The Diophantine Problem in Some Metabelian Groups

Olga Kharlampovich*, Laura López†, Alexei Myasnikov‡

Abstract

In this paper we show that the Diophantine problem for quadratic equations in Baumslag-Solitar groups $BS(1,k)$ and in wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, is decidable. We show also that one can decide if there are non-trivial solutions of systems of equations without coefficients in these groups and give some sort of description of solutions. Previously we stated that there is an algorithm that given a finite system of equations with constants in such a group decides whether or not the system has a solution in the group, this proof, unfortunately, has a gap.

1 Introduction

The problem of solving equations in various classes of groups and monoids has been an active research field for many years now. The first general results on equations in groups appeared in the 1960's in the works of Lyndon [11] and Malcev [12]. In the 1970's Makanin [13, 14] proved the solvability of (systems of) equations for free monoids and free groups. Makanin's decidability results have been extended to hyperbolic groups and right-angled Artin groups [3], and it was shown that certain group operations (graph products [2], HNN-extensions and amalgamated products over finite groups) preserve decidability [10]. Moreover, a significant progress concerning the computational complexity and the structure of solution sets have been obtained in recent years. On the negative side, by the Ershov-Romanovskii-Noskov result the first-order theory of a finitely generated solvable group is decidable if and only if the group is virtually abelian. The corresponding problem has been posed in [9]. Ershov proved this statement [5] in the nilpotent case, Romanovskii [19] generalized it to the polycyclic case, and finally, Noskov [15] established the most general statement for the case of a finitely generated solvable group. Denote by $\mathcal{EP}_1$ the problem of solvability of one equation. Roman'kov showed that $\mathcal{EP}_1$ is undecidable even for the subclass of all split equations of the form $w(x_1, \dots, x_n) = g$, where $w(x_1, \dots, x_n)$ is a

*Hunter College and Graduate Center, CUNY
†Graduate Center, CUNY
‡Stevens Institute

coefficient-free word and g is an element of the underlying group G that is a free nilpotent of class ≥ 9 [17] (this bound was later reduced to ≥ 4 in [18]) or G is a free metabelian non-abelian group [18]. In [4] the authors proved that $\mathcal{EP}_1$ is decidable in the Heisenberg group that is free nilpotent of rank 2 and class 2. But the Diophantine problem (denoted by $\mathcal{EP}$ in [4]) is undecidable in any non-abelian free nilpotent group.

In this paper we show that the Diophantine problem for quadratic equations in solvable Baumslag-Solitar groups $BS(1,k)$ and in wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, is decidable, i.e. there is an algorithm that given a finite quadratic system of equations with constants in such a group decides whether or not the system has a solution in the group. We show also that one can decide if there are non-trivial solutions of systems of equations without coefficients in these groups. In the published version of this paper we stated that there is an algorithm that given a finite system of equations with constants in such a group decides whether or not the system has a solution in the group, this proof, unfortunately, has a gap.

The metabelian Baumslag-Solitar groups are defined by one-relator presentations $BS(1,k) = \langle a, b \mid b^{-1}ab = a^k \rangle$, where $k \in \mathbb{N}$. If $k = 1$ then $BS(1,1)$ is free abelian of rank 2, so the Diophantine problem in this group is decidable (it reduces to solving finite systems of linear equations over the ring of integers $\mathbb{Z}$). Furthermore, the first-order theory of $BS(1,1)$ is also decidable [21]. However, if $k \geq 2$ then $BS(1,k)$ is metabelain which is not virtually abelian, so the first-order theory of $BS(1,k)$ is undecidable by [15]. As we mentioned above, in free metabelian non-abelian groups equations are undecidable [18]. In fact, in a finitely generated metabelian group G given by a finite presentation in the variety $\mathcal{M}_2$ of metabelian groups, the Diophantine problem is undecidable asymptotically almost surely if the deficiency of the presentation is at least 2 [6].

In general, if the quotient $G/\gamma_3(G)$ of a finitely generated metabelian group G by its third term of the lower central series is a non-virtually abelian nilpotent group, then the decidability of the Diophantine problem in G would imply decidability of the Diophantine problem for some finitely generated ring of algebraic integers O_G associated with $G/\gamma_3(G)$. The latter seems unlikely, since there is a well-known conjecture in number theory (see, for example, [1, 16]) that states that the Diophantine problem in rings of algebraic integers is undecidable. The discussion above shows that finitely generated metabelian groups G with virtually abelian quotients $G/\gamma_3(G)$ present an especially interesting case in the study of equations in metabelian groups. The groups $BS(1,k)$ and wreath products $A \wr \mathbb{Z}$, where A is a finitely generated abelian group and $\mathbb{Z}$ is an infinite cyclic group, are the typical examples of such groups. This gives also a new look at one-relator groups. The groups $BS(1,k)$, $k \geq 2$, were until recently the only known examples of one-relator groups with undecidable first-order theory. Recently, we were able to show (still unpublished) that any one-relator group containing non-abelian group $BS(1,k)$ has undecidable first-order theory. However, it is quite possible that equations in such groups are still decidable.

