Equations in Metabelian Baumslag-Solitar Groups

Olga Kharlampovich∗, Laura López†, Alexei Myasnikov‡

1 Introduction

In this paper we show that Diophantine problem in solvable Baumslag-Solitar groups $BS(1, k)$ is decidable, i.e., there is an algorithm that given a finite system of equations with constants in $BS(1, k)$ decides whether or not the system has a solution in the group.

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 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 [9]. However, if $k \geq 2$ then $BS(1, k)$ is metabelian which is not virtually abelian, so the first-order theory of $BS(1, k)$ is undecidable. Indeed, in [5] Noskov showed that the first-order theory of a finitely generated solvable group is decidable if and only if the group is virtually abelian. In free metabelian non-abelian groups equations are undecidable [7]. In fact, in a finitely generated metabelian group $G$ given by a finite presentation in the variety $\mathcal{M}_2$ of metabelian groups Diophantine problem is undecidable asymptotically almost surely if the deficiency of the presentation is at least 2 [2]. 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 non-virtually abelian nilpotent group then decidability of the Diophantine problem in $G$ would imply decidability of 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, 6]) that states that 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 $\mathbb{Z} \wr \mathbb{Z}$ or $\mathbb{Z}_n \wr \mathbb{Z}$ (here $\mathbb{Z}$ is an infinite cyclic group and $\mathbb{Z}_n$ is a cyclic group of order $n$) are the typical examples of such groups. As we

∗Hunter College and Graduate Center, CUNY
†Graduate Center, CUNY
‡Stevens Institute
mentioned above, equations in $BS(1, k)$ are decidable, so $BS(1, k)$ provide first examples of non-virtually abelian finitely generated metabelian groups with decidable Diophantine problem. This gives also a new look at one-relator groups. Since the Noskov’s result mentioned above the groups $BS(1, k), k \geq 2$, were the only one-relator groups with undecidable first-order theory. Recently, it was shown in [3] 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 Proof of the theorem

The main result is

**Theorem 1.** Equations in $B(1, k)$ are decidable.

To prove the theorem we have to construct an algorithm that decides whether the set of formulas of the form $\exists \bar{x} \wedge \sum_{i=1}^{n} t_i(\bar{x}, a, b) = 1$ is decidable, where $t_i(\bar{x}, a, b)$ is a term. Recall that the group $B(1, k)$ is isomorphic to the group $\mathbb{Z}[1/k] \rtimes \mathbb{Z}$, where $\mathbb{Z}[1/k] \cong \text{ncf}(a)$ and $\mathbb{Z} \cong \langle b \rangle$, where

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

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

$$(z_1 k^{-i_1}, r_1)(z_2 k^{-i_2}, r_2) = (z_1 k^{-i_1} + z_2 k^{-i_2 + r_1}, r_1 + r_2).$$

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

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

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

and

$$\sum \beta_j r_j = \delta. \quad (2)$$

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 $y_i, z_i, r_i, \beta_j$ are variables, and all $y_i \geq 0$.

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

**Proof.** Note that

$$(z_1 k^{-y_1}, r_1) \cdot (z_2 k^{-y_2}, r_2) \cdots (z_n k^{-y_n}, r_n) = (z_1 k^{-y_1} + z_2 k^{-y_2 + r_1} + \cdots + z_n k^{-(y_n + r_1 + \cdots + r_{n-1})}, r_1 + \cdots + r_n)$$

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

$\square$
To solve a system of equations in $B(1,k)$, we begin by solving system $\mathbf{2}$. This system is just a linear system of equations $AX = B$ with integer coefficients, where $X = (x_1, \ldots, x_n)^T$ 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 $\bar{A}X = \bar{B}$ such that $\bar{A}$ has a diagonal 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 $\bar{A}X = \bar{B}$ does not have a solution, then the corresponding system of equations in the group does not have a solution. If the system $\bar{A}X = \bar{B}$ 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 $\mathbf{1}$. We only have to check that there exist integer solutions $Z = \{z_1, \ldots, z_n\}, Y = \{y_1, \ldots, y_n\}$ and remaining $\bar{X}$ that we denote $\bar{X} = \{r_1, \ldots, r_m\}$.

