On NP-completeness of subset sum problem for Lamplighter group

Alexei Mishchenko\(^1\), Alexander Treier\(^1\)

\(^1\) Sobolev Institute of Mathematics Siberian Branch of the Russian Academy of Sciences
Omsk, Russia

E-mail: alexei.mishenko@gmail.com, alexander.treyer@gmail.com

Abstract. In the paper “Knapsack problem for groups” A. Myasnikov, A. Nikolaev, and A. Ushakov stated a group version of well known Subset sum and Knapsack problems and many others. Actually they created a new direction of research as intersection of group theory and discrete optimization. They called the new direction as non-commutative optimization. Our work belongs to this new direction. In present paper we show that Subset sum problem is NP-complete for lamplighter group. Our result was obtained by polynomial reduction of well known Exact set cover problem which is strongly NP-complete to Subset sum problem for lamplighter group. As we expected, this result provides a convenient approach to prove NP-completeness of Subset sum problem for a wide class of groups.

1. Introduction

In present paper we investigate one of non-commutative discrete optimization problem. The main aim of the non-commutative discrete optimization is to study complexity of the classical optimization problems in non-commutative groups. For example, several classical optimization problems concerning integers transform to problems where the group of additive integers \(\mathbb{Z}\) is replaced by an arbitrary group \(G\). In the paper [1] A. Myasnikov, A. Nikolaev, and A. Ushakov stated a group version of the well known Subset sum problem, Knapsack problem and many others. The motivation for our research and initial results in this direction may be found in [1], and further results in [2, 3, 4, 5]. For reader convenience let us give some excerpt of introduction of [1]: “This direction of research is gaining in popularity in recent years. It is caused by several reasons. One of them is algorithmic reason: these are algorithmic problems which are very interesting from the computational algebra viewpoint. They unify various techniques in group theory which seem to be far apart now. On the practical level, non-commutative discrete optimization problems occur in many everyday computations in algebra, so it is important to study their computational complexity and improve the algorithms.” Let us briefly describe our previous results in this direction that may be interesting to reader. In the papers [3, 5] authors independently shown that group version of Knapsack problem is undecidable for nilpotent groups and it was surprisingly since the similar by definition Subset sum problem has polynomial complexity for nilpotent groups. As stated above, we investigate the subset sum problem (SSP, see section 3 for definition, recent results and motivation to study SSP for lamplighter group). More precisely we research complexity of subset sum problem for well known lamplighter group (see section 2 for definition of lamplighter group). We show in theorem 2 that subset sum problem is NP-complete for lamplighter group.
2. Lamplighter Group
Lamplighter group $L$ is the wreath product $\mathbb{Z}_2 \wr \mathbb{Z}$, where $\mathbb{Z}$ is additive group of integer numbers, and $\mathbb{Z}_2$ is group isomorphic to quotient group $\mathbb{Z}/2\mathbb{Z}$. The lamplighter group $L$ is metabelian and has standard presentation:

$$\langle a, t | a^2, [t^m at^{-m}, t^n at^{-n}], m, n \in \mathbb{Z} \rangle. \quad (1)$$

It is convenient for our purposes to look at the group $L$ as semidirect product of two groups $B$ and $Z$, where $B$ is direct sum of countable many copies of $\mathbb{Z}_2$. The structure of group $L$ gives very useful presentation for group which clarifies the word “lamplighter” in the name of group $L$. Let us briefly describe this presentation. To any element $g$ of $L$ we put the pair $(b, z)$ where $b$ is infinite string of ones and zeroes with finite number of ones and marked starting position, and $z$ is the integer which denotes current position of the caret in string $b$. The string $b$ is called lamp line where symbol “1” means that lamp is switched on and “0” means that lamp is switched off. The integer $z$ is called position of lamplighter. To multiply two elements $(b, z)$ and $(c, y)$ of group $L$ we need to make a right shift of the lamp line $c$ to $y$ positions and then take a sum of two strings $b$ and shifted $c$ with respect to addition in $\mathbb{Z}_2$. In other words $(b, z) \cdot (c, y) = (b + c(\rightarrow y), z + y)$.