2 Equations in $BS(1,k)$

Our first main result is

Theorem 1. *Quadratic equations in $BS(1,k)$ are decidable. There is also an algorithm to decide if there is a non-trivial solution of a system of equations without coefficients.*

To prove the theorem we have to construct an algorithm that decides whether the set of formulas of the form $\exists \bar{x} \wedge_{i=1}^{s} t_i(\bar{x}, a, b) = 1$ is decidable, where $t_i(\bar{x}, a, b)$ is a group word in the alphabet $\bar{x}, a, b$. Recall that the group $BS(1,k)$ is isomorphic to the group $\mathbb{Z}[1/k] \rtimes \mathbb{Z}$, where $\mathbb{Z}[1/k] \cong ncl(a)$ and $\mathbb{Z} \cong \langle b \rangle$, where

$$\mathbb{Z}[1/k] = \{zk^{-i}, z \in \mathbb{Z}, i \in \mathbb{N}\}$$

and the action of $\langle b \rangle$ is given by $b^{-1}ub = u^k$. Thus, we can think of elements in $BS(1,k)$ as pairs (zk^{-i}, r) where $z, r, i \in \mathbb{Z}$. The product is defined as

$$(z_1k^{-i_1}, r_1)(z_2k^{-i_2}, r_2) = (z_1k^{-i_1} + z_2k^{-(i_2+r_1)}, r_1 + r_2).$$

The inverse of an element (zk^{-y}, r) is $(-zk^{-(y-r)}, -r)$

The following lemma reduces systems of equations in $BS(1,k)$ to systems of equations in $\mathbb{Z}$.

Lemma 1. *Any finite system of equations in $BS(1,k)$ is equivalent to a finite system of equations of the form*

$$\sum_i z_i k^{-y_i} (\sum_j \pm k^{\tau_{ij}(\bar{r})}) - \sum_t \gamma_t k^{\tau_t(\bar{r})} = 0 \tag{1}$$

and

$$\sum \beta_j r_j = \delta. \tag{2}$$

where $\tau_t(\bar{r}), \tau_{ij}(\bar{r}) = \sum_q \alpha_q r_q + c_q$ and where $\alpha_q, c_q, \delta, \gamma_t, \beta_j \in \mathbb{Z}$, and y_i, z_i, r_i, are variables.

The product $z_i k^{-y_i}$ can be also considered as one variable in $\mathbb{Z}[1/k]$.

Proof. Note that

$$(z_1k^{-y_1}, r_1) \cdot (z_2k^{-y_2}, r_2) \cdots (z_nk^{-y_n}, r_n) =$$
$$(z_1k^{-y_1} + z_2k^{-(y_2+r_1)} + ... + z_nk^{-(y_n+r_1+...+r_{n-1})}, r_1 + ... + r_n)$$

The system of equations in the first and second component corresponds to a system of equations of the form (1) and (2), respectively.

□

To solve a system of equations in $BS(1,k)$, we begin by solving system (2). This system is just a linear system of equations $AX = B$ with integer coefficients, where $X = (r_1, \ldots, r_n)^T$ and A is the matrix of the system. Using

integral elementary column operations on A and row operations on $(A|B)$ we can obtain an equivalent system $\bar{A}\bar{X} = \bar{B}$ such that $\bar{A}$ has a diagonal form. This is Smith normal form. Column operations on A correspond to change of variables. Row operations on $(A|B)$ correspond to transformations of the system of equations into an equivalent system. If the system $\bar{A}\bar{X} = \bar{B}$ does not have a solution, then the corresponding system of equations in the group does not have a solution. If the system $\bar{A}\bar{X} = \bar{B}$ is solvable, then we change variables X to $\bar{X}$. Some of the new variables $\bar{X}$ will have fixed integer values and some will be arbitrary integers. Substitute those $\bar{X}$'s into system (1). We only have to check that there exist integer solutions $Z = \{z_1, \dots, z_n\}$, $Y = \{y_1, \dots, y_n\}$ and remaining $\bar{X}$ that we denote $\hat{X} = \{r_{i_1} \dots r_{i_m}\}$.

