

## KNAPSACK PROBLEMS FOR WREATH PRODUCTS

MOSES GANARDI, DANIEL KÖNIG, MARKUS LOHREY, AND GEORG ZETZSCHE

**ABSTRACT.** In recent years, knapsack problems for (in general non-commutative) groups have attracted attention. In this paper, the knapsack problem for wreath products is studied. It turns out that decidability of knapsack is not preserved under wreath product. On the other hand, the class of knapsack-semilinear groups, where solutions sets of knapsack equations are effectively semilinear, is closed under wreath product. As a consequence, we obtain the decidability of knapsack for free solvable groups. Finally, it is shown that for every non-trivial abelian group  $G$ , knapsack (as well as the related subset sum problem) for the wreath product  $G \wr \mathbb{Z}$  is **NP**-complete.

## 1. INTRODUCTION

In [23], Myasnikov, Nikolaev, and Ushakov began the investigation of classical discrete optimization problems, which are formulated over the integers, for arbitrary (possibly non-commutative) groups. The general goal of this line of research is to study to what extent results from the commutative setting can be transferred to the non-commutative setting. Among other problems, Myasnikov et al. introduced for a finitely generated group  $G$  the *knapsack problem* and the *subset sum problem*. The input for the knapsack problem is a sequence of group elements  $g_1, \dots, g_k, g \in G$  (specified by finite words over the generators of  $G$ ) and it is asked whether there exists a solution  $(x_1, \dots, x_k) \in \mathbb{N}^k$  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 preferred) these problems are **NP**-complete (resp., **TC**<sup>0</sup>-complete) if the numbers  $g_1, \dots, g_k, g$  are encoded in binary representation [11, 8] (resp., unary notation [3]).

Another motivation is that decidability of knapsack for a group  $G$  implies that the membership problem for polycyclic subgroups of  $G$  is decidable. This follows from the well-known fact that every polycyclic group  $A$  has a generating set  $\{a_1, \dots, a_k\}$  such that every element of  $A$  can be written as  $a_1^{n_1} \cdots a_k^{n_k}$  for  $n_1, \dots, n_k \in \mathbb{N}$ , see e.g. [27, Chapter 9].

In [23], Myasnikov et al. encode elements of the finitely generated group  $G$  by words over the group generators and their inverses, which corresponds to the unary encoding of integers. There is also an encoding of words that corresponds to the binary encoding of integers, so called straight-line programs, and knapsack problems under this encodings have been studied in [18]. In this paper, we only consider the case where input words are explicitly represented. Here is a (non-complete) list of known results concerning knapsack and subset sum problems:

- Subset sum and knapsack can be solved in polynomial time for every hyperbolic group [23]. In [4] this result was extended to free products of any number of hyperbolic groups and finitely generated abelian groups.
- For every virtually nilpotent group, subset sum belongs to **NL** (nondeterministic logspace) [12]. On the other hand, there are nilpotent groups of class 2 for which knapsack is undecidable. Concrete examples are direct products of sufficiently many

---

1991 *Mathematics Subject Classification.* 20F10.

*Key words and phrases.* knapsack, wreath products, decision problems in group theory.

The fourth author is supported by a fellowship within the Postdoc-Program of the German Academic Exchange Service (DAAD) and by Labex DigiCosme, Univ. Paris-Saclay, project VERICONISS..

copies of the discrete Heisenberg group  $H_3(\mathbb{Z})$  [12], and free nilpotent groups of class 2 and sufficiently high rank [22].

- Knapsack for the discrete Heisenberg group  $H_3(\mathbb{Z})$  is decidable [12]. In particular, together with the previous point it follows that decidability of knapsack is not preserved under direct products.
- 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  $F$ , the Baumslag-Solitar group  $BS(1, 2)$  [23], and every polycyclic group that is not virtually nilpotent [26].
- Knapsack is decidable for every co-context-free group (a group is co-context-free if the set of all words over the generators that do not represent the group identity is a context-free language) [12].
- Knapsack belongs to NP for every virtually special group [18]. A group is virtually special if it is a finite extension of a subgroup of a graph group. For graph groups (also known as right-angled Artin groups) a complete classification of the complexity of knapsack was obtained in [19]: If the underlying graph contains an induced path or cycle on 4 nodes, then knapsack is NP-complete; in all other cases knapsack can be solved in polynomial time (even in LogCFL).
- Decidability of knapsack is preserved under finite extensions, HNN-extensions over finite associated subgroups and amalgamated free products over finite subgroups [18].

In this paper, we study the knapsack problem for wreath products. The wreath product is a fundamental construction in group theory and semigroup theory, see Section 4 for the definition. An important application of wreath products in group theory is the Magnus embedding theorem [20], which allows to embed the quotient group  $F_k/[N, N]$  into the wreath product  $\mathbb{Z}^k \wr (F_k/N)$ , where  $F_k$  is a free group of rank  $k$  and  $N$  is a normal subgroup of  $F_k$ . From the algorithmic point of view, wreath products have some nice properties: The word problem for a wreath product  $G \wr H$  is  $AC^0$ -reducible to the word problems for the factors  $G$  and  $H$ , and the conjugacy problem for  $G \wr H$  is  $TC^0$ -reducible to the conjugacy problems for  $G$  and  $H$  and the so called power problem for  $H$  [21].

As in the case of direct products, it turns out that decidability of knapsack is not preserved under wreath products: For this we consider direct products of the form  $H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$ , where  $H_3(\mathbb{Z})$  is the discrete 3-dimensional Heisenberg group. It was shown in [12] that for every  $\ell \geq 0$ , knapsack is decidable for  $H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$ . We prove in Section 6 that for every non-trivial group  $G$  and every sufficiently large  $\ell$ , knapsack for  $G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$  is undecidable.

