Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups

Daniel König*[1], Markus Lohrey†[1], and Georg Zetzsche‡[2]

[1]University of Siegen, Germany
[2]Fachbereich Informatik, Technische Universität Kaiserslautern

February 23, 2019

1 Introduction

In their paper [21], Myasnikov, Nikolaev, and Ushakov started the investigation of classical discrete integer optimization problems in general non-commutative groups. Among other problems, they introduced for a finitely generated (f.g.) group G the *knapsack problem* and the *subset sum problem*. The input for the knapsack problem is a sequence of group elements $g_1, \ldots, g_k, g \in G$ and it is asked whether there exists a solution $(x_1, \ldots, x_k) \in \mathbb{N}^k$ of the equation $g_1^{x_1} \cdots g_k^{x_k} = g$. For the subset sum problem one restricts the solution to $\{0, 1\}^k$. For the particular case $G = \mathbb{Z}$ (where the additive notation $x_1 \cdot g_1 + \cdots + x_k \cdot g_k = g$ is usually prefered) these problems are NP-complete if the numbers $g_1, \ldots, g_k, g$ are encoded in binary representation. For subset sum this is shown in Karp's classical paper [12]. The statement for knapsack (in the above version) can be found in [9].

In [21] the authors enocde elements of the finitely generated group G by words over the group generators and their inverses. For $G = \mathbb{Z}$ this representation corresponds to the unary encoding of integers. It is known that for unary encoded integers, knapsack and subset sum over $\mathbb{Z}$ can be both solved in polynomial time, and the precise complexity is $\mathsf{DLOGTIME}$-uniform TC^0 [6], which is a very small complexity class that roughly speaking captures the complexity of multiplying binary coded integers. In [21], Myasnikov et al. proved the following new results:

- Subset sum and knapsack can be solved in polynomial time for every hyperbolic group.

*koenig@eti.uni-siegen.de
†lohrey@eti.uni-siegen.de
‡zetzsche@cs.uni-kl.de

- Subset sum for a virtually nilpotent group (a finite extension of a nilpotent group) can be solved in polynomial time.
- For the following groups, subset sum is NP-complete (whereas the word problem can be solved in polynomial time): free metabelian non-abelian groups of finite rank, the wreath product $\mathbb{Z} \wr \mathbb{Z}$, Thompson's group F, and the Baumslag-Solitar group $\mathrm{BS}(1, 2)$.

In this paper, we continue the investigation of knapsack and subset sum for arbitrary groups. We prove the following results, where as in [21] group elements are represented by finite words over the group generators and their inverses:

- For every virtually nilpotent group, subset sum belongs to NL (nondeterministic logspace).
- There is a polycyclic group with an NP-complete subset sum problem.
- There is a nilpotent group of class two for which knapsack is undecidable. This nilpotent group is a direct product of sufficiently many copies of the discrete Heisenberg group $H_3(\mathbb{Z})$. In [17], the second author proved that there exists a nilpotent group (of large class) for which knapsack is undecidable. Here we improve this result to class two and at the same time simplify the construction from [17]. As a byproduct of our construction, we show that there exists a fixed nilpotent group of class two together with four finitely generated abelian subgroups G_1, G_2, G_3, G_4 such that membership in the product $G_1G_2G_3G_4$ is undecidable. It is known that membership in a product of two subgroups of a polycyclic group is decidable [15].
- The knapsack problem for the the discrete Heisenberg group $H_3(\mathbb{Z})$ is decidable. In particular, together with the previous point it follows that decidability of knapsack is not preserved under direct products.
- The class of groups with a decidable knapsack problem is closed under finite extensions.
- The knapsack problem is decidable for every co-context-free group. Recall that a group is co-context-free if the complement of the word problem is a context-free language [10].

2 Nilpotent and polycyclic groups

Let A be a square matrix of dimension d over some commutative ring R. With $A[i, j]$ we denote the entry of A in row i and column j. The matrix A is called *triangular* if $A[i, j] = 0$ whenever $i > j$, i.e., all entries below the main diagonal are 0. A *unitriangular matrix* is a triangular matrix A such that $A[i, i] = 1$ for all $1 \leq i \leq d$, i.e., all entries on the main diagonal are 1. We denote the set of unitriangular matrices of dimension d over the ring R by $\mathrm{UT}_d(R)$. It is well known that for every commutative ring R, the set $\mathrm{UT}_d(R)$ is a group (with respect to matrix multiplication).

An *n-step solvable group* G is a group G that has a a subnormal series $G = G_n \rhd G_{n-1} \rhd G_{n-2} \rhd \cdots \rhd G_1 \rhd G_0 = 1$ (i.e., G_i is a normal subgroup of G_{i+1} for all $0 \leq i \leq n-1$) such that every quotient G_{i+1}/G_i is abelian ($0 \leq i \leq n-1$). If every quotient G_{i+1}/G_i is cyclic, then G is called *polycyclic*. The number of $0 \leq i \leq n-1$ such that $G_{i+1}/G_i \cong \mathbb{Z}$ is called the *Hirsch length* of G; it does not depend on the chosen subnormal series. If $G_{i+1}/G_i \cong \mathbb{Z}$ for all $0 \leq i \leq n-1$ then G is called *strongly polycyclic*. The following characterizations of the class of polycyclic groups are known:

- A group is polycyclic if and only if it is solvable and every subgroup is finitely generated.
- A group is polycyclic if and only if it is a solvable group of integer matrices; this is a famous result by Auslander and Swan [2, 23] . In particular, every polycyclic group is linear, i.e., can be embedded into a matrix group over some field.

For a group G its *lower central series* is the series $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots$ of subgroups, where $G_{i+1} = [G_i, G]$, which is the subgroup generated by all commutators $[g, h]$ with $g \in G_i$ and $h \in G$. Indeed, G_{i+1} is a normal subgroup of G_i. The group G is *nilpotent of class c*, if $G_c = 1$. Every f.g. nilpotent group is polycyclic, and every group $\mathrm{UT}_d(\mathbb{Z})$ ($d \geq 1$) is f.g. nilpotent of class $d-1$.

The group $\mathrm{UT}_3(\mathbb{Z})$ is also denoted by $H_3(\mathbb{Z})$ and called the *discrete Heisenberg group*. Thus, $H_3(\mathbb{Z})$ is the group of all (3×3)-matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

for $a, b, c, \in \mathbb{Z}$. The center $Z(H_3(R))$ of this group consists of all matrices of the form

$$\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for $c \in \mathbb{Z}$. The group $H_3(\mathbb{Z})$ is nilpotent of class two (it is in fact the free nilpotent group of class two and rank two). In other words, every commutator $ABA^{-1}B^{-1}$ ($A, B \in H_3(\mathbb{Z})$) belongs to the center $Z(H_3(\mathbb{Z}))$. The identity (3×3)-matrix will be denoted by Id_3. Clearly, a direct product of copies of $H_3(\mathbb{Z})$ and $\mathbb{Z}$ is also nilpotent of class two.