We say that a system of equations $S(X) = 0$ with variables X is equivalent to a disjunction of systems $S_1(X) = 0, \dots, S_m(X) = 0$ if every solution of $S(X) = 1$ is a solution of one of $S_i(X) = 0, i = 1, \dots, m$ and every solution of $S_i(X) = 0$ is a solution of $S(X) = 0$. One can consider system (1) as a linear system with variables $z_i k^{-y_i}$, and linear combinations of exponential functions as coefficients (which contain variables $\hat{X}$). It can be transformed using row operations to an equivalent disjunction of triangular like systems (with respect to variables $z_s k^{-y_s}$, $s = 1, \dots, q$) of the following form:

$$z_s k^{-y_s}(\sum_j \delta_{sj} k^{\tau_{sj}(\bar{r})}) = \sum_{i>q} z_i k^{-y_i}(\sum_j \delta_{ij} k^{\sigma_{ij}(\bar{r})}) + \sum_t \gamma_t k^{\tau_t(\bar{r})}, s = 1, \dots, q, \tag{3}$$

$$\sum_j a_j k^{\phi_j(\bar{r})} = 0 \text{ (system of such equations).} \tag{4}$$

where $\delta_{sj}, \delta_{ij}, \gamma_t, a_j \in \mathbb{Z}$ and $\tau_{sj}, \sigma_{ij}, \tau_t, \phi_j$ are linear combinations of elements in $\hat{X}$ and constants. We will get a disjunction of systems because when multiplying equations by some coefficient we have to consider separately the case when this coefficient is zero.

Now we have to solve systems (3) and (4). We will first find all solutions of system (4). Semenov's ideas in [20] (where he proved that the theory of $\langle \mathbb{Z}, +, k^x \rangle$ is decidable) can be used to prove the following lemma.

Lemma 2. *Any system of equations over $\mathbb{Z}$ of the form*

$$F(\bar{y}) = \sum_j \beta_j k^{y_j} + C = 0, \tag{5}$$

where $\beta_j \in \mathbb{Z}$, $k \in \mathbb{N}, k > 1$, with variables $\bar{y} = (y_1, ..., y_n)$, is equivalent to a disjunction of linear systems of equations over $\mathbb{Z}$.

Proof. Let $\bar{y} = (y_1, \dots, y_n)$ and let $\lambda : \{y_1, \dots, y_n\} \to \{+, -\}$ be a map that assigns to each variable a positive or negative sign (the agreement will be that zero has a positive sign). System (5) over $\mathbb{Z}$ is equivalent to a disjunction of 2^n systems each with an assignment λ. Now we fix one of these systems and we show how to describe all solutions.

We begin by rewriting each equation so that all variables are positive. We may do this by substituting in each equation $-y_i$ for y_i for each y_i that has a negative assignment. Then we multiply each equation by $k^{y_{i_1}+\ldots+y_{i_s}}$, where $y_{i_1}, \ldots, y_{i_s}$ are all the variables whose signs were changed. For instance, suppose we have an equation $k^{y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 < 0, y_2 \geq 0, y_3 \geq 0$. Then we rewrite it as $k^{-y_1} - k^{y_2} + k^{y_3} + c = 0$ with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$ and multiply the equation by k^{y_1}. We then obtain the equation

$$1 - k^{y_1+y_2} + k^{y_1+y_3} + ck^{y_1} = 0$$

with assignment $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0$. We now obtain a system over $\mathbb{N}$ of the form

$$\sum_i \beta_i k^{\sum_j y_{ij}} + C = 0$$

Next, we substitute all sums in exponents of k by new variables to obtain a system of equations over $\mathbb{N}$ of the form

$$F'(\bar{y}) = \sum_i \beta_i k^{\hat{y}_i} + C = 0 \tag{6}$$

Claim: A finite system of equations in the form (6) is equivalent to a disjunction of systems of linear equations of the form $\{\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_{s-1} = \hat{y}_s + c_s\}$.

Proof. Denote the new variables as $\bar{y}' = (\hat{y}_1, \ldots \hat{y}_m)$. We begin by showing that for each i, there is a $\Delta_i \in \mathbb{N}$ such that system (6) does not have a solution if $\hat{y}_i > \hat{y}_j + \Delta_i$ for all $j \neq i$.

Fix i. We can rewrite each equation in the system in the form $k^{\hat{y}} + \sum_i \gamma_i k^{\hat{x}_i} = \sum_j \delta_j k^{\hat{z}_j} + C$, where all γ_i, δ_j are positive integers, $\hat{y} = \hat{y}_i$ and $\hat{x}_i, \hat{z}_j$ are all variables in $\bar{y}' - \hat{y}_i$. For each equation, let $\Delta > \log_k(\sum_j \delta_j + C)$ if $C \geq 0$ and $\Delta > \log_k(\sum_j \delta_j)$ if $C < 0$, and $\hat{y} > \hat{x}_i + \Delta$ and $\hat{y} > \hat{z}_j + \Delta$ for all i, j. Then $k^{\hat{y}} > k^{\Delta} k^{\hat{z}_j} > (\sum_j \delta_j + C) k^{\hat{z}_j}$ for all j. Thus, the right side of the equation will always be smaller than the left side, and the equation has no solution. Thus, we can take Δ_i to be the smallest such Δ.