**Example.** Let $g, h$ are elements of group $L$ and

$$g = (\ldots 011010\ldots, 1),$$

$$h = (\ldots 101110\ldots, 2).$$

Then

$$g \cdot h = (\ldots 011010\ldots + \ldots 101110(\rightarrow 2)\ldots, 1 + 2) =$$

$$= (\ldots 01101000\ldots + 00101110\ldots, 3) =$$

$$= (\ldots 01000110\ldots, 3).$$

3. The Subset sum problem
In this paper we focus on Subset sum problem for a given group $G$ which has solvable word problem. We formulate the subset sum problem as follows:

**The subset sum problem (SSP):** Given elements $g, g_1, \ldots, g_n$ of group $G$, decide if

$$g = g_1^{e_1} \cdots g_n^{e_n},$$

for some $e_1, \ldots, e_n \in \{0, 1\}$ in group $G$. Let us briefly describe previous results for Subset sum problem in groups. First of all we note that if equality problem is decidable in group $G$ for some generating set $X$ then SSP is decidable for group $G$ for words presented in alphabet $X$. This implies that SSP is decidable for lamplighter group given in presentation (1). In [1] is shown that complexity of subset sum problem for additive group of integer numbers $\mathbb{Z}$ depends whether the set $X$ of generators $Z$ is finite or infinite. If group $\mathbb{Z}$ generated by the set $X = \{1\}$ then SSP for $\mathbb{Z}$ is in polynomial time. However, if group $\mathbb{Z}$ is generated by the set $X = 2^n | n \in \mathbb{N}$ then SSP for $\mathbb{Z}$ is NP-complete. Moreover, in [1] is shown that SSP is NP-complete in metabelian groups of finite rank $r \geq 2$, the wreath product $\mathbb{Z} \wr \mathbb{Z}$, each of the Baumslag-Solitar metabelian groups $B(1, p)$, $p \geq 2$. On the other hand, in [2] is shown that SSP is in polynomial time for every finitely generated nilpotent group and for any hyperbolic group.
4. Exact Set Cover

In this section we give definition of classical discrete optimization problem which is named “exact set cover”. Let $X = \{x_1, \ldots , x_n\}$ be a finite set and $S$ be the set of subsets of $X$. We call the set $S^{*} \subseteq S$ exact cover of $X$ if the following two conditions hold:

(i) The union of all sets from $S^{*}$ is equals to $X$;
(ii) Any two sets from $S^{*}$ are disjoint.

The decision search of exact cover problem for finite set $S$ belongs to famous R. Carp list of NP-complete problems [6]. Two sets $X = \{x_1, \ldots , x_n\}$ and $S = \{A_1, \ldots , A_m\}$ are input for exact set cover problem and size of input defined as sum of numbers $n = |X|$ and $k = |S|$.

The Exact Set Cover (ESC) problem belongs to the class of strongly NP-complete problems which means that ESC is NP-complete even in the case of numeric value of the input. We note that classical Subset sum problem for integers is not strongly NP-complete and there is the pseudo-polynomial algorithm for SSP over integers. For any input $X$ and $S$ of exact set cover problem we define the input for subset sum problem for lamplighter group $L$, such that searching decision of ESC is equivalent to searching decision of SSP for group $L$.

5. Reduction

In this section we describe the polynomial reduction of classical Exact set cover problem to Subset sum problem over Lamplighter group. Let $X = \{1, \ldots , n\}$ and $S = \{A_1, \ldots , A_k\}$ be an input of Exact set cover problem. Denote by $BS$ the correspondence matrix with $k$ rows and $n$ columns. There is 1 on the $i$-th row and $j$-th column if $j \in A_i$ and 0 otherwise. On the next step we define the extended correspondence matrix $BES$. To do this we mark all elements of $A_i$ by additional index $i$ and denote by $A'_i$ the set of all marked elements from $A_i$. Denote by $S' = \{A'_1, \ldots , A'_k\}$. Finally, we put $BES = BES'$.