We need the following results about nilpotent groups:

Theorem 2.1 (Theorem 17.2.2 in [11]). *Every f.g. nilpotent group G has a torsion-free normal subgroup H of finite index (which is also f.g. nilpotent).*

Theorem 2.2 (Theorem 17.2.5 in [11]). *For every torsion-free f.g nilpotent group G there exists $d \geq 1$ such that G can be embedded into $\mathrm{UT}_d(\mathbb{Z})$.*

A group is *virtually nilpotent* if it has a nilpotent subgroup of finite index.

3 Subset sum and knapsack problems in groups

Let G be a f.g. group, and fix an arbitrary finite generating set Σ for G. In this paper, we consider the following computational problems for G, where elements of G are represented by finite words over $\Sigma \cup \Sigma^{-1}$:

- Subset sum problem for G (briefly $\mathbf{SSP}(G)$): Given $g_1, \ldots, g_k, g \in G$, decide whether there exist $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that $g = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$.

- Knapsack problem for G (briefly $\mathbf{KP}(G)$): Given $g_1, \ldots, g_k, g \in G$, decide whether there exist natural numbers $e_1, \ldots, e_k \geq 0$ such that $g = g_1^{e_1} \cdots g_k^{e_k}$.

These problems were studied for general f.g. groups in [21, 7], where among others the following results were shown:

- The subset sum problem for every f.g. virtually nilpotent group can be solved in polynomial time [21].

- The subset sum problem and the knapsack problem for every hyperbolic group can be solved in polynomial time [21].

- The knapsack problem can be solved in polynomial time in any free product of hyperbolic groups and finitely generated abelian groups [7].

- The subset sum problem for the following groups is NP-complete: $\mathbb{Z} \wr \mathbb{Z}$, free metabelian (but non-abelian) groups of finite rank, and Thompson's group F [21].

There is a variant of knapsack, where we ask wether for given $g_1, \ldots, g_k, g \in G$, there exist *integers* $e_1, \ldots, e_k \in \mathbb{Z}$ such that $g = g_1^{e_1} \cdots g_k^{e_k}$, i.e., whether g belongs belongs to the product of cyclic groups $\langle g_1 \rangle \cdots \langle g_k \rangle$. This second version is reducible to the above version with exponents from $\mathbb{N}$: Simply replace $g_i^{e_i}$ (with e_i from $\mathbb{Z}$) by $g_i^{c_i}(g_i^{-1})^{d_i}$ (with c_i, d_i from $\mathbb{Z}$). We will prove undecidability results for the "easier" version with integer quotients, whereas decidability results will be shown for the harder version with positive exponents.

4 Subset sum problems in nilpotent groups

In this section, we show that the subset sum problem for a finitely generated virtually nilpotent group belongs to nondeterministic logspace (NL). This is the class of all problems that can be solved on a *nondeterministic* Turing-machine with a working tape of length $O(\log n)$, where n is the length of the input, see e.g. [1] for details. Actually, we consider a problem more general than the subset sum problem: the membership problem for acyclic finite automaton, which was also studied in [7].

Recall that a *finite (nondeterministic) automaton* over a finite alphabet Σ is a tuple $\mathcal{A} = (Q, \Delta, q_0, F)$, where

- Q is a finite set of states,
- $\Delta \subseteq Q \times \Sigma^* \times Q$ is a finite set of transitions,
- $q_0 \in Q$ is the initial state, and
- $F \subseteq Q$ is the set of final states.

If the directed graph $(Q, \{(p,q) \mid \exists w \in \Sigma^* : (p,w,q) \in \Delta\})$ has no directed cycle, then the finite automaton $\mathcal{A}$ is *acyclic*. An accepting run for a word w is a sequence of transitions $(q_0, w_1, q_1), (q_1, w_2, q_2), \ldots, (q_{n-1}, w_n, q_n) \in \Delta$ such that $w = w_1 w_2 \cdots w_n$ and $q_n \in F$. The language $L(A) \subseteq \Sigma^*$ is the set of all words over Σ that have an accepting run. By splitting transitions, one can compute in logspace from a finite automaton $\mathcal{A}$ an automaton $\mathcal{B}$ such that $L(\mathcal{A}) = L(\mathcal{B})$ and all transitions of $\mathcal{B}$ are from $Q \times (\Sigma \cup \{\varepsilon\}) \times Q$. Moreover, $\mathcal{B}$ is acyclic if $\mathcal{A}$ is acyclic.

Let G be a finitely generated group, and let Σ be a finite group generating set for G. Hence, $\Sigma \cup \Sigma^{-1}$ generates G as a monoid and there is a canonical homomorphism $h : (\Sigma \cup \Sigma^{-1})^* \to G$. For a finite automaton $\mathcal{A}$ over $\Sigma \cup \Sigma^{-1}$ and a word $x \in (\Sigma \cup \Sigma^{-1})^*$ we also write $x \in_G L(\mathcal{A})$ for $h(x) \in h(L(\mathcal{A}))$. The *acyclic rational subset membership problem for* G (briefly $\mathbf{ARatMP}(G)$) is the following computational problem:

Input: An acyclic finite automaton $\mathcal{A}$ over $\Sigma \cup \Sigma^{-1}$ and a word $x \in (\Sigma \cup \Sigma^{-1})^*$.
Question: Does $x \in_G L(\mathcal{A})$ hold?

Clearly, $\mathbf{SSP}(G)$ is logspace reducible to $\mathbf{ARatMP}(G)$.

Theorem 4.1. *For every* $d \geq 1$, $\mathbf{ARatMP}(\mathsf{UT}_d(\mathbb{Z}))$ *belongs to* NL.

Proof. Let $\mathcal{A}$ be a finite automaton with n states, whose transitions are labelled with generator matrices of $\mathsf{UT}_d(\mathbb{Z})$ or the identity matrix. We nondeterministically guess a path of length at most n from the initial state of $\mathcal{A}$ to a final state of $\mathcal{A}$ and thereby multiply the matrices along the path. We only store the current state of $\mathcal{A}$, the product of the matrices seen so far, and the length of the path travelled so far (so that after n steps we can stop). The state of the automaton as well as the length of the path need $O(\log n)$ bits. Hence, we only have to show that the product matrix can be stored in logarithmic space. For this, it suffices to show that the matrix entries are bounded polynomially in n. Then, the binary coding of the matrix needs only $O(\log n)$ many bits (note that the matrix dimension d is a constant). For this, we can use the following simple result (see [16, Proposition 4.18] for a proof), which only holds for unitriangular matrices: For a $(d \times d)$-matrix $M = (a_{i,j})_{1 \leq i,j \leq d}$ over $\mathbb{Z}$ let $|M| = \sum_{i=1}^{d} \sum_{j=1}^{d} |a_{i,j}|$. Let $M_1, \ldots, M_n \in \mathsf{UT}_d(\mathbb{Z})$, $n \geq 2d$, and let $m = \max\{|M_i| \mid 1 \leq i \leq n\}$. For the product of these matrices we have

$$|M_1 M_2 \cdots M_n| \leq d + (d-1)\binom{n}{d-1} d^{2(d-2)} m^{d-1}.$$

In our situation, the matrices M_i are from a fixed set (generators and the identity matrix). Hence, m and also d are constants. Hence, the above bound is polynomial in n, which means that every entry of the product $M_1 M_2 \cdots M_n$ can be stored with $O(\log n)$ bits. □

Theorem 4.2. *Let H be a finite index subgroup of the f.g. group G (hence, H is f.g. too). Then* $\mathbf{ARatMP}(G)$ *is logspace-reducible to* $\mathbf{ARatMP}(H)$.