So we have shown that for all variables $\hat{y}_i$, if F' (or a finite system of equations where each equation has form F') has a solution then there is a $j \neq i$ such that $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Now consider a finite graph $\mathcal{G}$ with n vertices labeled $\hat{y}_1, \ldots, \hat{y}_m$ and directed edges from $\hat{y}_i$ to $\hat{y}_j$ whenever $\hat{y}_i \leq \hat{y}_j + \Delta_i$. Note that each vertex must be the initial vertex of some edge and thus the graph must contain a cycle in every connected component. Suppose there is a cycle $\hat{y}_{i_1}, \ldots, \hat{y}_{i_s} = \hat{y}_{i_1}$, $s \leq m + 1$. Then

$$\hat{y}_{i_1} \leq \hat{y}_{i_2} + \Delta_{i_1} \leq \hat{y}_{i_3} + \Delta_{i_2} + \Delta_{i_1} \leq \ldots \leq \hat{y}_{i_s} + \Delta_{i_{(s-1)}} + \ldots + \Delta_{i_1}$$

$$= \hat{y}_{i_1} + \Delta_{i_{(s-1)}} + \ldots + \Delta_{i_1}$$

Therefore for any $2 \leq j \leq s-1$, we have that

$$\hat{y}_{i_1} - \sum_{t=1}^{j-1} \Delta_{i_t} \leq \hat{y}_{i_j} \leq \hat{y}_{i_1} + \sum_{t=j}^{s-1} \Delta_{i_t}$$

Therefore, the value of any $\hat{y}_{i_j}$ with $2 \leq j \leq s-1$ is bounded by the value of $\hat{y}_{i_1}$.

Fix a y_{i_j} and let $\Delta_{j_1} = \sum_{t=1}^{j-1} \Delta_{i_t}$ and $\Delta_{j_2} = \sum_{t=j}^{m-1} \Delta_{i_t}$. Then we may replace the equation $F'(\bar{y})$ by a disjunction of equations $G(\bar{y} \backslash \hat{y}_{i_j})$ where G is the same as the formula F', but $\hat{y}_{i_j}$ is replaced by $\hat{y}_{i_1} - \Delta_{j_1}$ in one equation, $y_{i_1} - \Delta_{j_1} + 1$ in the next, and so on until $y_{i_1} + \Delta_{j_2}$.

Now we may eliminate variables from each equation in m variables inductively, obtaining at each step a new disjunction consisting of a system of equations in less variables and a set of linear equations of the form $\hat{y}_i = \hat{y}_j + c_i$ which we use to eliminate one variable. At the last level of each branch of this procedure, we will have one of three possible outcomes:

1. All exponential terms have canceled out and we have a false equation with constant terms. In this case there is no solution to (6) or (5) in this branch.

2. There is an equation $0 = 0$ (i.e. all terms cancel out after a substitution). In this case all variables (after renumbering) $\hat{y}_{i+1}, \ldots, \hat{y}_m$ that remained in the previous step of the branch are taken as free variables, and we obtain a general solution $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ to system (6) along this branch.

3. There is one equation left of the form $\beta_s k^{y_s} + C = 0$. In this case, this equation has a unique solution $y_s = b$ or no solution.

In the second case, any solution in $\mathbb{Z}$ of the linear system $\hat{y}_1 = \hat{y}_2 + c_1, \hat{y}_2 = \hat{y}_3 + c_2, \ldots, \hat{y}_i = \hat{y}_{i+1} + c_i$ will be a solution to system (6) since when we substitute the variables into this equation, the same cancellations will occur and we will remain with the equation $0 = 0$. This proves the claim. □

System (5) can also be reduced to a disjunction of linear systems by substituting each $\hat{y}_i$ back to the corresponding linear combination of $y_1, \ldots, y_n$. This completes the proof of the lemma. □

System (4) is also equivalent to a disjunction of linear systems –we first replace sums appearing in the exponent of k by new variables and then apply Lemma 2. We now solve this disjunction of linear systems –if it is solvable, the general solution will correspond to the disjunction of systems of linear equations on $\hat{X}$. We fix one of these systems and substitute those r_i's that are fixed numbers into system (3) that has triangular form. Denote the new tuple of r_i's by $\tilde{X}$.

Proof of Theorem 1.

We will first prove the second statement. Suppose a system of equations in $BS(1,k)$ does not have coefficients. Then systems (1) and (3) do not have the last term.

