Decidability of knapsack problem for Baumslag-Solitar group

Fedor Dudkin\textsuperscript{1}, Alexander Treier\textsuperscript{2}
\textsuperscript{1} Sobolev Institute of Mathematics Siberian Branch of the Russian Academy of Sciences
Omsk, Russia
\textsuperscript{2} Omsk State Technical University Omsk, Russia
E-mail: alexander.treyer@gmail.com

Abstract. In this work we investigate a decidability problem of group version of the knapsack problem for Baumslag-Solitar group $BS(p, q)$. We proved, that the knapsack problem is decidable for group $BS(p, q)$ for coprime integers $p > 1, q > 1$. In the case when $p = 1, q \in \mathbb{N}$, we proved that knapsack problem is decidable for group $BS(1, q)$ with some restriction on the input of the problem. However, the problem of the decidability of the knapsack problem for group $BS(1, q)$ on the whole set of inputs remains open.

1. Introduction

The Baumslag–Solitar groups are particular class of two-generator one-relator groups which have played a surprisingly useful role in combinatorial and geometric group theory. In a number of situations they have provided examples which mark boundaries between different classes of groups and they often provide a testbed for theories and techniques.

These groups have a deceptively simple definition. For each pair $p$ and $q$ of non-zero integers, there is a corresponding group defined by the presentation

$$BS(p, q) = \langle a, t | t^{-1} \cdot a^p \cdot t = a^q \rangle,$$

where, as usual, this notation means that the group is the quotient of the free group on the two generators by the normal closure of the single element $t^{-1} \cdot a^p \cdot t \cdot a^{-q}$. When $|p| = |q| = 1$, $BS(p, q)$ is the fundamental group of the torus or Klein bottle, both of which have been long familiar and well understood — and can therefore be regarded as standing somewhat apart from the remaining groups.

The Baumslag-Solitar groups were introduced in [1] to provide some simple examples of so-called non-Hopfian groups. The main result concerning finiteness conditions and the Baumslag–Solitar groups are following: $BS(p, q)$ is residually finite (i.e. the intersection of all its subgroups of finite index is trivial) if and only if $|p| = |q| = 1$ or $|p| = 1$ or $|q| = 1$. $BS(p, q)$ is Hopfian if and only if it is residually finite or $\pi(p) = \pi(q)$, where $\pi(p)$ denotes the set of prime divisors of $p$.

Although the above theorem divides the Baumslag–Solitar groups into three classes: those that are residually finite, those that are Hopfian but not residually finite and those that are non-Hopfian, the most marked contrast is between those Baumslag–Solitar groups where $|p| = 1$ or $|q| = 1$ and those for which $|p|, |q| \neq 1$. For a group $BS(1, q)$ there is an obvious homomorphism...
onto the infinite cyclic group, obtained by setting $a = 1$, and standard techniques show that the kernel is isomorphic to the additive group of $q$-adic rational numbers. Thus, such groups are metabelian and have strong structural properties; in particular, they do not contain a free subgroup of rank two. Moreover, these groups have a particularly simple normal form for their elements.

We give formulation of the knapsack problem for groups, following [2]:

**Knapsack Problem.** Let the elements $g_1, \ldots, g_k, g$ of the group $G$ are given. Are there numbers $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N} \cup \{0\}$ such that

$$g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g. \quad (1)$$

The group version of the knapsack problem generalizes the classical knapsack problem for integers (more precisely, one of its formulations). Taking the additive group of integers as the group $G$, we obtain the well-known classical version of the knapsack problem. We call attention of the reader that the group $G$ can be either commutative or non-commutative, and the main interest of researchers here is related to the knapsack problem for non-commutative groups. In this direction, naturally arises the question of decidability of the knapsack problem for a group or class of groups and the question of its algorithmic complexity.

We briefly describe some results related to the knapsack problem for groups. In the work [2], in addition to setting the problem of knapsack for groups, the first results in this direction were obtained. In particular, it is shown that the knapsack problem is solvable polynomially for classes of abelian and hyperbolic groups. In the article [4] it is proved that the knapsack problem for partially commutative groups is algorithmically solvable and belongs to the class NP. In articles [6, 5] independently of each other it was proved that there exist nilpotent groups for which the knapsack problem is algorithmically unsolvable. Also, in [6] it is shown that if a two-step nilpotent torsion-free group has a commutator rank greater than 316, then in this group the knapsack problem is algorithmically unsolvable.