Proof. Let G and H be as in the statement of the theorem. Let Γ (resp., Σ) be a finite generating set for G (resp., H). Let $Hg_0, Hg_1, \ldots, Hg_n$ be a list of all right cosets of H, where $g_0 = 1$.

Let $\mathcal{A} = (Q, \Delta, q_0, F)$ be an acyclic finite automaton over the alphabet $\Gamma \cup \Gamma^{-1}$ and let $x \in (\Gamma \cup \Gamma^{-1})^*$. We can assume that $\Delta \subseteq Q \times (\Gamma \cup \Gamma^{-1} \cup \{\varepsilon\}) \times Q$. Assume that $x = yg_s$ in G, where $y \in (\Sigma \cup \Sigma^{-1})^*$. We can compute the word y and the coset representative g_s in logspace as follows: Let $x = a_1 a_2 \cdots a_m$. We store an index $i \in \{0, \ldots, n\}$, which is initially set to 0. Then, for $1 \leq j \leq m$ we do the following: If $g_i a_j = wg_k$ for $w \in (\Sigma \cup \Sigma^{-1})^*$, then we append the word w at the output tape and we set $i := k$. At the end, the word y is written on the output tape and the final index i is s such that $x = yg_s$.

We now construct a new acyclic automaton $\mathcal{B}$ over the alphabet $\Sigma \cup \Sigma^{-1}$ as follows:

- The state set is $Q \times \{g_0, g_1 \ldots, g_n\}$.
- Assume that $(p, a, q) \in \Delta$ is a transition of $\mathcal{A}$ $(a \in \Gamma \cup \Gamma^{-1} \cup \{\varepsilon\})$ and let $i \in \{0, 1, \ldots, n\}$. Assume that $g_i a = wg_j$ in G, where $w \in (\Sigma \cup \Sigma^{-1})^*$. Then, we add the transition $(\langle p, g_i \rangle, w, \langle q, g_j \rangle)$ to $\mathcal{B}$.
- The initial state of $\mathcal{B}$ is $\langle q_0, g_0 \rangle$.
- The set of final states of $\mathcal{B}$ is $F \times \{g_s\}$.

From the construction, we get $x \in_G L(\mathcal{A})$ if and only if $y \in_H L(\mathcal{B})$. □

Theorem 4.3. *Let G be finitely generated virtually nilpotent. Then, the problem* $\mathbf{ARatMP}(G)$ *is* NL*-complete.*

Proof. Hardness for NL follows immediately from the NL-hardness of the graph reachability problem for acyclic directed graphs. For the membership in NL let G be finitely generated virtually nilpotent. By Theorem 2.1 and 2.2, G has a finite index subgroup H such that H is isomorphic to a subgroup of $\mathsf{UT}_d(\mathbb{Z})$. W.l.o.g we assume that H is a subgroup of $\mathsf{UT}_d(\mathbb{Z})$. Membership in NL follows from Theorem 4.1 and Theorem 4.2. □

By Theorem 4.3, the subset sum problem for a finitely generated virtually nilpotent belongs to NL. It is open, whether this upper bound can be further improved. In particular, it is open whether the subset sum problem for the Heisenberg group $H_3(\mathbb{Z})$ can be solved in deterministic logspace. Recall from the introduction that subset sum for $\mathbb{Z}$ (and unary encoded numbers) belongs to $\mathsf{DLOGTIME}$-uniform TC^0 which is a subclass of deterministic logspace. This result generalizes easily to any f.g. abelian group.

5 Subset sum in polycyclic groups

We show in this section that there exists a polycyclic group with an NP-complete subset sum problem, which is in sharp contrast to nilpotent groups (assuming $\mathsf{NL} \neq \mathsf{NP}$). Let us start with a specific example of a polycyclic group. Consider the two matrices

$$g_a = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \text{ and } h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where $a \in \mathbb{R}$, $a \geq 2$. Let $G_a = \langle g_a, h \rangle \leq \mathsf{GL}_2(\mathbb{R})$. Let us remark that, for instance, the group G_2 is not polycyclic, see e.g. [24, p. 56]. On the other hand, we have:

Proposition 5.1 (c.f. [13])**.** *The group $G_{1+\sqrt{2}}$ is polycyclic.*

Theorem 5.2. SSP$(G_{1+\sqrt{2}})$ *is* NP*-complete.*

Proof. Let $\alpha = 1 + \sqrt{2}$. We follow the standard proof for the NP-completeness of subset sum for binary encoded integers. But we will work with real numbers of the form

$$x = \sum_{i=0}^{n} x_i \cdot \alpha^{3i},$$

where the x_i are natural numbers with $0 \leq x_i \leq 5$. The numbers x_i are uniquely determined by x in the following sense:

Claim 1: If

$$\sum_{i=0}^{n} x_i \cdot \alpha^{3i} = \sum_{i=0}^{m} y_i \cdot \alpha^{3i} \tag{5.1}$$

with $x_0, \ldots x_n, y_0, \ldots, y_m \in \{0, 1, \ldots, 5\}$ and $x_n \neq 0 \neq y_m$, then $n = m$ and $x_i = y_i$ for all $0 \leq i \leq n$.

Proof of Claim 1. Assume that the conclusion of the claim fails. Then, by canceling α-powers with highest exponent, we obtain from 5.1 an identity of the form

$$\sum_{i=0}^{n} x_i \cdot \alpha^{3i} = \sum_{i=0}^{m} y_i \cdot \alpha^{3i}$$

where $n > m$, $x_0, \ldots x_n, y_0, \ldots, y_m \in \{0, 1, \ldots, 5\}$ and $x_n \neq 0$. In order to lead this to a contradiction, it suffices to show

$$\alpha^{3n} > \sum_{i=0}^{n-1} 5 \cdot \alpha^{3i}.$$

Indeed, we have

$$\sum_{i=0}^{n-1} 5 \cdot \alpha^{3i} < \sum_{i=0}^{n-1} (\alpha^{3i} + \alpha^{3i+1} + \alpha^{3i+2}) = \sum_{i=0}^{3n-1} \alpha^{i} = \frac{\alpha^{3n} - 1}{\alpha - 1} < \alpha^{3n}.$$

Let us now take a 3CNF-formula $C = \bigwedge_{i=1}^{m} C_i$, where $C_i = (z_{i,1} \vee z_{i,2} \vee z_{i,3})$. Every $z_{i,j}$ is a literal, i.e., a boolean variable or a negated boolean variable. Let $x_1, \dots, x_n$ be the boolean variables appearing in C.