The system has a non-trivial solution if and only if system (4) has a non-trivial solution. We can describe all solutions of (4) because they come from systems of linear equations. Then we substitute any solution of (4) in (3) and find all solutions of (3) in $Z(1/k)$ as a homogenous system of linear equations over $Z(1/k)$.

It cannot happen that (4) has only finitely many solutions and the number of equations is more than the number of variables (so each $z_i = 0$). Indeed then there are no a's in the solution and we have a homogeneous linear system in abelian group that either has only zero solution or infinitely many.

Now we will show that there is an algorithm to decide if a quadratic equation has a solution. Every quadratic equation is equivalent to an equation in the standard form

$$\Pi_{i=1}^{g}[x_i, y_i]\Pi_{i=1}^{n} z_i^{-1} c_i x_i = 1$$

or

$$\Pi_{i=1}^{g}[x_i, y_i]\Pi_{i=1}^{n} z_i^{-1} c_i x_i = 1$$

The commutator width of $BS(1,n)$ is one. Indeed, since the relator has b-exponent 0 and a-exponent $1-k$, any word on a, b tat represents an element of the derived subgroup must have b-exponent 0 and a-exponent a multiple of $k-1$. Therefore, each element of the derived subgroup may be written as $b^s a^{m(k-1)} b^{-s}$, which is equal to

$$b^s a^{mk} b^{-s} b^s a^{-m} b^{-s} = b^{s-1} a^m b^{1-s} b^s a^{-m} b^{-s} = b^{s-1} a^m b a^{-m} b^{-s} = [b, a^{-m} b^{-s}].$$

The verbal width of the subgroup generated by the squares in $BS(1,n)$ is two. Hence an orientable equation of genus $g \geq 1$ has a solution if and only if $\Pi_{i=1}^{n} c_i \in BS(1,n)'$. A non-orientable equation of genus $g \geq 2$ has a solution if and only if $\Pi_{i=1}^{n} c_i$ belongs to this verbal subgroup. Therefore (except non-orientable of genus 1) we only have to deal with equations of genus zero.

$$\Pi_{i=1}^{n} z_i^{-1} c_i z_i = 1.$$

Lemma 3. *The question about the existence of solutions to quadratic equation of genus zero reduces to the question about existence of solutions to certain system (4) or, equivalently, (6).*

Proof. Consider

$$\Pi_{i=1}^{n} x_i^{-1} \bar{c}_i x_i = 1$$

and let $x_i = (z_i k^{-y_i}, r_i)$ and $\bar{c}_i = (c_i k^{-d}, s_i)$. Then

$$\Pi_{i=1}^{n}(z_i k^{-y_i}, r_i)(c_i k^{-d_i}, s_i)(z_i k^{-y_i}, r_i)^{-1} = \Pi_{i=1}^{n}(z_i k^{-y_i}, r_i)(c_i k^{-d_i}, s_i)(-z_i k^{-y_i + r_i}, -r_i)$$

$$= (\sum_{i=1}^{n} k^{-\sum_{j=1}^{i-1} s_i}(c_i k^{-d_i - r_i} + z_i k^{-y_i}(1 - k^{-s_i})), \sum_{i=1}^{n} s_i) = (0,0).$$

Therefore, $\sum_{i=1}^{n} s_i$.

There are two possible cases. In the first case $s_i = 0$ for all $i = 1, \ldots, n$, then the system is equivalent to a system $\sum_{i=1}^{n} c_i k^{\bar{y}_i} = 0$ for new integer variables $\bar{y}_i, i = 1, \ldots, n$. This is exactly system (6).

In the second case, some s_i is non-zero. Take $s = gcd(|s_1|, \ldots, |s_i|)$, then $(k^s - 1) = gcd((k^{|s_i|} - 1), i = 1, \ldots, n)$ and the quadratic equation has a solution if and only if the congruence

$$\sum_{i=1}^{n} c_i k^{\bar{y}_i} \equiv 0 (mod(k^s - 1))$$

has a solution in $\mathbb{Z}(1/k)$. Therefore we only have to consider $\bar{y}_i$'s such that $-s \leq y_i \leq s$. This finishes the proof in the second case. □

3 Restricted wreath products with $\mathbb{Z}$

The restricted wreath product $G \wr \mathbb{Z}$ is isomorphic to the semidirect product $\oplus_{i \in \mathbb{Z}} G \rtimes \mathbb{Z}$, where the action of $\mathbb{Z}$ on $\oplus_{i \in \mathbb{Z}} G$ is by translation of indices, that is, $k \cdot \{g_n\}_{n \in \mathbb{Z}} = \{g_{n+k}\}_{n \in \mathbb{Z}}$. The product of two elements $(\{g_n\}_{n \in \mathbb{Z}}, k) \cdot (\{h_n\}_{n \in \mathbb{Z}}, l)$ is $(\{g_n + h_{n+k}\}_{n \in \mathbb{Z}}, k + l)$. When $G = \mathbb{Z}_2$ the group is called the lamplighter group.

