{1+t_i}} \bar{g}_{6+t_i}^{\zeta_{2+t_i}} & \\ \bar{f}_{3+s_i} \bar{g}_{7+t_i}^{\zeta_{1+t_i}} \bar{g}_{8+t_i}^{\zeta_{2+t_i}} \bar{g}_{9+t_i}^{\zeta_{3+t_i}} \bar{f}_{4+s_i} \bar{g}_{10+t_i}^{\zeta_{3+t_i}} & \end{aligned}$$

Just as in Lemma 5, we can conclude that the element $b(1) = b_{1 \rightarrow 6} b_8 \cdot b_{9 \rightarrow 14} b_{16} \cdot \dots \cdot b_{(8e-7) \rightarrow (8e-2)} b_{8e}$ belongs to \bar{M}_1 if and only if all the relations of system (4) are satisfied.

Construction of submonoid generators associated with the system (4).

Consider the equations of system (4). For each of these d equations, we sequentially define the corresponding block $\mathbb{H}(j) = \mathbb{H}^4$, $j = e+1, \dots, e+d$. Consistently compose the group

$$(15) \quad \mathbb{H}^{4d} = \prod_{j=1}^d \mathbb{H}(e+j)$$

from the obtained blocks. We assume that the group \mathbb{H}^{4d} consists of the $4d$ factors of the group $\tilde{\mathbb{H}}$ following after the previously considered factors of \mathbb{H}^{8e} of the group $\tilde{\mathbb{H}}$. Now we consider the group $\mathbb{H}^{8e} \times \mathbb{H}^{4d}$, which consists of the first $8e + 4d$ factors \mathbb{H} of the group $\tilde{\mathbb{H}}$.

Let M_2 be the projection of M into \mathbb{H}^{4d} . The projections of the generators of the submonoid M considered above into the components \mathbb{H}^{4d} are trivial. We define successively $7d$ projections \bar{g}_i, \bar{f}_j of the generators g_i, f_j for $i = 10e+1, \dots, 10e+6d$ and $j = 4e+1, \dots, 4e+d$ of M (6 projections \bar{g}_i and 1 projection of \bar{f}_j for each block \mathbb{H}^4) into \mathbb{H}^{4d} which are the generators of the submonoid \bar{M}_2 of \mathbb{H}^{4d} . Recall that the projections of these generators into \mathbb{H}^{8e} are trivial. Therefore, the projection $\bar{M}_{1,2}$ of the submonoid M into the group \mathbb{H}^{8e+4d} coincides with $\bar{M}_1 \bar{M}_2$.

The generators of the block $\mathbb{H}(e+j)$, $j = 1, \dots, d$, are constructed in exactly the same way as in Lemma 3. The generators of the submonoid \bar{M}_2 in the block $\mathbb{H}(e+j)$ are (for simplicity we denote $r_j = 4(j-1)$):

$$\bar{g}_{10e+1+r_j} = a_{10e+1+r_j} c_{10e+1+r_j} c_{10e+4+r_j}, \bar{g}_{10e+2+r_j} = a_{10e+2+r_j} c_{10e+2+r_j} c_{10e+4+r_j},$$

$$(16) \quad \bar{g}_{10e+3+r_j} = a_{10e+3+r_j} c_{10e+3+r_j} c_{10e+4+r_j}^{-1}, \bar{g}_{10e+4+r_j} = a_{10e+1+r_j}^{-1},$$

$$\bar{g}_{10e+5+r_j} = a_{10e+2+r_j}^{-1}, \bar{g}_{10e+6+r_j} = a_{10e+3+r_j}^{-1}, \bar{f}_{4e+j} = b_{4e+1+j} b_{4e+2+j} b_{4e+3+j}$$

with trivial other components.

The analogue of the formula (9) for the block $\mathbb{H}(i+j)$ is the following formula:

$$(17) \quad b_{e+1+r_j \rightarrow e+3+r_j} = \bar{g}_{e+1+r_j}^{\zeta_{e+1+r_j}} \bar{g}_{e+2+r_j}^{\zeta_{e+2+r_j}} \bar{g}_{e+3+r_j}^{\zeta_{e+3+r_j}} \bar{f}_{e+1+r_j} \bar{g}_{e+4+r_j}^{\zeta_{e+1+r_j}} \bar{g}_{e+5+r_j}^{\zeta_{e+2+r_j}} \bar{g}_{e+6+r_j}^{\zeta_{e+3+r_j}}.$$

Just as in Lemma 3, we can conclude that the element $b(2) = b_{(10e+1) \rightarrow (10e+3)} \cdot b_{(10e+5) \rightarrow (10e+7)} \cdot \dots \cdot b_{10e+4(d-1)+1 \rightarrow 10e+4d-1}$ belongs to \bar{M}_2 if and only if all the relations of system (4) are satisfied.