We now define numbers $u_1, \dots, u_{2n+2m}$, and t as follows, where $1 \le i \le n$ and $1 \le j \le m$:

$$\begin{aligned}
u_{2i-1} &= \alpha^{3i-3} + \sum_{x_i \in C_k} \alpha^{3n+3k-3} \\
u_{2i} &= \alpha^{3i-3} + \sum_{\overline{x}_i \in C_k} \alpha^{3n+3k-3} \\
u_{2n+2j-1} &= u_{2n+2j} = \alpha^{3n+3j-3} \\
t &= \sum_{i=1}^{n} \alpha^{3i-3} + \sum_{k=1}^{m} 3 \cdot \alpha^{3n+3k-3}
\end{aligned}$$

Claim 2: C is satisfiable if and only if there exists a subset $I \subseteq \{1, \dots, 2n+2m\}$ such that $\sum_{k \in I} u_k = t$.

Proof of Claim 2. First assume that C is satisfiable, and let $\varphi : \{x_1, \dots, x_n\} \to \{0, 1\}$ be a satisfying assignment for C. We set $\varphi(\overline{x}_i) = 1 - \varphi(x_i)$. For every clause $C_j = (z_{j,1} \vee z_{j,2} \vee z_{j,3})$ let $\gamma_j = |\{k \in \{1, 2, 3\} \mid \varphi(z_{j,k}) = 1\}|$ be the number of literals in C_j that are true under φ. Thus, we have $1 \le \gamma_j \le 3$.

We define the set I as follows, where $1 \le i \le n$ and $1 \le j \le m$:

- $2i - 1 \in I$ iff $\varphi(x_i) = 1$
- $2i \in I$ iff $\varphi(x_i) = 0$
- If $\gamma_j = 3$, then $2n + 2j - 1 \notin I$ and $2n + 2j \notin I$.
- If $\gamma_j = 2$, then $2n + 2j - 1 \in I$ and $2n + 2j \notin I$.
- If $\gamma_j = 1$, then $2n + 2j - 1 \in I$ and $2n + 2j \in I$.

With this set I we have indeed $\sum_{k \in I} u_k = t$.

For the other direction, let $I \subseteq \{1, \dots, 2n + 2m\}$ such that $\sum_{k \in I} u_k = t$. Note that in the sum $\sum_{k \in I} u_k$ no power α^{3k} can appear more than 5 times (a power $\alpha^{3n+3j-3}$ with $1 \le j \le m$ can appear at most 5 times, since it appears in 3 of the numbers $u_1, \dots, u_{2n}$ and in 2 of the numbers $u_{2n+1}, \dots, u_{2n+2m}$). This allows to use Claim 1. A comparision of t and $\sum_{k \in I} u_k$ shows that either $2i - 1 \in I$ or $2i \in I$. We define the assignment $\varphi : \{x_1, \dots, x_n\} \to \{0, 1\}$ as follows:

- $\varphi(x_i) = 1$ iff $2i - 1 \in I$
- $\varphi(x_i) = 0$ iff $2i \in I$

As above, let γ_j be the number of literals in C_j that are true under φ. Moreover, let $\delta_j = |I \cap \{2n+2j-1, 2n+2j\}|$ for $1 \leq j \leq m$. We get

$$\sum_{k \in I} u_k = \sum_{i=1}^{n} \alpha^{3i-3} + \sum_{j=1}^{m} (\gamma_j + \delta_j) \cdot \alpha^{3n+3j-3} = t = \sum_{i=1}^{n} \alpha^{3i-3} + \sum_{j=1}^{m} 3 \cdot \alpha^{3n+3j-3}.$$

Since $\delta_j \in \{0,1,2\}$ we must have $\gamma_j \geq 1$ for all $1 \leq j \leq m$. This shows that φ satisfies C.

We now map each of the numbers $u_1, \ldots, u_{2n+2m}, t$ to a word over the generators g_α, h (and their inverses) of the polycyclic group G_α. First, for $i \geq 0$ let us define

$$w_i = g_\alpha^i h g_\alpha^{-i}$$

In the group G_α we have

$$w_i = \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix}$$

Finally, take a number $Y = \sum_{i=0}^{n} y_i \cdot \alpha^i$. We define the word

$$w_Y = \prod_{i=0}^{n} w_i^{y_i}.$$

In the group G_α we have

$$w_Y = \begin{pmatrix} 1 & Y \\ 0 & 1 \end{pmatrix}.$$

The words $w_{u_1}, \ldots, w_{u_{2n+2m}}, w_t$ can be computed in polynomial time (even in logspace) from the 3CNF-formula C. Moreover, the construction implies that C is satisfiable iff there exists a subset $I \subseteq \{1, \ldots, 2n+2m\}$ such that $\sum_{k \in I} u_k = t$ iff there are $\varepsilon_1, \ldots, \varepsilon_{2n+2m} \in \{0,1\}$ such that $w_{u_1}^{\varepsilon_1} \cdots w_{u_{2n+2m}}^{\varepsilon_{2n+2m}} = w_t$ in the group G_α. □

6 Knapsack problems in nilpotent groups

The goal of this section is to prove that the knapsack problem is undecidable for a direct product of sufficiently many copies of $H_3(\mathbb{Z})$, which is nilpotent of class two.

6.1 Exponential expressions

Let $\mathcal{X}$ be a countably infinite set of variables. An *exponential expression* E over a group G is a formal product of the form

$$E = g_1^{x_1} g_2^{x_2} \cdots g_l^{x_l}$$

with $x_1, \ldots, x_l \in \mathcal{X}$ and $g_1, \ldots, g_l \in G$. We do not assume that $x_i \neq x_j$ for $i \neq j$. The group elements $g_1, \ldots, g_l$ will be also called the *base elements* of E.

The *length* of E is l. Let $\mathrm{Var}(E) = \{x_1, \dots, x_n\}$ be the set of variables that appear in E. For a finite set X with $\mathrm{Var}(E) \subseteq X \subseteq \mathcal{X}$ and $g \in G$, the set of X-*solutions* of the equation $E = g$ is the set of mappings

$$S_X(E = g) = \{\nu : X \to \mathbb{Z} \mid g_1^{\nu(x_1)} g_2^{\nu(x_2)} \cdots g_l^{\nu(x_l)} = g \text{ in } G\}.$$

Note that not every variable from X has to appear as an exponent in E. We moreover set $S(E = g) = S_{\mathrm{Var}(E)}(E = g)$.

For every $1 \leq i \leq n$ consider an exponential expression E_i over a group G_i. Then we can define the exponential expression $E = \prod_{i=1}^n E_i$ over the group $G = \prod_{i=1}^n G_i$. It is defined by replacing in E_i every occurrence of a base element $g \in G_i$ by the corresponding element

$$(\underbrace{1, \dots, 1}_{i-1 \text{ many}}, g, \underbrace{1, \dots, 1}_{n-i \text{ many}}) \in G$$

and taking the concatenation of the resulting exponential expressions. With this definition, the following lemma is obvious.