Example. Let $X = \{1, 2, 3, 4\}$. $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $A_3 = \{1, 2, 3\}$, $A_4 = \{4\}$. $B_S =$ 

\[
\begin{pmatrix}
A_1 & 1 & 1 & 0 & 0 \\
A_2 & 0 & 1 & 1 & 0 \\
A_3 & 1 & 1 & 1 & 0 \\
A_4 & 0 & 0 & 0 & 1
\end{pmatrix}, \quad BES = \begin{pmatrix}
A_1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
A_2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
A_3 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
A_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

Denote by $C_i$ the set of columns in $BES$ corresponded to element $i \in X$. Let $BBS_1$ be the matrix which we getting from $BES$ by inserting $n \cdot l$ columns filled by zeroes between $C_i$ and $C_{i+1}$. Denote by $\overline{0}$ zero valued vector of length $n \cdot l$.

Example. In notations of examples above, we have the following matrix $BBS$:

\[
BBS = \begin{pmatrix}
A_1 & 1 & 0 & \overline{0} & 0 & 0 & \overline{0} & 0 \\
A_2 & 0 & 0 & \overline{0} & 1 & 0 & \overline{0} & 0 \\
A_3 & 0 & 1 & \overline{0} & 0 & 0 & 1 & \overline{0} \\
A_4 & 0 & 0 & \overline{0} & 0 & 0 & \overline{0} & 1
\end{pmatrix},
\]

where $\overline{0}$ — is zero valued vector of length 32.

We continue to build an input of SSP. An input of SSP will contain two type of elements. The elements of first type $h_1, \ldots , h_k \in L$ will be corresponded with $S = \{A_1, \ldots , A_k\}$. We put $h_i = (a_i, z_i)$, where $a_i \in \mathbb{Z}^{+\infty}$, $z_i \in \mathbb{Z}$. Let $z_i = 0$ and $a_i$ is $i$-th row of matrix $BBS$, and first element of row $a_i$ of matrix $BBS$ has position 1 as element of group $L$. We will assume that 1 denotes a switched on lamp, and 0 — is switched off lamp.

Example. For examples above we have the the following elements $h_1, \ldots , h_4 \in L$: 

\[
\begin{pmatrix}
A_1 & 1 & 0 & \overline{0} & 1 & 0 & \overline{0} & 0 & \overline{0} & 0 \\
A_2 & 0 & 0 & \overline{0} & 1 & 0 & \overline{0} & 0 & \overline{0} & 0 \\
A_3 & 0 & 1 & \overline{0} & 0 & 0 & 1 & \overline{0} & 0 & \overline{0} \\
A_4 & 0 & 0 & \overline{0} & 0 & 0 & \overline{0} & 0 & \overline{0} & 1
\end{pmatrix}.
\]
Denote by $g_1, \ldots, g_e$ the second type of elements for input of SSP, where $e$ — is the number of non zero columns of matrix BBES. In other words, $e = \sum_{i=1}^{k} |A_i|$ — the sum of cardinals of for all sets from $S$. Let $\alpha(i)$ be the element number of the of the set $X$ which corresponds to $i$-th non-zero column of matrix BBES. Let $\beta(i)$ be the number of column of matrix BBES which is corresponded to $i$-th nonzero column of matrix BBES. The values $\alpha(i)$ and $\beta(i)$ are connected by the following formula: $\beta(i) = \beta(i) = l \cdot n \cdot (\alpha(i) - 1) + i$.

**Example.** In notations above, $\alpha(1) = \alpha(2) = 1, \alpha(3) = \alpha(4) = \alpha(5) = 2, \alpha(6) = \alpha(7) = 3, \alpha(8) = 4$. $\beta(1) = 1, \beta(2) = 2, \beta(3) = 2 + 32 + 1 = 35, \beta(4) = 36, \beta(5) = 37, \beta(6) = 70, \beta(7) = 71, \beta(8) = 104$.

Define $g_i = (\ldots, 010, \ldots, n)$, where position of unique 1 in the lamp line is equals to $\beta(i) - n \ast (\alpha(i) - 1)$. Finally we put $g = (0, n^2)$.