System $\mathbf{1}$ is equivalent to a system in the following form:

$$z_{s}k^{-y_{s}}(\sum_{j} \sum_{i>s} \gamma_{ji}k^{\tau_{ij}(\bar{r})} + \sum_{t} \gamma_{ti}k^{\tau_{it}(\bar{r})}) = 1, \quad r_{1}, \ldots, r_{m}$$

(3)

where $\gamma_{ij}, \tau_{ij}, \tau_{ik}$ are linear combinations of elements in $\bar{X}$ and constants. One can consider this as a system in triangular form with variables $z_{1}k^{-y_{1}}, \ldots, z_{k}k^{-y_{k}}$ and linear combinations of exponential functions as coefficients (which contain variables $\bar{X}$).

We first will find all solutions of system $\mathbf{1}$ using Semenov’s ideas from $\mathbf{8}$ where he proved that the theory of $(\mathbb{Z}, +, k^x)$ is decidable.

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

$$F(y) = \sum_{j} \beta_{j}k^{y_{j}} + C = 0,$$

(5)

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

**Proof.** Let $\bar{y} = (y_1, \ldots, y_n)$ and let $\lambda : \{y_1, \ldots, y_n\} \to \{+, -\}$ be a map that assigns to each variable a positive or negative sign. System $\mathbf{5}$ over $\mathbb{Z}$ is equivalent to a disjunction of $2^n$ systems each with an assignment $\lambda$. 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 $y_{1} < 0, y_{2} > 0, y_{3} > 0$. Then we rewrite it as $k^{-y_{1}} - k^{y_{2}} + k^{y_{3}} + c = 0$ with assignment
$y_1 > 0, y_2 > 0, y_3 > 0$ and multiply the equation by $k^{y_1}$. We then obtain the equation

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

with assignment $y_1 > 0, y_2 > 0, y_3 > 0$. 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

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

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

Proof. Denote the new variables as $\bar{y}' = (\bar{y}_1, \ldots, \bar{y}_m)$. We begin by showing that for each $i$, there is a $\Delta_i \in \mathbb{N}$ such that $F'$ does not have a solution if $\bar{y}_i > \bar{y}_j + \Delta_i$ for all $j \neq i$. We can rewrite the equation in the form $k^0 + \sum_i \gamma_i k^{\bar{x}_i} = \sum_j \delta_j k^{\bar{z}_j} + C$, where all $\gamma_i, \delta_j$ are positive, $\bar{y} = \bar{y}_i$ and $\bar{x}_i, \bar{z}_j$ are all variables in $\bar{y}' - \bar{y}_i$. Let $\Delta_i = \Delta > \log k (\sum_j \delta_j + C)$ and $\bar{y} > \bar{x}_i + \Delta$ and $\bar{y} > \bar{z}_j + \Delta$ for all $i, j$. Then $k^0 > k^{\Delta} k^{\bar{z}_j} > (\sum_j \delta_j + C) k^{\bar{z}_j}$ for all $j$. Thus, the right side of the equation will always be smaller than the left side, and the equation has no solution.

So we have shown that for all variables $\bar{y}_i$, if $F'$ (or a finite system of equations where each equation has form $F'\bar{y}$) has a solution then there is a $j \neq i$ such that $\bar{y}_i \leq \bar{y}_j + \Delta_i$. Now consider a finite graph $G$ with $n$ vertices labeled $\bar{y}_1, \ldots, \bar{y}_m$ and directed edges from $\bar{y}_i$ to $\bar{y}_j$ whenever $\bar{y}_i \leq \bar{y}_j + \Delta_i$. 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 $\bar{y}_{i_1}, \ldots, \bar{y}_{i_s} = \bar{y}_{i_1}, s \leq m + 1$. Then

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

$$= \bar{y}_{i_1} + \Delta_{i_{s-1}} + \ldots + \Delta_{i_1}$$

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

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

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

Fix a $y_{i_1}$ and let $\Delta_{i_1} = \sum_{t=1}^{j-1} \Delta_{i_t}$ and $\Delta_{i_2} = \sum_{t=j}^{s-1} \Delta_{i_t}$. Then we may replace the equation $F'(\bar{y})$ by a disjunction of equations $G(\bar{y}, \bar{y}_{i_1})$ where $G$ is
the same as the formula $F'$, but $\hat{y}_j$ is replaced by $\hat{y}_i - \Delta_{j_1}$ in one equation, $y_i - \Delta_{j_1} + 1$ in the next, and so on until $\hat{y}_i + \Delta_{j_2}$.