Lemma 6.1. *For $1 \leq i \leq n$ let E_i be an exponential expression over a group G_i. Let $g_i \in G_i$ for $1 \leq i \leq n$. Let $X = \bigcup_{i=1}^n \mathrm{Var}(E_i)$. Then for the exponential expression $E = \prod_{i=1}^n E_i$ and the element $g = (g_1, \dots, g_n) \in \prod_{i=1}^n G_i$ we have:*

$$S_X(E = g) = \bigcap_{i=1}^n S_X(E_i = g_i).$$

Proposition 6.2. *There are fixed constants $d, e \in \mathbb{N}$ and a fixed exponential expression E over $G = H_3(\mathbb{Z})^d \times \mathbb{Z}^e$ such that the following problem is undecidable:*

Input: A element $g \in G$.
Question: Does $S(E = g) \neq \emptyset$ hold?

Proof. Let $P(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be a fixed polynomial such that the following question is undecidable:

Input: A number $a \in \mathbb{N}$.
Question: Is there a tuple $(z_1, \dots, z_n) \in \mathbb{Z}^n$ such that $P(z_1, \dots, z_n) = a$.

By Matiyasevich's proof for the unsolvability of Hilbert's 10th problem, we know that such a polynomial exists, see [19] for details. By introducing additional variables, we can construct from the polynomial $P(x_1, \dots, x_n)$ a system $\mathcal{S}$ of equations of the form $x \cdot y = z$, $x + y = z$, $x = c$ (for $c \in \mathbb{Z}$) such that the equation $P(x_1, \dots, x_n) = a$ has a solution in $\mathbb{Z}$ if and only if the system of equations $\mathcal{S}_a := \mathcal{S} \cup \{x_0 = a\}$ has a solution in $\mathbb{Z}$. Here x_0 is a distinguished variable of $\mathcal{S}$. Let X be the set of variables that occur in $\mathcal{S}_a$.

Take an integer $a \in \mathbb{Z}$ (the input for our reduction). Assume that $\mathcal{S}_a$ contains d many equations of the form $x \cdot y = z$ and e many equations of the form $x + y = z$ or $x = c$. Enumerate all equations as $\mathcal{E}_1, \dots, \mathcal{E}_{d+e}$, where $\mathcal{E}_1, \dots, \mathcal{E}_d$

are all equations of the form $x \cdot y = z$. Let $G_i = H_3(\mathbb{Z})$ for $1 \le i \le d$ and $G_i = \mathbb{Z}$ for $d+1 \le i \le d+e$ We define for every $1 \le i \le d+e$ an element $g_i \in G_i$ and an exponential expression E_i over G_i as follows:

Case 1. $\mathcal{E}_i = (x \cdot y = z)$ and thus $G_i = H_3(\mathbb{Z})$. Then, we set $g_i = \mathrm{Id}_3$ (the identity matrix) and

$$E_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^x \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^y \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}^x \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^y \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^z.$$

One can easily check that a mapping $\nu : X \to \mathbb{Z}$ is a solution of $E_i = g_i$ if and only if $\nu(x) \cdot \nu(y) = \nu(z)$.

Case 2. $\mathcal{E}_i = (x + y = z)$ and thus $G_i = \mathbb{Z}$. Then, $g_i = 0$ and E_i is (written in additive form) $E_i = x + y - z$ (or, written multiplicatively, $E_i = a^x a^y a^{-z}$, where a is a generator of $\mathbb{Z}$). Then, a mapping $\nu : X \to \mathbb{Z}$ is a solution of $E_i = g_i$ if and only if $\nu(x) + \nu(y) = \nu(z)$.

Case 3. $\mathcal{E}_i = (x = c)$ (this includes the distinguished equation $x_0 = a$) and thus $G_i = \mathbb{Z}$. Then, $g_i = c$ and $E_i = x$ (or, written multiplicatively, $E_i = a^x$). Then, a mapping $\nu : X \to \mathbb{Z}$ is a solution of $E_i = g_i$ if and only if $\nu(x) = c$.

Let $E = \prod_{i=1}^{d} E_i$ and $g = (g_1, \dots, g_d)$. By Lemma 6.1, a mapping $\nu : X \to \mathbb{Z}$ is a solution of $E = g$ if and only if ν is a solution of the system $\mathcal{S}_a$. Also note that $g \in G$ depends on the input integer a, but the exponential expression E only depends on the fixed polynomial $P(x_1, \dots, x_n)$. □

Remark 6.3. The fixed exponential expression E from Proposition 6.2 has the following property that will be exploited in the next section: We can write $E = E_1 E_2 \cdots E_m$ such that every E_i has length at most 4 and every base element g from E_i commutes with every base element h from E_j whenever $i \neq j$. For this, note that the last matrix in the exponential expression from Case 1 is central in $H_3(\mathbb{Z})$.

6.2 Undecidability of knapsack for nilpotent groups of class two

Let $E = g_1^{x_1} g_2^{x_2} \cdots g_l^{x_l}$ be an exponential expression over the f.g. group G and let $X = \mathrm{Var}(E)$. Consider the group $G \times \mathbb{Z}^l$. For $1 \le i \le l$ let $e_i \in \mathbb{Z}^l$ be the i-th unit vector from $\mathbb{Z}^l$. For every $x \in X$ define

$$e_x = \sum_{1 \le i \le l, x_i = x} e_i \ \in \ \mathbb{Z}^l \quad \text{and} \quad h_x = (1, e_x) \in G \times \mathbb{Z}^l.$$

Note that h_x is central in $G \times \mathbb{Z}^l$. Moreover, for $1 \le i \le l$ let

$$h_i = (g_i, -e_i) \in G \times \mathbb{Z}^l.$$

Then, for a given group element $g \in G$, we have $S(E = g) \neq \emptyset$ if and only if

$$(g, 0) \in \prod_{x \in X} \langle h_x \rangle \prod_{i=1}^{l} \langle h_i \rangle.$$

By applying the above construction to the fixed exponential expression E over the fixed group $G = H_3(\mathbb{Z})^d \times \mathbb{Z}^e$ from Proposition 6.2, we obtain (note that $\mathbb{Z} \leq H_3(\mathbb{Z})$):

Theorem 6.4. *There exist a fixed constant d and a fixed list $g_1, \ldots, g_\lambda \in H_3(\mathbb{Z})^d$ of group elements such that membership in the product $\prod_{i=1}^{\lambda} \langle g_i \rangle$ is undecidable.*

In particular, we have:

Theorem 6.5. *There exists a fixed constant d such that $\mathbf{KP}(H_3(\mathbb{Z})^d)$ is undecidable.*

Finally, from the construction in the previous section, we also obtain the following undecidability result.

Theorem 6.6. *There exist a fixed constant d and a fixed list of four abelian subgroups $G_1, G_2, G_3, G_4 \leq H_3(\mathbb{Z})^d$ such that membership in the product $G_1 G_2 G_3 G_4$ is undecidable.*

Proof. Recall from Remark 6.3 that the exponential expression from Proposition 6.2 can be written as $E_1 E_2 \cdots E_m$ such that every E_i has length at most 4, and every base element g from E_i commutes with every base element h from E_j whenever $i \neq j$. The above construction implies that the sequence of group elements $g_1, g_2, \ldots, g_\lambda$ from Theorem 6.4 can be split into blocks $B_1, B_2, \ldots, B_\mu$ of length at most 4 such that every group element from block B_i commutes with every group element from B_j whenever $i \neq j$. This allows to rearrange the product of cyclic groups $\prod_{i=1}^{\lambda} \langle g_i \rangle$ as a product of four abelian subgroups G_1, G_2, G_3, G_4, where G_i is generated by all group elements, which are at the i-th position in their block. □

Remark 6.7. In contrast to Theorem 6.6, it was shown in [15] that a product of two subgroups of a polycyclic group is closed in the profinite topology. Since polycyclic groups are finitely presented it follows that membership in a product of two subgroups of a polycyclic group is decidable. This leaves open whether membership in a product of three subgroups of a polycyclic (or nilpotent) group is decidable.