Thus, we have defined the projections \bar{g}_i, \bar{f}_j of all $14e + 7d$ generating elements g_i, f_j of the submonoid M into the product $\mathbb{H}^{8e} \times \mathbb{H}^{4d}$ of the first $8e + 4d$ factors \mathbb{H} of the group $\tilde{\mathbb{H}}$.

Summarizing the above, we conclude that the element $b(1)b(2)$ belongs to the submonoid $\bar{M}_{1,2}$ if and only if the joint system of equations (3-4) is solvable.

Construction of submonoid generators associated with the systems (5) and (6). Since all the variables of the systems (3) and (5) are different, both these systems are decidable together. It remains to take into account the equalities between these variables.

The difference between this construction and the above constructions related to systems (3) and (4) is that the considered direct product of the blocks of the group \mathbb{H} is not only expanded by new factors \mathbb{H} , but also the already defined projections

of the generators of the submonoid M are supplemented with new components. In other words, these generators are modified by the added components.

Let us add to the constructed group \mathbb{H}^{8e+4d} by $q + 1$ factors \bar{H} and get the group $\tilde{\mathbb{H}}$, where q is the number of equations in the system (5). Let's assign to these components the numbers $8e + 4d + i$ for $i = 1, \dots, q$ and $8e + 4d + q + 1$ relatively.

Then for any equation P_{e+d+k} ($k = 1, \dots, q$) of the form $\zeta_{i(k)} = \zeta_{j(k)}$ from (5) we add some elements to the $8e + 4d + kt$ th component of $\tilde{\mathbb{H}}$ as follows.

First, for each $k = 1, \dots, q$ we find among the representations (14) and (17) one of the generating elements g of the M submodule whose projection exponent is equal to $\zeta_{i(k)}$. Add the element $c_{8e+4d+k}$ to the component $8e + 4d + k$ of g . Then we will perform a similar operation corresponding to the exponent $\zeta_{j(k)}$. This component will be trivial in the considered product of generating elements of the submonoid M if and only if $\zeta_{i(k)} = \zeta_{j(k)}$.

Then for equation (6), we find among the representations (14) and (17) one of the generating elements g of the M submodule whose projection exponent is equal to ζ_t and add the element $c_{8e+4d+q+1}$ to the $8e + 4d + q + 1$ th component of g . Note, that this component is equal to $c_{8e+4d+q+1}^{\zeta_t}$ in the considered product of the generators of M , i.e., this product is equal to $b(1)b(2)c_{8e+4d+q+1}^{|\zeta_t|}$.

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

5. MAIN RESULTS

In this section we give formal proofs of the main results.

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

Proof. Suppose that the equation (1) has a solution in integers. From the equation (1), we construct a nonnegative Skolem system S_v equivalent to it, as explained in the point 1.1.1 and Lemma 1. Suppose that $\zeta_1, \dots, \zeta_{3e+3d}$ is an integer solution to the system S_v . In this case equations (3–6) turn into equalities.

Define $n = 8e + 4d + q + 1$ and the group $\tilde{\mathbb{H}} = \mathbb{H}^n$. Construct the generating elements g_i for $i = 1, \dots, 10e, 10e + 1, \dots, 10e + 6d$ and f_j for $j = 1, \dots, 4e, 4e + 1, \dots, 4e + d$ of the submonoid M of the group $\tilde{\mathbb{H}}$, as described in the section 4. Define the element

$$(18) \quad g(v) = b(1)b(2)c_{8e+4d+q+1}^{|\zeta_t|},$$

where $b(1) = b_{1 \rightarrow 6} b_8 \cdot b_{9 \rightarrow 14} b_{16} \cdot \dots \cdot b_{(8e-7) \rightarrow (8e-2)} b_{8e}$, $b(2) = b_{(10e+1) \rightarrow (10e+3)} \cdot b_{(10e+5) \rightarrow (10e+7)} \cdot \dots \cdot b_{10e+4(d-1)+1 \rightarrow 10e+4d-1}$.

The section 4 shows that the element $b(1)b(2)$ is represented in a certain way as the product of the projections of the generating elements of the submonoid M onto the group \mathbb{H}^{8e+4d} (formulas (14) and (17)). Consider the corresponding product of generating elements of the submonoid M . It follows from their construction and the fulfillment of the equalities (5) that all components $8e + 4d + k$ ($k = 1, \dots, q$) of

this product are trivial. The $(8e + 4d + q + 1)$ th component in view of the equality (6) is equal to $c_{8e+4d+q+1}^{|v|}$. Hence, the element $g(v)$ belongs to the submonoid M .