If A is finitely generated abelian, then $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ as an additive group. Denote by R the ring $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. In this case $A \wr \mathbb{Z}$ is isomorphic to the group of matrices of the form

$$M = \begin{pmatrix} t^x & P \\ 0 & 1 \end{pmatrix}$$

where P is a Laurent polynomial in $R[t, t^{-1}]$. Note that $P = f(t)t^{-k}$ where $f(t) \in R[t]$ and $k \in \mathbb{N}$.

We will first show that equations in $A \wr \mathbb{Z}$ are decidable for $A = \mathbb{Z}_n$ and $A = \mathbb{Z}$. We will denote $\mathbb{Z}_n \wr \mathbb{Z}$ by L_n and $\mathbb{Z} \wr \mathbb{Z}$ by L.

Theorem 2. *Quadratic equations in L_n are decidable. There is also an algorithm to decide if an arbitrary coefficient free system has a non-trivial solution.*

Proof. The product of n elements in L_n is

$$\begin{pmatrix} t^{x_1} & P_1 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} t^{x_n} & P_n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t^{x_1 + \ldots + x_n} & Q \\ 0 & 1 \end{pmatrix}$$

where $P_j = f_j(t)t^{-y_j}$ and

$$Q = f_n(t)t^{-y_n}t^{x_1+\ldots+x_{n-1}} + f_{n-1}(t)t^{-y_{n-1}}t^{x_1+\ldots+x_{n-2}} + \ldots + f_1(t)t^{-y_1}$$

In a system of equations in L_n, some of the $x_i, f_j(t)$ and y_j may be constants and some may be variables.

Thus, any system of equations in L_n is equivalent to a system of equations of the form:

$$F_1(\bar{x}, t, t^{-1}) f_1(t) t^{-y_1} + \ldots + F_m(\bar{x}, t, t^{-1}) f_m(t) t^{-y_m} = P(\bar{x}, t, t^{-1}) \quad (7)$$

and

$$\sum_i c_i x_i + C = 0 \quad (8)$$

where $F_j(\bar{x}, t, t^{-1}) = \sum_i \alpha_i t^{\sigma_i(\bar{x})}$ where $\alpha_i = \pm 1$, and $\sigma_i(\bar{x})$ is a linear combination of elements in x and a constant, and $f_j(t)$ is a variable that runs over $\mathbb{Z}_n[t]$, y_j is a variable that runs over $\mathbb{N}$, $P(\bar{x}, t, t^{-1})$ is a polynomial in $\mathbb{Z}_n[t, t^{-1}]$ with linear combinations of $\bar{x}$ in the exponents of t and $c_i, C \in \mathbb{Z}$.

We begin by solving the linear system (8) as in Section 2. If the system does not have a solution, then system (7) will not have a solution either. If the system has a solution, then we substitute those values of x_i into system (7). Some x_i will be replaced by integers, others by linear combinations of elements in $\bar{x}$ and constants.

Now we solve system (7). This system can be put in Smith normal form by regarding the terms $f_j(t)t^{-y_j}$ as variables, the terms $F_j(\bar{x}, t, t^{-1})$ as coefficients, and $P(\bar{x}, t, t^{-1})$ as a constant coefficient.

Thus, the system is equivalent to a disjunction of systems of the form:

$$F'_s(\bar{x}, t, t^{-1}) f_s(t) t^{-y_s} = \sum_{i>q} F'_{s_i}(\bar{x}, t, t^{-1}) f_i(t) t^{-y_i} + P'_s(\bar{x}, t, t^{-1}) \quad (9)$$

for $s = 1, \ldots, q$, and

$$\sum_i a_i t^{\sigma_i(\bar{x}, d_i)} = 0 \quad (10)$$

where $a_i, \in \mathbb{Z}_n$ and $\sigma_i(\bar{x}, d_i)$ is a linear combination of elements in $\bar{x}$ with constants.

To solve system (10), we begin by grouping terms in each equation such that the sum of the coefficients of each group is zero modulo n. If there is no way to group each equation in the system in this way, then this system does not have a solution. For, suppose there is a solution to system (10), then after substituting the solution in each equation and simplifying, the coefficients of each t^i should be zero in each equation, thus the sum of the coefficients of t^i before simplifying must be zero modulo n.

There may be many ways to group the terms of each equation. We fix one system after grouping and for each equation, we set the powers of t in the terms that were grouped together equal to each other, consequently obtaining a system of linear equations.