Now we may eliminate variables from an 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.

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 (5) 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 $X$. 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 $\tilde{X}$. We now describe two procedures: the first will stop if it finds a solution to (3), the second will stop if there is no solution.

**Procedure 1.** If an integer solution to the system (3) exists, we can find it enumerating all integer values of $\tilde{X}, Y, Z$.

Now we will justify the second procedure. We can assume all $y \in Y$ are non-negative. Splitting into several cases as before, we can also assume that all $r \in \tilde{X}$ are non-negative. Then system (3) is equivalent to a disjunction of systems

$$z_ik^{-y_s}\left(\sum_j k^{\tau_{y_j}(\bar{r})}\right) = \sum_{i>q} z_i k^{-y_i}\left(\sum_j k^{\sigma_{y_j}(\bar{r})}\right) + C,$$

where $s = 1, \ldots, q, y_j, r_j \in \mathbb{N}, \tau_{y_j}, \sigma_{y_j}$ are linear combinations of elements in $\tilde{X}$ and constants and $C \in \mathbb{Z}$.

**Lemma 3.** There is an integer solution to system (7) if and only if there is a solution to this system modulo $p^m$ for any prime number $p$ not dividing $k$, and any natural $m$. 
Proof. If there is an integer solution to system (7) then there is a solution modulo $p^m$ for any prime number $p$ not dividing $k$ and any natural $m$.

Suppose there is no integer solution to system (7). There is always a rational solution $\{z_i\}$. An integer solution may fail to exist only if for any integer values of $\tilde{X}, Y$, for any choice of integer $z_i, i > q$, there exists $s$ such that the term $\sum_j k^{\alpha_j} r_j + \alpha_s$ does not divide the right-hand side of the equation in $\mathbb{Z}[1/k]$. This implies that there is $p^m$ dividing the term $(\sum_j k^{\alpha_j} r_j + \alpha_s)$ and not dividing the right side of the corresponding equation. Here $p$ does not divide $k$. This proves the statement of the lemma.

The lemma implies that we can create the second process.

Procedure 2. If an integer solution to system (7) does not exist, then solving the system modulo different prime powers we will eventually find $p^m$ such that the solution does not exist.

First fix a prime $p$ that does not divide $k$, take $p^m$. Then the function $k^y$ is periodic modulo $p^m$ with some period $P$. For each $y \in Y$ and $x \in \tilde{X}$ we have to consider only values $\{0, 1, \ldots, P\}$. Therefore there is only a finite number of possible values of $k^y$ modulo $p^m$. There is also a finite number of different possibilities for variables in $Z$. Consider each possibility separately. If none of the systems corresponding to a finite number of possibilities has a solution, then system (7) does not have a solution. If some of the possibilities for $\tilde{X}, Y, Z$ give a solution, then we rewrite the variables $\tilde{X}, Y, Z$ in the form $r_i = t + (P - 1)\bar{r}_i$, where $0 \leq t \leq p - 1$, take this solution and continue to the next prime number $p_1$ with each such possibility.

We organize two procedures. One will enumerate integers $X, Y, Z$, and if the solution exists it will find it. The second procedure will check for each prime number $p^m$ if there is a solution modulo $p^m$. If there is no solution the second procedure will stop.

References

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

[2] A. Gareta, A. Miasnikov, D. Ovshinnikov, Properties of random nilpotent groups. ArXiv e-prints, 2016.

[3] O. Kharlampovich, A. Miasnikov, Model theory in one relator groups, preprint.

[4] A. Khelif, Bi-interpétabilité et structures QFA: étude des groupes résolubles et des anneaux commutatifs, C. R. Acad. Sci. Paris, Ser. I 345 (2007) 59-61.

[5] G. Noskov. The elementary theory of a finitely generated almost solvable group. Izv. Akad. Nauk SSSR Ser. Mat., 47(3):498-517, 1983.
[6] T. Pheidas and K. Zahidi. Undecidability of existential theories of rings and fields: A survey. Contemporary Mathematics, 270, 49-106, 2000.

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

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

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