In this paper we concentrate on the decidability of the Knapsack problem for Baumslag-Solitaire groups of the form $BS(1,p)$ (section 2) and $BS(p,q)$, where $p, q > 1$ are co-prime natural numbers (section 3). In the case of group $BS(1,p)$, we have proved the decidability of the knapsack problem for a sufficiently large set of inputs; in the case of coprime $p, q > 1$, $BS(p,q)$ is solvable on the whole set inputs. The approaches of proofs for the cases $BS(1,p)$ and $BS(p,q)$ are very different. In the first case, model-theoretic results on the decidability of elementary theories of the systems of the form $\langle \mathbb{N}, +, p^x \rangle$, are used, where $p$ is an arbitrary natural number (for more details, see [3]). The proof of the second case is based on the study of the normal form of elements in $HNN$ — extensions and the number-theoretic approach.

2. Case $BS(1,p)$

2.1. Normal form

Let $p$ be a natural number. Denote

$$B = BS(1,p) = \langle a, t | t^{-1} \cdot a \cdot t = a^p \rangle. \quad (2)$$

It is not hard to show, that the group $B$ is metabelian. The group $B$ is semidirect product of the following form:

$$B \cong \mathbb{Z}[\frac{1}{p}] \rtimes \mathbb{Z}, \quad (3)$$

where $\mathbb{Z}[\frac{1}{p}] = \{ \frac{m}{p^n} | a \in \mathbb{Z}, m \in \mathbb{Z} \}$.

The product (3) defines convenient presentation of elements of group $B$ as a pair $(k, i)$, where $k \in \mathbb{Z}[\frac{1}{p}]$ and $i \in \mathbb{Z}$. Let $a$ and $t$ are generators from (2) of group $B$, then $a = (1,0), \ t = (0,1)$ and
\[(k, i) \cdot (1, 0) = (k+1, i), \quad (1, 0) \cdot (k, i) = (k+p^i, i), \quad (k, i) \cdot (0, 1) = (pk, i+1), \quad (0, 1) \cdot (k, i) = (k, i+1).\]

Actually, if \((k, i), \ (l, j) \in B, \) then
\[
(k, i) \cdot (l, j) = (kp^j + \ell, i + j) \tag{4}
\]

and inverse element is may be written in the following way:
\[
(k, i)^{-1} = (-kp^{-i}, -i). \tag{5}
\]

In the next lemma we give a formula for calculating the power of elements of group \(B: \)

**Lemma 1.** Let \((s, t) \in B, \ \lambda \in \mathbb{N}, \) then
\[
(s, t)^\lambda = \begin{cases} 
(s \frac{p^\lambda - 1}{p^\ell - 1}, \lambda t) & \text{if} \ t \neq 0, \\
(\lambda s, 0) & \text{if} \ t = 0.
\end{cases}
\]

**Proof.** Case when \(t = 0\) follows from 4. Lets prove lemma for the case when \(t \neq 0.\) Actually,
\[
(s, t)^\lambda = (s + \ell t, 2t) \cdot (s, t)^{\lambda-2} = \ldots = \\
(s + \ell t s + p^{2\ell} s + \ldots + p^{(\lambda-1)\ell} s, \lambda t) = \\
(s \frac{p^\lambda - 1}{p^\ell - 1}, \lambda t).
\]

The lemma is proved. \(\blacksquare\)

**Lemma 2.** Let \(g_1, \ldots, g_k, g \in B \) and \(\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N} \cup \{0\} \) is that \(g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g \) in the group \(B.\) Also \(g_i = (s_i, t_i), \ i = 1, \ldots, k, \ g = (s, t). \) Then for any \(m \in \mathbb{Z}, \) \(g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g' \) is holds, where \(g'_i = (ms_i, t_i), \ i = 1, \ldots, k, \) \(g' = (ms, t). \) And vice versa, if \(g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g', \) then \(g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g \) in the group \(B.\)

**Proof.** The lemma is follows from (4) and (5).

### 2.2. Decidability of knapsack problem for \(BS(1, p)\)

The mail goal for this section is giving a proof of the following theorem:

**Theorem 1.** Let \(p \) be a natural number and \(I = \{(g_1, \ldots, g_k, g \in BS(1, p))\} \) be the set of all inputs of knapsack problem such that, for all \(i = 1, \ldots k, \ g_i = (s_i, t_i) \) and \(t_i \neq 0.\) Then knapsack problem is decidable for group \(BS(1, p)\) for any input from \(I.\)

**Proof.** Let \(g_1, \ldots, g_k, g \in I. \) We will reduce exponential group equation in the group \(BS(1, p): \)
\[
g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g, \tag{6}
\]

where \(\varepsilon_i \in \mathbb{N} \cup \{0\}, \ i = 1, \ldots, k, \) to existential formula of first order logic for algebraic structure \(\mathbb{N}' = (\mathbb{N}; + , p^\mathbb{N}). \) Decidability of elementary theory of \(\mathbb{N}' \) is proved by A. Semenov in [3]. Without loss of generality we may assume that \(\mathbb{N} \) contains 0. Note that having binary operation of addition of naturals not hard to define relation of order for natural numbers. Using the order relation we can define constants 0 \(\in \mathbb{N} \) and \(1 = p^0 \in \mathbb{N}. \)

