Journal of Symbolic Computation 84 (2018) 84–94

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Subset sum problem in polycyclic groups

Andrey Nikolaev, Alexander Ushakov

Stevens Institute of Technology, Hoboken, NJ 07030, USA

ARTICLE INFO

Article history:
Received 9 September 2016
Accepted 14 February 2017
Available online 24 March 2017

MSC:
03D15
20F65
20F10
20F16

Keywords:
Polycyclic groups
Nilpotent groups
Subset sum problem
NP-completeness

ABSTRACT

We consider a group-theoretic analogue of the classic subset sum problem. It is known that every virtually nilpotent group has polynomial time decidable subset sum problem. In this paper we use subgroup distortion to show that every polycyclic non-virtually-nilpotent group has **NP**-complete subset sum problem.

1. Introduction

The study of discrete optimization problems in groups was initiated in Miasnikov et al. (2015), where the authors introduced group-theoretic generalizations of the classic knapsack problem and its variations, e.g., subset sum problem and bounded submonoid membership problem. In the subsequent papers (Myasnikov et al., 2014, 2016), the authors studied generalizations of the Post correspondence problem and classic lattice problems in groups. The investigation of knapsack-type problems in groups continued in papers (Frenkel et al., 2016; König et al., 2015; Lohrey and Zetzsche, 2016; Mishchenko and Treyer, 2016a, 2016b). The computational properties of these problems, aside from being interesting in their own right, were shown to be closely related to a wide range of well-known geometric and algorithmic properties of groups. For instance, the complexity of knapsack-type problems in certain groups depends on geometric features of a group such as growth, subgroup distortion, and negative

E-mail addresses: anikolae@stevens.edu (A. Nikolaev), aushakov@stevens.edu (A. Ushakov).

http://dx.doi.org/10.1016/j.jsc.2017.03.007
0747-7171/

curvature. The Post correspondence problem in G is closely related to twisted conjugacy problem in G, equalizer problem in G, and a strong version of the word problem. Furthermore, lattice problems are related to the classic subgroup membership problem and finite state automata. We refer the reader to the aforementioned papers for details.

In this paper, we prove **NP**-completeness of the subset sum problem in any virtually polycyclic non-virtually-nilpotent group by exploiting properties of exponentially distorted subgroups. This highlights a notable connection between geometric and combinatorial properties of polycyclic groups.

1.1. Subset sum problem

Let G be a group generated by a finite set $X = \{x_1, \dots, x_n\} \subseteq G$. Elements in G can be expressed as products of the generators in X and their inverses. Hence, we can state the following combinatorial problem.

The subset sum problem SSP(G, X)**:** Given $g_1, \dots, g_k, g \in G$ decide if

$$g = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} \tag{1}$$

for some $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$.

By Miasnikov et al. (2015, Proposition 2.5), computational properties of **SSP** do not depend on the choice of a finite generating set X and, hence, the problem can be abbreviated as **SSP**(G). Also, the same paper provides a variety of examples of groups with **NP**-complete (or polynomial time) subset sum problems. For instance, **SSP** is **NP**-complete for the following groups:

(a) abelian group $\mathbb{Z}^\omega$;
(b) free metabelian non-abelian groups;
(c) wreath products of finitely generated infinite abelian groups;
(d) metabelian Baumslag–Solitar groups $BS(m, n)$ with $0 \neq m \neq n \neq 0$;
(e) metabelian group $GB = \langle a, s, t \mid [a, a^t] = 1, [s, t] = 1, as = aa^t \rangle$;
(f) Thompson's group F.

One can observe that in a number of the above examples, **NP**-completeness of **SSP** is a consequence of exponential subgroup distortion. Recently, König, Lohrey, and Zetzsche (2015) found a polycyclic group G with **NP**-complete **SSP**. Upon inspection of the proof, one can notice that exponential subgroup distortion plays a key role in their argument, as well. In the present work, we show that this is not coincidental. Specifically, in the case of polycyclic groups, we investigate subgroup distortion to give a complete description of **SSP**. We determine out that **SSP** in a polycyclic group is **NP**-complete if the group is not virtually nilpotent, and polynomial time decidable if it is. The latter is known by Miasnikov et al. (2015); it is also shown by König et al. (2015) that for virtually nilpotent groups, **SSP** is decidable in nondeterministic logspace. Our work is heavily inspired by results of Osin (2002), even though we do not, strictly speaking, rely on them.

1.2. Zero–one equation problem

Recall that a vector $v \in \mathbb{Z}^n$ is called a *zero–one* vector if each entry in v is either 0 or 1. Similarly, a square matrix $A \in \mathrm{Mat}(n, \mathbb{Z})$ is called a *zero–one* matrix if each entry in A is either 0 or 1. Let 1^n denote the vector $(1, \dots, 1) \in \mathbb{Z}^n$. The following problem is **NP**-complete (see Dasgupta et al., 2006, Section 8.3).

Zero–one equation problem (ZOE): Given a zero–one matrix $A \in \mathrm{Mat}(n, \mathbb{Z})$ decide if there exists a zero–one vector $\overline{x} \in \mathbb{Z}^n$ satisfying $A \cdot \overline{x} = 1^n$, or not.

2. Preliminary results in nilpotent groups

In this section, we prove a technical result on nilpotent groups (Proposition 3) that we use later in the proof of **NP**-hardness in Section 5.