**Example.** Write down the whole input for Subset sum problem for group $L$ which is equivalent to the posted Exact set cover problem:

$$
\begin{array}{cccccccc}
1 & 2 & \ldots & 35 & 36 & 37 & \ldots & 70 & 71 & \ldots & 104 \\
\hline
h_1 &=& (1 & 0 & \emptyset & 1 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0 & 0) \\
h_2 &=& (0 & 0 & \emptyset & 0 & 1 & 0 & 0 & \emptyset & 1 & 0 & \emptyset & 0 & 0 & 0) \\
h_3 &=& (0 & 1 & \emptyset & 0 & 0 & 1 & \emptyset & 0 & 1 & \emptyset & 0 & 0 & 0 & 0) \\
h_4 &=& (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 1 & 0 & 0 & 0) \\
\end{array}
$$

\[ g_1 = (0 & 1 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_2 = (0 & 1 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_3 = (0 & 0 & \emptyset & 1 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_4 = (0 & 0 & \emptyset & 0 & 1 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_5 = (0 & 0 & \emptyset & 0 & 0 & 1 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_6 = (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 1 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_7 = (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 1 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]
\[ g_8 = (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 1 & \emptyset & 0 & 0 & 0 & 0) \]

\[ g = (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]

\[ g = (0 & 0 & \emptyset & 0 & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & \emptyset & 0 & 0 & 0) \]

The notation “$\leftarrow s$” means that positions of all lamps in the lamp line is less that position of corresponded lamps for elements $h_j$ by the number $s$. In other words the lamp line for element $h_j$ is shifted by $s$ positions to the left.

Finally we need to describe a map between decisions of Subset Sum Problem and Exact Set Cover problem. Let $E = \{\varepsilon_1, \ldots, \varepsilon_r\}$ be the decision of SSP. Then the corresponded decision of Exact Set Cover Problem will be the set $S' = \{A_{s_1}, \ldots, A_{s_r}\}$, such that $A_i \in S'$ if and only if $\varepsilon_i = 1$ in decision $E$ of SSP for group $L$.

**Example.** Decision of ESP from examples above are sets $A_3 = \{1, 2, 3\}$ and $A_4 = \{4\}$. Decision of equivalent SSP are elements $h_3, h_4, g_2, g_5, g_7$ and $g_8$.

### 6. Main results

Let us formulate main results of present paper.
Theorem 1. There is the polynomial reduction of the exact set cover problem to subset sum problem for Lamplighter group.

Theorem 2. Let $L$ be the Lamplighter group. Then the subset sum problem for group $L$ is strongly $NP$-complete.

7. Conclusion

In conclusion we want to say some words about some unsuccessful naive attempts of solving our problem and some words on the class of groups that our approach can cover with $NP$-completeness of Subset sum problem. It is not hard to show that Subset sum problem is polynomial hard for some subgroups of $L$ which is “simpler” than group $L$ and thus $NP$-completeness of SSP for lamplighter group can’t be proven by reduction to SSP for this subgroups. To demonstrate it we note that for $B < L$ (subgroup $B$ is defined above) finding decision of SSP is equivalent to solving a finite system of linear equations over $F_2$ (the finite field of order 2) and it can be solved using Gauss method in polynomial time. The subgroup of integers $\mathbb{Z}$ of $L$ is generated by $\{1\}$ and hence SSP is polynomial hard for this subgroup. On the other hand, lamplighter group is a subgroup for a wide class of solvable groups and wreath products, so our results give an answer to the question about complexity class for Subset Sum Problem for this class of groups too.

Acknowledgments

The work was supported by Russian Science Foundation, grant 14-11-00085

References

[1] Myasnikov A, Nikolaev A and Ushakov A 2015 Knapsack Problems in Groups Mathematics of Computation, 84(292) pp 987–1016
[2] Frenkel E, Nikolaev A and Ushakov A 2016 Knapsack problems in products of groups Journal of Symbolic Computation 74 pp 96–108
[3] Lohrey M and Zetzsche G 2015 Knapsack in graph groups, HNN-extensions and amalgamated products arXiv:1509.05957 Accepted in STACS16
[4] Konig D, Lohrey M and Zetzsche G Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups arXiv:1507.05145
[5] Mishchenko A and Treier A 2017 Knapsack problem for nilpotent groups Groups, Complexity and Cryptology 9 (1) pp 87–98
[6] Karp R 1972 Reducibility Among Combinatorial Problems Complexity of Computer Computations (New York: Plenum) pp 85–103