Let us finally prove that the knapsack problem for the discrete Heisenberg group $H_3(\mathbb{Z})$ is decidable.

Theorem 6.8. *For every $e \geq 0$, $\mathbf{KP}(H_3(\mathbb{Z}) \times \mathbb{Z}^e)$ is decidable.*

Proof. Let us first show the result for $H_3(\mathbb{Z})$. Take matrixes $A, A_1, \ldots, A_l \in H_3(\mathbb{Z})$ and let

$$A = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad A_i = \begin{pmatrix} 1 & a_i & c_i \\ 0 & 1 & b_i \\ 0 & 0 & 1 \end{pmatrix}$$

A straightforward induction over n shows that

$$A_i^n = \begin{pmatrix} 1 & a_i \cdot n & c_i \cdot n + a_i b_i \frac{(n-1)n}{2} \\ 0 & 1 & b_i \cdot n \\ 0 & 0 & 1 \end{pmatrix}$$

Hence, there is a solution $(x_1, \ldots, x_l) \in \mathbb{N}^l$ of $A = A_1^{x_1} \cdots A_l^{x_l}$ if and only if the following system of three Diophantine equations has a solution over $\mathbb{N}$:

$$a = \sum_{i=1}^{l} a_i \cdot x_i$$

$$b = \sum_{i=1}^{l} b_i \cdot x_i$$

$$c = \sum_{i=1}^{l} c_i \cdot x_i + \sum_{i=1}^{l} a_i b_i \frac{(x_i - 1)x_i}{2} + \sum_{1 \le i < j \le l} a_i b_j x_i x_j$$

This is a Diophantine system with a single quadratic equation and two linear equations. By [4], a system consisting of a single quadratic Diophantine equation together with an arbitrary number of linear equations can be reduced to a single quadratic Diophantine equation, which has the same solutions over $\mathbb{Z}$. By [**?**], one can decide whether this quadratic Diophantine equation has a solution over $\mathbb{N}$.

Finally, the above proof also works for the group $H_3(\mathbb{Z}) \times \mathbb{Z}^e$, since we only get additional linear equations. □

Corollary 6.9. *The class of f.g. groups with a decidable knapsack problem is not closed under direct products.*

Proof. This follows directly from Theorem 6.5 and 6.8. □

7 Knapsack problems for finite extensions

We show that in contrast to direct products, decidability of the knapsack problem is preserved under finite extensions. For this, it will be convenient to consider a slightly extended version of the knapsack problem, which we will prove equivalent (with respect to polynomial time reducibility) to the knapsack problem. The *generalized knapsack problem* (briefly $\mathbf{GKP}(G)$) is the following decision problem: Given $g_1, \ldots, g_k \in G$ and $f_0, \ldots, f_k \in G$, decide whether

$$f_0 g_1^{n_1} f_1 g_2^{n_2} f_2 \cdots g_k^{n_k} f_k = 1 \tag{7.1}$$

for some $n_1, \ldots, n_k \in \mathbb{N}$. An *instance* of the generalized knapsack problem is therefore a tuple $(f_0, g_1, f_1, \ldots, g_k, f_k)$ with $f_0, \ldots, f_k \in G$ and $g_1, \ldots, g_k \in G$. If (7.1) holds, we call the tuple $(n_1, \ldots, n_k)$ a *solution*. If two instances have the same set of solutions, we call them *equivalent*.

Proposition 7.1. *$\mathbf{KP}(G)$ and $\mathbf{GKP}(G)$ are inter-reducible in polynomial time.*

Proof. Since $g_1^{n_1} \cdots g_k^{n_k} = g$ if and only if $g^{-1} g_1^{n_1} \cdots g_k^{n_k} = 1$, $\mathbf{KP}(G)$ clearly reduces to $\mathbf{GKP}(G)$ in polynomial time.

Let us reduce $\mathbf{GKP}(G)$ to $\mathbf{KP}(G)$. Let $(f_0, g_1, f_1, \ldots, g_k, f_k)$ be an instance of $\mathbf{GKP}(G)$. Observe that since $g_i^{n_i} f_i = f_i (f_i^{-1} g_i f_i)^{n_i}$, if we replace f_{i-1}, g_i, and f_i by $f_{i-1} f_i$, $f_i^{-1} g_i f_i$ and 1, respectively, we obtain an equivalent instance in which $f_i = 1$. By repeating this step k times, starting with f_k, we arrive at an instance with $f_1 = \cdots = f_k = 1$. Then, clearly, $f_0 g_1^{n_1} \cdots g_k^{n_k} = 1$ is equivalent to $g_1^{n_1} \cdots g_k^{n_k} = f_0^{-1}$. □

From now on, let G be finitely generated and H be a finite index subgroup of G, which is therefore finitely generated too. Furthermore, let $R \subseteq G$ be a finite set of representatives of right cosets of H in G. Then for each $g \in G$, there is a unique $\rho(g) \in R$ such that $g \in H\rho(g)$. Also recall from the proof of Theorem 4.2 that from a given element $g \in G$ we can compute effectively a decomposition $g = hr$ with $h \in H$ and $r \in R$. This fact will be implicitly used throughout this section.

Lemma 7.2. *Let $g_1, g_2 \in G$ and $\rho(g_1 g_2) = \rho(g_1)$. We can compute $h_1, h_2 \in H$ and $r \in R$ such that $g_1 g_2^t = h_1 h_2^t r$ for every $t \geq 0$.*

Proof. Since $\rho(g_1 g_2) = \rho(g_1)$, we can write $g_1 = h_1 r$ and $g_1 g_2 = h_{12} r$ for $h_1, h_{12} \in H$ and $r \in R$. Moreover, we can find $h_2 \in H$ and $r_2 \in R$ with $r g_2 = h_2 r_2$. Then

$$h_{12} r = g_1 g_2 = h_1 r g_2 = h_1 h_2 r_2$$

and hence $r_2 = r$. This means $r g_2 = h_2 r$ and thus $r g_2^t = h_2^t r$ and

$$g_1 g_2^t = h_1 r g_2^t = h_1 h_2^t r.$$

□

Theorem 7.3. *Let H be a finite-index subgroup of a finitely generated group G. Then $\mathbf{KP}(G)$ is decidable if and only if $\mathbf{KP}(H)$ is decidable.*

Proof. Since the "only if" direction is trivial, it remains to prove the "if" direction. According to Proposition 7.1, it suffices to show that if $\mathbf{GKP}(H)$ is decidable, then $\mathbf{GKP}(G)$ is decidable.