For example in L_5, the equation

$$3t^{3-x_1+x_2} + 4t^{-2+x_1} + 2t^{x_3-2} + 1 = 0$$

can be grouped as follows:

$$(3t^{3-x_1+x_2} + 2t^{x_3-2}) + (4t^{-2+x_1} + 1) = 0$$

We then obtain the linear system

$$3 - x_1 + x_2 = x_3 - 2$$

$$-2 + x_1 = 0$$

We now solve this system of linear equations. If there is no solution, system (9) has no solution in this branch. If there is a solution, then we substitute the general solution back into (9).

Proof of Theorem 2 Every non-abelian abelian-by-cyclic group $A \rtimes_\phi \mathbb{Z}$ has commutator width 1. Indeed, the derived subgroup equals the image of $\phi - 1 \in End(A)$ that consists of commutators. The action of ϕ on $A/(\phi - 1)A$ is trivial, therefore $(A \rtimes_\phi \mathbb{Z})' \in (\phi - 1)A$. Therefore, everything again reduces to genus zero equations.

Consider

$$\Pi_{i=1}^n \bar{x}_i \bar{c}_i \bar{x}_i^{-1} = 1$$

and let $\bar{x}_i = \begin{pmatrix} t^{x_i} & f_i(t)t^{-y_i} \\ 0 & 1 \end{pmatrix}$ Then $\Pi_{i=1}^n \bar{x}_i \bar{c}_i \bar{x}_i^{-1} = \begin{pmatrix} t^{\sum_{i=1}^i s_i} & P \\ 0 & 1 \end{pmatrix}$, where

$$P = \sum_{i=1}^{n} (f_i(t)t^{y_i}(1 - t^{s_i}) + c_i t^{-d_i - x_i})t^{\sum_{j=1}^{i-1} s_i}$$

Therefore, $\sum_{i=1}^n s_i$.

There are two possible cases. In the first case $s_i = 0$ for all $i = 1, \ldots, n$, then the system is equivalent to a system $\sum_{i=1}^n c_i t^{\bar{y}_i} = 0$ for new integer variables $\bar{y}_i, i = 1, \ldots, n$. This is exactly system (10).

In the second case, some s_i is non-zero. Take $s = gcd(|s_1|, \ldots, |s_i|)$, then $(t^s - 1) = gcd((t^{|s_i|} - 1), i = 1, \ldots, n)$. For non-prime n, the ring $\mathbb{Z}_n[t, t^{-1}]$ is not a domain. But one can still use an analogue of the Euclidean algorithm and induction on n, to show that $t^s - 1$ can be represented as a linear combination of $t^{|s_i|} - 1, i = 1, \ldots, n$ with coefficients in $\mathbb{Z}_n[t, t^{-1}]$. Quadratic equation $\Pi_{i=1}^n \bar{x}_i \bar{c}_i \bar{x}_i^{-1} = 1$ in this case has a solution if and only if the congruence

$$\sum_{i=1}^{n} c_i t^{\bar{y}_i} \equiv 0 (mod(t^s - 1))$$

has a solution in $\mathbb{Z}[t, t^{-1}]$. To check this congruence we only have to consider $\bar{y}_i$'s such that $-s \leq y_i \leq s$. This finishes the proof in the second case. □

The second statement of the theorem is proved similarly to the proof for $BS(1, k)$.

Theorem 3. *Quadratic equations in L are decidable. There is also an algorithm to decide if an arbitrary coefficient free system has a non-trivial solution.*

A system of equations in L reduces to equations of the form (7) and (8), but the $f_j(t)$ are variables in $\mathbb{Z}[t]$ and $P(\bar{x}, t, t^{-1})$ is a polynomial with coefficients in $\mathbb{Z}$. To solve system (10) we group terms whose coefficients add up to 0. Then we reduce this system to system (**??**).

Theorem 3 implies the following corollary.

Corollary 1. *The Diophantine problem is decidable for coefficient free and for quadratic equations in* $\mathbb{Z}^n \wr \mathbb{Z}$.

Proof. Equations in $\mathbb{Z}^n \wr \mathbb{Z}$ have the same form as equations (7) and (8) in the proof of Theorem 3, with the exception that the terms $f_i(t)$ are in the ring $\mathbb{Z}^n[t]$. Each equation of the form (7) is equivalent to n equations, each corresponding to a component of $\mathbb{Z}^n$. Thus, any system of equations in $\mathbb{Z}^n \wr \mathbb{Z}$ is equivalent to a system in $\mathbb{Z} \wr \mathbb{Z}$, so the decidability follows from the decidability of $\mathbb{Z} \wr \mathbb{Z}$. □

Combining Theorems 2 and 3 we obtain the second main result.