Denote by \(C_i = \frac{s_i}{p^{t_i-1}}, \ i = 1, \ldots, k. \) Let \(t'_j = \text{sign}(t_j)t_j, \ i = 1, \ldots, k. \) Then coefficient \(C_i \) is defined by \(t'_j \) in the following way:
\[
C_i = \frac{s_i}{p^{t'_i-1}},
\]
if $t_i > 0$ and

$$C_i = \frac{s_ip_i^{t_i}}{1-p_i^{t_i}},$$

if $t_i < 0$.

Divisor of $C_i$ is integer number, since belongs to $\mathbb{Z}[\frac{1}{p_i}]$. Using lemma 2, we will multiply elements $g,g_i$, $i = 1,\ldots,k$ by natural $d$, such that $u_i = dC_i$, $1 \leq i \leq k$ and $u = ds$ is integer. After substitution expression $K$ will be:

We omit the full description of reduction of expression (6) and provide the final system of equations over integers. In notations above the resulting group equation is equivalent to the existential theory of the system

$$K = \exists x,y \ w(x,y)=t.$$ 

In the system (7) all coefficients except for some $u_i$ and $\text{sign}(t_i)$ is non-negative integers. We will send negative coefficients to the right hand side of equation and vice versa. Finally we have the finite system of equation which is equivalent to existential formula of first order logic of decidable theory of algebraic structure $\langle \mathbb{N},+,p^\varphi \rangle$. The theorem is proved.

Why does not the proof is not true for the whole set of inputs? If we remove the restrictions $t_i \neq 0$ for the input $g_1 = (s_1,t_1),\ldots,g_k = (s_k,t_k),g_i$, then terms of the form $x \cdot p^\varphi$ appear in the system (7), where $x,y$ are natural variables. According to Yu.G. Penzin [7], the elementary theory of the system $P = \langle \mathbb{N},+,x \cdot p^\varphi,p^\varphi \rangle$ is undecidable, although it is not yet known whether the existential theory of the system $P$ is decidable or not.

3. Co-prime $p,q > 1$

Let’s give several necessary definitions from [8].

Given subgroups $A$ and $B$ of the group $H$ and $\phi: A \rightarrow B$ is an isomorphism. Then the group

$$H^* = \langle H,t \mid t^{-1}at = \phi(a), a \in A \rangle$$

is called the HNN extension.

A sequence $g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n$, where $g_i \in H, \varepsilon_i = \pm 1$ is called reduced if it contains no consecutive $t^{-1}, g_i, t$, where $g_i \in A$, and $t,g_j,t^{-1}$, where $g_j \in B$. Substitutions $t^{-1}at = \phi(a)$ and $tbt^{-1} = \phi^{-1}(b)$ are called t-reductions.

A sequence $g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n$ is called cyclically reduced if every cyclic permutation of the sequence is reduced.

Denote by $T_A$ ($T_B$) the right transversal of $A$ ($B$ resp.) in $H$. Then left normal form is the sequence $g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n$ such that

(i) $g_0$ is an element from $H$,

(ii) if $\varepsilon_i = -1$, then $g_i \in T_A, g_i \notin A$,

(iii) if $\varepsilon_i = +1$, then $g_i \in T_B, g_i \notin B$.

The right normal form defines similarly.

Given $w = g_0t^{\varepsilon_1}g_1 \ldots g_{n-1}t^{\varepsilon_n}g_n \in H^*$ such that the sequence $g_0, t^{\varepsilon_1}, g_1, \ldots, g_{n-1}, t^{\varepsilon_n}, g_n$ is reduced. The number $n$ of occurrences of $t^{\pm 1}$ in $w$ is called length of $w$ and denoted by $|w|$.

For all nonzero integers $p,q$ group $BS(p,q)$ is the HNN extension with base group $\langle a^p \rangle$, stable letter $t$ and associated subgroups $\langle a^p \rangle$ and $\langle a^q \rangle$. 
The following lemma is useful in the combinatorial approach to the knapsack problem for Baumslag-Solitar groups.

**Lemma 3.** Given \( q \in \mathbb{Z}_{>1}, p \in \mathbb{Z}, p \perp q, |p| \not\in \{1, 0\} \) and let \( \{\alpha_i\}_{i=0}^\infty \) be a sequence of integers. Suppose that there exists \( \beta \in \mathbb{Z} \) and \( \tau \in \mathbb{Z}_{>0} \) such that:

\[
\alpha_{i+1} = \left(\frac{p}{q}\right)^\tau (\alpha_i + \beta), \quad i = 0, 1, \ldots, L,
\]

for some \( L > \frac{\log_q |\beta| p^\tau - \alpha_0 (q^\tau - p^\tau)|}{|q|^\tau} \). Then \( \alpha_0 = k \cdot p^\tau, \beta = k \cdot (q^\tau - p^\tau) \) for some \( k \in \mathbb{Z} \) and \( \alpha_i = \alpha_0 = k \cdot p^\tau \), for \( i \in \mathbb{Z}_{>0} \).