We say that an instance $I = (f_0, g_1, f_1, \ldots, g_k, f_k)$ of $\mathbf{GKP}(G)$ is *j-pure* if $f_0, g_1, \ldots, f_{j-1}, g_j \in H$. In particular, every instance is 0-pure. We call an instance *pure* if it is k-pure. If an instance is j-pure, but not $(j+1)$-pure, then $k-j$ is its *impurity*.

First, we prove the following claim by induction on the impurity of I: For every instance $I = (f_0, g_1, f_1, \ldots, g_k, f_k)$ of $\mathbf{GKP}(G)$, we can construct finitely many pure instances of $\mathbf{GKP}(G)$ such that the solution set of I is the union of affine images of their solution sets.

Suppose I is j-pure but not $(j+1)$-pure. Write $f_j = hr$ for $h \in H$ and $r \in R$. Since R is finite, there are $m, \ell \in \mathbb{N}$ with $\rho(rg_{j+1}^m) = \rho(rg_{j+1}^{m+\ell})$. We use Lemma 7.2 to find $h_1, h_2 \in H$ and $r' \in R$ such that $rg_{j+1}^{m+t\ell} = h_1 h_2^t r'$ for all $t \geq 0$. In particular

$$f_j g_{j+1}^{m+t\ell} = hrg_{j+1}^{m+t\ell} = hh_1 h_2^t r'.$$

We can also find for each $0 \leq s < m$ elements $\hat{h}_s \in H$ and $\hat{r}_s \in R$ with $rg_{j+1}^s = \hat{h}_s \hat{r}_s$. Finally, we can find for each $0 \leq s < \ell$ a decomposition $r' g_{j+1}^s = \bar{h}_s \bar{r}_s$ with $\bar{h}_s \in H$, $\bar{r}_s \in R$. Note that each element $f_j g_{j+1}^n$ can be written in one of the following forms:

$$\begin{aligned} f_j g_{j+1}^n &= h\hat{h}_s \hat{r}_s && \text{for some } 0 \leq s < m, \\ f_j g_{j+1}^n &= hh_1 h_2^t \bar{h}_s \bar{r}_s && \text{for some } 0 \leq s < \ell \text{ and } t \geq 0. \end{aligned}$$

Here, the first equality holds if $n < m$ and the second one holds if $n \geq m$ and $n = m + t\ell + s$ with $0 \leq s < \ell$.

We therefore construct two types of instances. The first type consists of the instances

$$(f_0, g_1, f_1, \ldots, g_{j-1}, f_{j-1}, g_j, h\hat{h}_s \hat{r}_s f_{j+1}, g_{j+2}, f_{j+2}, \ldots, g_k, f_k),$$

for $0 \leq s < m$. The second type consists of instances

$$(f_0, g_1, f_1, \ldots, g_{j-1}, f_{j-1}, g_j, hh_1, h_2, \bar{h}_s \bar{r}_s f_{j+1}, g_{j+2}, f_{j+2}, \ldots, g_k, f_k)$$

for each $0 \leq s < \ell$. Observe that I has a solution if and only if one of these new instances has one. Furthermore, each of these instances has lower impurity than I. Hence, the induction hypothesis yields the desired finite set of instances. This proves our claim.

Let us now prove the theorem. Given an instance I of $\mathbf{GKP}(G)$, we construct pure instances $I_1, \ldots, I_m$ of $\mathbf{GKP}(G)$ such that I has a solution if and only if one of $I_1, \ldots, I_m$ has one. Since I_i is pure, if $I_i = (f_0, g_1, f_1, \ldots, g_k, f_k)$, then $f_0, g_1, \ldots, f_{k-1}, g_k \in H$, but f_k may not be in H. However, the equation

$$f_0 g_1^{n_1} f_1 \cdots g_k^{n_k} f_k = 1$$

can only have a solution if $f_k \in H$. Moreover, if $f_k \in H$, then I is in fact an instance of $\mathbf{GKP}(H)$. Since we can decide whether $f_k \in H$, we can pick from $I_1, \ldots, I_m$ those that are instances of $\mathbf{GKP}(H)$. This means, from I we have constructed finitely many instances of $\mathbf{GKP}(H)$ such that I has a solution if and only if one of the new instances has one. This proves the theorem. □

8 Knapsack problems for co-context-free groups

In this section, we exhibit another class of groups with a decidable knapsack problem, namely co-context-free groups, which we introduce first.

A *language* is a subset of a free monoid X^*, where X is an *alphabet*, i.e. a finite set of abstract symbols. A *context-free grammar* is a tuple $\Gamma = (N, T, P, S)$, where

- N and T are disjoint alphabets, their members are called *nonterminals* and *terminals*, respectively,
- $P \subseteq N \times (N \cup T)^*$ is a finite set of *productions*,
- $S \in N$ is the *start symbol.*

A production $(A, w) \in P$ is also denoted $A \to w$. In a context-free grammar, the productions allow us to rewrite words. Specifically, for $u, v \in (N \cup T)^*$, we write $u \Rightarrow_\Gamma v$ if there are $x, y \in (N \cup T)^*$ such that $u = xAy$ and $v = xwy$ for some production $A \to w$ in P. Furthermore, $\Rightarrow_\Gamma^*$ denotes the reflexive transitive closure of $\Rightarrow_\Gamma$. The language *generated by* Γ is then defined as

$$L(\Gamma) = \{w \in T^* \mid S \Rightarrow_\Gamma^* w\}.$$

A language is called *context-free* if it is generated by some context-free grammar.

Let Σ be a finite generating set of the group G and let $h\colon (\Sigma \cup \Sigma^{-1})^* \to G$ be the canonical monoid homomorphism. The *word problem* and the *co-word problem (with respect to* $\Sigma \cup \Sigma^{-1}$*)* of G are the languages

$$\{w \in (\Sigma \cup \Sigma^{-1})^* \mid h(w) = 1\} \quad \text{and}$$
$$\{w \in (\Sigma \cup \Sigma^{-1})^* \mid h(w) \neq 1\}$$

respectively. Since it does not depend on the chosen generating set whether the word problem or the co-word problem are context-free [10], we may define a group G to be *(co-)context-free* if its (co-)word problem is a context-free language. Co-context-free groups were introduced by Holt, Rees, Röver, and Thomas [10] and shown to significantly extend the class of context-free groups (which are, by a well-known result of Muller and Schupp and Dunwoody, precisely the virtually free groups [20, 5]): The class of co-context-free groups is closed under taking direct products, taking restricted standard wreath products with a context-free top-group, passing to finitely generated subgroups and finite index overgroups. Furthermore, Lehnert and Schweitzer [14] have shown that the Higman-Thompson groups are co-context-free as well.

Theorem 8.1. *Every co-context-free group has a decidable knapsack problem.*

Note that this means in particular that the wreath product $\mathbb{Z} \wr \mathbb{Z}$ has a decidable knapsack problem, which is in contrast to the fact that this group has an undecidable submonoid membership problem [18].