Suppose now that the element $g(v)$ belongs to the submonoid M . Its projection $b(1)b(2)$ is represented in a certain way as a product of the projections of generating elements of the submonoid M only if the equalities (3) and (4) hold (Lemmas 3 and 5, formulas (14) and (17)). This product completely determines the product of generators of the submonoid M . In this case, the components with numbers $8e + 4d + k$ ($k = 1, \dots, q$) must be trivial, which corresponds to the fulfillment of the equalities (5). The $(8e + 4d + q + 1)$ th component must be equal to $c_{8e+4d+q+1}^{|v|}$, which means that (6) is satisfied. Consequently, the exponents $\zeta_1, \dots, \zeta_{3(e+d)}$, with which the generators of the submonoid M enter the representation of the element $g(v)$, are the solution of the system S_v . \square

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 [7]–[10]) proved that such an algorithm does not exist. In addition, he established that there exists a Diophantine polynomial $D_0(\zeta_1, \dots, \zeta_t)$ with a zero constant term such that there is no algorithm that determines the solvability of equations of the form

$$(19) \quad D_0(\zeta_1, \dots, \zeta_t) = v, \quad v \in \mathbb{Z}.$$

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 (19) with a fixed left-hand side and parameter v 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 M with an unsolvable membership problem.*

Proof. First, an equation of the form (19), which is unsolvable in integers, is taken. Then the equivalent nonnegative Skolem system $S(v)$ is constructed from this equation. The rest of the proof completely repeats the proof of the Theorem 1. Variations of the parameter v in the equation (19) correspond to variations of the element $g(v)$. The submonoid M does not change. An element $g(v)$ belongs to the submonoid M if and only if the system S_v is solvable in nonnegative integers. This is equivalent to saying that the equation (19) with this parameter is solvable in integers. This implies the assertion of the theorem. \square

Note that the existence of a finitely generated submonoid with an unsolvable occurrence 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 an undecidable membership problem. Then the free nilpotent group $N_{k,c}$ of rank k of the class c contains a finitely generated submonoid \widetilde{M} with an undecidable membership problem.*

Proof. Consider the natural homomorphism $\mu : N_{k,c} \rightarrow N$. 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 M is generated by elements g_1, \dots, 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 $\ker(\mu) = \text{gp}(f_1, \dots, f_t)$. Then the submonoid \widetilde{M} is generated by the elements $\tilde{g}_1, \dots, \tilde{g}_l, f_1^{\pm 1}, \dots, f_t^{\pm 1}$. \square

It follows from the Theorem 2 and the Proposition 1 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] Yu. G. Kleiman, *Identities and some algorithmic problems in groups*, Dokl. Akad. Nauk SSSR, **244**:4 (1979), 814–818.
- [4] 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.
- [5] 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
- [6] A.I. Maltsev, *Homomorphisms onto finite groups*, Ivanov Gos. Ped. Inst. Uchen. Zap., **18** (1958), 49–60.
- [7] Yu. V. Matiyasevich, *The Diophantineness of enumerable set*, Soviet Mathematics, **11**:2 (1970), 354–357.
- [8] Yu. V. Matiyasevich, *Diophantine representation of enumerable predicate*, Izvestiya Math., **5**:1 (1971), 1–28. Zbl 0219.02035
- [9] 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.
- [10] Y. Matijasevic, J. Robinson, *Reduction of Diophantine equation to one in 13 unknowns*, Acta Arith., **27** (1975), 521–553.
- [11] G.A. Noskov, V.N. Remeslennikov, V.A. Roman'kov, *Infinite groups*, J. Sov. Math., **18**:5 (1982), 669–735. Zbl 0479.20001
- [12] 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
- [13] N.N. Repin, *The solvability problem for equations in one unknown in nilpotent groups*, Izvestiya Math., **25**:3 (1985), 601–618.
- [14] V.A. Roman'kov, *Unsolvability of the endomorphic reducibility problem in free nilpotent groups and in free rings*, Algebra and Logic, **16**:4 (1977), 310–320.
- [15] V.A. Roman'kov, *Equations in free metabelian groups*, Siberian Math. J., **20**:3 (1979), 469–471.
- [16] V.A. Roman'kov, *Diophantine questions in the class of finitely generated nilpotent groups*, J. of Group Theory, **19**:3 (2016), 497–514.
- [17] V.A. Roman'kov, *Algorithmic theory of solvable groups*, Prikl. Diskr. Mat., **52** (2021), 16–64. Zbl 7382418
- [18] V.A. Roman'kov, *Two problems for solvable and nilpotent groups*, Algebra and Logic, **59**:6 (2021), 483–492. Zbl 7350231

- [19] 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.
- [20] 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).
- [21] 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