Theorem 4. *The Diophantine problem is decidable for coefficient free and for quadratic equations in* $A \wr \mathbb{Z}$, *where* A *is a finitely generated abelian group.*

Proof. Let $A = \mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Equations in $A \wr \mathbb{Z}$ have the same form as equations (7) and (8) in the proof of Theorems 2, 3 with the exception that the terms $f_i(t)$ are in the ring $R[t]$ (recall that R is the same as A but viewed as a ring). Each system of the form (7) is equivalent to several systems, some of them over $\mathbb{Z}$ and some over $\mathbb{Z}_{n_i}$, each corresponding to a component of $\mathbb{Z}^m \oplus \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Solving these systems simultaneously we will solve the original system. □

We conclude with some open problems.

Problem 1. *Is the Diophantine problem decidable in* $BS(1, k)$ *and in wreath products* $A \wr \mathbb{Z}$, *where* A *is a finitely generated abelian group?*

Problem 2. *Is the existential theory of* $BS(1, k)$ *and wreath products* $A \wr \mathbb{Z}$, *where* A *is a finitely generated abelian group, decidable?*

Problem 3. *Describe finitely generated metabelian groups with decidable Diophantine problem.*

References

[1] J. Denef, L. Lipshitz. Diophantine sets over some rings of algebraic integers. Journal of the London Mathematical Society, s2-18(3), (1978) 385-391.

[2] V. Diekert, M. Lohrey, Existential and Positive Theories of Equations in Graph Products, Theory Comput. Syst. 37 (2004), pp. 133-156.

[3] V. Diekert, A. Muscholl Solvability of Equations in Graph Groups is Decidable, Internat. J. Algebra Comput. 16 (2006), pp. 1047-1069.

[4] M. Duchin, H. Liang, M. Shapiro, Equations in nilpotent groups. Proc. Amer. Math. Soc. 143 (2015), no. 11, 4723-4731.

[5] Yu. L. Ershov, Elementary theory of groups, Dokl. Akad. Nauk SSSR, 203, No. 6 (1972), 1240-1243.

[6] A. Garreta, A. Miasnikov, D. Ovchinnikov, Random nilpotent groups, polycyclic presentations, and Diophantine problems, Groups Complex. Cryptol. 9 (2017), no. 2, 99-115.

[7] O. Greco, Unique non-unique factorization, Master's thesis, 2010, University of Stockholm.

[8] A. Khelif, Bi-interpretabilite et structures QFA: Etude des groupes solubles et des anneaux commutatifs, C. R. Acad. Sci. Paris, Ser. I 345 (2007) 59-61.

[9] M.I. Kargapolov, V.N. Remeslennikov, N.S. Romanovskii, V.A. Roman'kov and V.A. Churkin, Algorithmic problems for $\mathcal{O}$-powered groups, Algebra and Logic, 8, No. 6 (1969), 363-374.

[10] M. Lohrey, G. Senizergues, Theories of HNN-extensions and amalgamated products. Automata, languages and programming. Part II, 504-515, Lecture Notes in Comput. Sci., 4052, Springer, Berlin, 2006.

[11] R. C. Lyndon. Equations in free groups. Trans. Amer. Math. Soc. 96 (1960), 445-457.

[12] A. I. Malcev, On equation $xyx^{-1}y^{-1} = aba^{-1}b^{-1}$ in a free group, Algebra and Logic, 1 (1962), 45-50.

[13] G. S. Makanin, The problem of solvability of equations in a free semigroup, Mat. Sb. (N.S.), 1977, 103(145):2(6), pp. 147-236.

[14] G. S. Makanin, Equations in a free group (Russian), Izv. Akad. Nauk SSSR, Ser. Mat., 46 (1982), pp. 1199-1273, transl. in Math. USSR Izv., 21 (1983)

[15] G. Noskov. The elementary theory of a finitely generated almost solvable group. Izv. Akad. Nauk SSSR Ser. Mat., 47(3):498-517, 1983.

[16] T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. Contemporary Mathematics, 270, 49-106, 2000.

[17] V.A. Roman'kov, Unsolvability of the problem of endomorphic reducibility in free nilpotent groups and in free rings., Algebra and Logic, 16 (1977), no. 4, 310-320.

[18] V. A. Roman'kov. Equations in free metabelian groups. Siberian Mathematical Journal, 20(3), 469-471, 1979.

[19] N. S. Romanovskii, On the elementary theory of an almost polycyclic group, Mathematics of the USSR-Sbornik, 39, No. 1 (1981),125-132.

[20] A L Semenov 1984 Math. Logical theories of one-place functions on the set of natural numbers. USSR Izv. 22, 587-618.

[21] W. Szmielew, (1955), Elementary properties of Abelian groups, Fundamenta Mathematicae, 41, 203-271.

20F16, 20F70