Proof of Theorem 8.1. Let W be the co-word problem of G with respect to $\Sigma \cup \Sigma^{-1}$ and let W be context-free.

We will need some terminology. A language $L \subseteq X^*$ is called *regular* if it can be obtained from the empty set and the singletons $\{x\}$, $x \in X$, by the operations

- *union*, which turns $K \subseteq X^*$ and $M \subseteq X^*$ into $K \cup M$,
- *concatenation*, which turns $K, M \subseteq X^*$ into $\{uv \mid u \in K,\ v \in M\}$, and
- *iteration*, which maps $M \subseteq X^*$ to the submonoid of X^* generated by M.

For every context-free language $L \subseteq X^*$, homomorphisms $\alpha \colon X^* \to Y^*$ and $\beta \colon Z^* \to X^*$ and regular language $K \subseteq X^*$, the languages $\alpha(L)$, $\beta^{-1}(L)$, and $L \cap K$ are context-free as well and we can effectively compute a grammar for the resulting languages [3].

Suppose we are given $g_1, \ldots, g_k, g$ as an instance of the knapsack problem. and let these elements be written as words $w_1, \ldots, w_k, w$, respectively, over $\Sigma \cup \Sigma^{-1}$. Consider the alphabets $X = \{a_1, \ldots, a_k\}$, $Y = X \cup \{a\}$, and the homomorphisms $\alpha \colon Y^* \to (\Sigma \cup \Sigma^{-1})^*$, with $\alpha(a_i) = w_i$ for $1 \leq i \leq k$ and $\alpha(a) = w^{-1}$. Here, w^{-1} is the word obtained by inverting the generators and then reversing the word. Furthermore, observe that the language $K = \{a_1\}^* \cdots \{a_k\}^* \{a\}$ is regular. Moreover, let $\beta \colon Y^* \to X^*$ be the homomorphism with $\beta(a_i) = a_i$ for $1 \leq i \leq k$ and $\beta(a) = \varepsilon$. Then, the language

$$M = \beta(\alpha^{-1}(W) \cap K) = \{a_1^{e_1} \cdots a_k^{e_k} \mid g_1^{e_1} \cdots g_k^{e_k} \neq g\}$$

is effectively context-free. Clearly, there exist $e_1, \ldots, e_k \in \mathbb{N}$ with $g_1^{e_1} \cdots g_k^{e_k} = g$ if and only if $M \neq \{a_1\}^* \cdots \{a_k\}^*$. In order to decide the latter, we will employ Parikh's Theorem.

For each $w \in X^*$, let $\Psi(w) = (e_1, \ldots, e_k)$, where e_i is the number of occurrences of a_i in w for $1 \leq i \leq k$. The resulting map $\Psi \colon X^* \to \mathbb{N}^k$ is called the *Parikh map.* Parikh's Theorem [22] states that for each context-free $L \subseteq X^*$, its *Parikh image* $\Psi(L) = \{\Psi(w) \mid w \in L\}$ is *semilinear*, meaning that it is a finite union of sets of the form

$$\{v_0 \ + \ x_1 \cdot v_1 \ + \ \cdots \ + \ x_n \cdot v_n \mid x_1, \ldots, x_n \in \mathbb{N}\},$$

where $v_0 \in \mathbb{N}^k$ and $v_1, \ldots, v_n \in \mathbb{N}^k$ are called the *base vectors* and the *period vectors*, respectively. Again, Parikh's theorem is effective, meaning that given a context-free grammar, we can compute base vectors and period vectors for its semilinear Parikh image.

Furthermore, given a semilinear set $S \subseteq \mathbb{N}^k$, its complement $\mathbb{N}^k \setminus S$ is effectively semilinear as well [8]. Since $M = \{a_1\}^* \cdots \{a_k\}^*$ if and only if $\Psi(M) = \mathbb{N}^k$, we can compute $\mathbb{N}^k \setminus \Psi(M)$ and check if it is non-empty. This concludes the proof of the theorem. □

References

[1] S. Arora and B. Barak. *Computational Complexity - A Modern Approach.* Cambridge University Press, 2009.

[2] L. Auslander. On a problem of Philip Hall. *Annals of Mathematics*, 86(2):112–116, 1967.

[3] J. Berstel. *Transductions and Context-Free Languages.* Teubner, 1979.

[4] M. Duchin, H. Liang, and M. Shapiro. Equations in nilpotent groups. *Proceedings of the American Mathematical Society*, 2014. DOI: `http://dx.doi.org/10.1090/proc/12630`.

[5] M. Dunwoody. The accessibility of finitely presented groups. *Inventiones mathematicae*, 81(3):449–457, 1985.

[6] M. Elberfeld, A. Jakoby, and T. Tantau. Algorithmic meta theorems for circuit classes of constant and logarithmic depth. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:128, 2011.

[7] E. Frenkel, A. Nikolaev, and A. Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 2015. DOI: `doi:10.1016/j.jsc.2015.05.006`.

[8] S. Ginsburg and E. H. Spanier. Semigroups, Presburger formulas, and languages. *Pacific Journal of Mathematics*, 16(2):285–296, 1966.

[9] C. Haase. *On the complexity of model checking counter automata.* PhD thesis, University of Oxford, St Catherine's College, 2011.

[10] D. F. Holt, S. Rees, C. E. Röver, and R. M. Thomas. Groups with context-free co-word problem. *Journal of the London Mathematical Society*, 71(3):643–657, 2005.

[11] M. I. Kargapolov and J. I. Merzljakov. *Fundamentals of the Theory of Groups*, volume 62 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1979.

[12] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, New York, 1972.

[13] D. König and M. Lohrey. Evaluating matrix circuits. In *Proceedings of the 21st International Conference on Computing and Combinatorics, COCOON 2015*, volume 9198 of *Lecture Notes in Computer Science*, pages 235–248. Springer, 2015.

[14] J. Lehnert and P. Schweitzer. The co-word problem for the Higman-Thompson group is context-free. *Bulletin of the London Mathematical Society*, 39(2):235–241, 2007.

[15] J. C. Lennox and J. S. Wilson. On products of subgroups in polycyclic groups. *Archiv der Mathematik*, 33(4):305–309, 1979/80.

[16] M. Lohrey. *The Compressed Word Problem for Groups.* SpringerBriefs in Mathematics. Springer, 2014.

[17] M. Lohrey. Rational subsets of unitriangular groups. *International Journal of Algebra and Computation*, 25(1-2):113–121, 2015.

[18] M. Lohrey, B. Steinberg, and G. Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243(0):191–204, 2015.

[19] Y. V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts, 1993.

[20] D. E. Muller and P. E. Schupp. Groups, the theory of ends, and context-free languages. *Journal of Computer and System Sciences*, 26(3):295–310, 1983.

[21] A. Myasnikov, A. Nikolaev, and A. Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015.

[22] R. J. Parikh. On context-free languages. *Journal of the ACM*, 13(4):570–581, 1966.

[23] R. Swan. Representations of polycyclic groups. *Proceedings of the American Mathematical Society*, 18:573–574, 1967.

[24] B. A. F. Wehrfritz. *Infinite Linear Groups.* Springer, 1977.