We will apply the next lemma to describe a solution of some equations in Baumslag-Solitar groups.

**Lemma 4.** [9] Given \( g, h \in BS(p, q), p \perp q, p, q \not\in \{0, 1, -1\} \). If \( g^{-1} h^k g = h^l, h \neq 1, k \neq l \), then

1) \( h = u^{-1} a^s u \), for some \( u \in BS(p, q), s \in \mathbb{Z}, s \neq 0 \).
2) \( l = \left(\frac{p}{q}\right)^m k \), for some \( m \in \mathbb{Z} \).

Using the following lemma it is possible to bound some variables in knapsack equation.

**Lemma 5.** Given \( q \in \mathbb{Z}_{>1}, p \in \mathbb{Z}, p \perp q \) and \( |p| \not\in \{1, 0\} \). Suppose that \( g_1, \ldots, g_n, g \in BS(p, q), x_1, \ldots, x_n \in \mathbb{Z}_{>0}, g_i = u_i^{-1} w_i u_i, w_i \) is cyclically reduced and \( |w_i| \geq 1 \). There exists computable numbers \( M \) and \( C \) depending on \( g_1, \ldots, g_n, g \) and not depending on \( x_1, \ldots, x_n \) such that if for some \( 1 \leq i \leq n - 1 \) the length of cancellation in word \( g_i^{x_i} \cdot g_{i+1}^{x_{i+1}} \) greater than \( M \), then

\[
g_i^{x_i} \cdot g_{i+1}^{x_{i+1}} = r \cdot a^y \cdot w^z \cdot u
\]

for some \( z, y \in \mathbb{Z}, u, r, w \in BS(p, q) \) and \( |u|, |w|, |r| \leq C \).

Our goal to prove, that knapsack problem is solvable for Baumslag-Solitar groups \( BS(p, q) \) with co-prime \( p, q > 1 \).

**Theorem 2.** Given \( q \in \mathbb{Z}_{>1}, p \in \mathbb{Z}, p \perp q, |p| \not\in \{1, 0\} \) and \( g_1, \ldots, g_n, g \in BS(p, q) \). There is an algorithm to find a solution of equation \( g_1^{x_1} \cdot g_2^{x_2} \cdots g_n^{x_n} = g \) (or to prove that it is unsolvable) in a finite number of steps depending on \( g_1, \ldots, g_n, g \).

4. Conclusion

Groups defined by generators and relations arise from topological and geometric contexts. It is perhaps therefore not altogether surprising that the Baumslag–Solitar groups play a role in questions concerning groups defined by particular topological or geometric conditions. In present paper we tried to solve particular combinatorial problem for Baumslag-Solitar group and we may see that relation played crucial role in approaches and methods of proofs. We hope that our work helps to prove decidability of the knapsack problem for HNN extension of groups.

**Acknowledgments**

The results of the section 2 was supported by Russian Science Foundation, grant 17-11-01117

**References**

[1] Baumslag G and Solitar D 1962 Some two-generator one-relator non-Hopfian groups Bull. Amer. Math. Soc. 68(3) pp 199–201

[2] Myasnikov A, Nikolaev A and Ushakov A 2015 Knapsack Problems in Groups Mathematics of Computation 84(292) pp 987–1016
[3] Semënov A L LOGICAL THEORIES OF ONE-PLACE FUNCTIONS ON THE SET OF NATURAL NUMBERS Mathematics of the USSR-Izvestiya 22(3) pp 623–658
[4] Lohrey M and Zetzsche G 2015 Knapsack in graph groups, HNN-extensions and amalgamated products arXiv:1509.05957
[5] Koenig D, Lohrey M and Zetzsche G Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups arXiv:1507.05145
[6] Mishchenko A and Treier A 2017 Knapsack problem for nilpotent groups. Groups, Complexity and Cryptology 9(1) pp 87–98
[7] Penzin Yu G 1973 Solvability of the theory of integers with addition, order, and multiplication by an arbitrary number Mathematical notes of the Academy of Sciences of the USSR 13(5) pp 401–405
[8] Lyndon R C and Schupp P E 1977 Combinatorial Group Theory Springer-Verlag, New York
[9] Dudkin F A 2009 Subgroups of Baumslag–Solitar groups Algebra and Logic 48(1) pp 1–19