By the above discussion, we need stronger assumptions on  $G$  and  $H$  to obtain decidability of knapsack for  $G \wr H$ . We exhibit a very weak condition on  $G$  and  $H$ , knapsack-semilinearity, which is sufficient for decidability of knapsack for  $G \wr H$ . A finitely generated group  $G$  is knapsack-semilinear if for every knapsack equation, the set of all solutions (a solution can be seen as an vector of natural numbers) is effectively semilinear.

Clearly, for every knapsack-semilinear group, the knapsack problem is decidable. While the converse is not true, the class of knapsack-semilinear groups is extraordinarily wide. The simplest examples are finitely generated abelian groups, but it also includes the rich class of virtually special groups [18], all hyperbolic groups (see Appendix A), and all co-context-free groups [12]. Furthermore, it is known to be closed under direct products (an easy observation), finite extensions, HNN-extensions over finite associated subgroups and amalgamated free products over finite subgroups (the last three closure properties are simple extensions of the transfer theorems in [18]). In fact, the only non-knapsack-semilinear groups with a decidable knapsack problem that we are aware of are the groups  $H_3(\mathbb{Z}) \times \mathbb{Z}^n$ .

We prove in Section 7 that the class of knapsack-semilinear groups is closed under wreath products. As a direct consequence of the Magnus embedding, it follows that knapsack is

decidable for every free solvable group. Recall, that in contrast, knapsack for free nilpotent groups is in general undecidable [22].

Finally, we consider the complexity of knapsack for wreath products. We prove that for every non-trivial finitely generated abelian group  $G$ , knapsack for  $G \wr \mathbb{Z}$  is NP-complete (the hard part is membership in NP). This result includes important special cases like for instance the lamplighter group  $\mathbb{Z}_2 \wr \mathbb{Z}$  and  $\mathbb{Z} \wr \mathbb{Z}$ . Wreath products of the form  $G \wr \mathbb{Z}$  with  $G$  abelian turn out to be important in connection with subgroup distortion [1]. Our proof also shows that for every non-trivial finitely generated abelian group  $G$ , the subset sum problem for  $G \wr \mathbb{Z}$  is NP-complete. In [23] this result is only shown for infinite abelian groups  $G$ .

## 2. PRELIMINARIES

We assume standard notions concerning groups. A group  $G$  is *finitely generated* if there exists a finite subset  $\Sigma \subseteq G$  such that every element  $g \in G$  can be written as  $g = a_1 a_2 \cdots a_n$  with  $a_1, a_2, \dots, a_n \in \Sigma$ . We also say that the word  $a_1 a_2 \cdots a_n \in \Sigma^*$  evaluates to  $g$  (or represents  $g$ ). The set  $\Sigma$  is called a finite generating set of  $G$ . We always assume that  $\Sigma$  is symmetric in the sense that  $a \in \Sigma$  implies  $a^{-1} \in \Sigma$ . An element  $g \in G$  is called *torsion element* if there is an  $n \geq 1$  with  $g^n = 1$ . The smallest such  $n$  is the *order* of  $g$  and denoted  $\text{ord}(g)$ . If  $g$  is not a torsion element, we set  $\text{ord}(g) = \infty$ .

A set of vectors  $A \subseteq \mathbb{N}^k$  is *linear* if there exist vectors  $v_0, \dots, v_n \in \mathbb{N}^k$  such that

$$A = \{v_0 + \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n \mid \lambda_1, \dots, \lambda_n \in \mathbb{N}\}.$$

The tuple of vectors  $(v_0, \dots, v_n)$  is a *linear representation* of  $A$ . A set  $A \subseteq \mathbb{N}^k$  is *semilinear* if it is a finite union of linear sets  $A_1, \dots, A_m$ . A *semilinear representation* of  $A$  is a list of linear representations for the linear sets  $A_1, \dots, A_m$ . It is well-known that the semilinear subsets of  $\mathbb{N}^k$  are exactly the sets definable in *Presburger arithmetic*. These are those sets that can be defined with a first-order formula  $\varphi(x_1, \dots, x_k)$  over the structure  $(\mathbb{N}, 0, +, \leq)$  [7]. Moreover, the transformations between such a first-order formula and an equivalent semilinear representation are effective. In particular, the semilinear sets are effectively closed under Boolean operations.

## 3. KNAPSACK FOR GROUPS

Let  $G$  be a finitely generated group with the finite symmetric generating set  $\Sigma$ . Moreover, let  $V$  be a set of formal variables that take values from  $\mathbb{N}$ . For a subset  $U \subseteq V$ , we use  $\mathbb{N}^U$  to denote the set of maps  $\nu: U \rightarrow \mathbb{N}$ , which we call *valuations*. An *exponent expression* over  $G$  is a formal expression of the form  $E = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$  with  $k \geq 0$  and words  $u_i, v_i \in \Sigma^*$ . Here, the variables do not have to be pairwise distinct. If every variable in an exponent expression occurs at most once, it is called a *knapsack expression*. Let  $V_E = \{x_1, \dots, x_k\}$  be the set of variables that occur in  $E$ . For a valuation  $\nu \in \mathbb{N}^{V_E}$  such that  $V_E \subseteq U$  (in which case we also say that  $\nu$  is a valuation for  $E$ ), we define  $\nu(E) = v_0 u_1^{\nu(x_1)} v_1 u_2^{\nu(x_2)} v_2 \cdots u_k^{\nu(x_k)} v_k \in \Sigma^*$ . We say that  $\nu$  is a *solution* of the equation  $E = 1$  if  $\nu(E)$  evaluates to the identity element 1 of  $G$ . With  $\text{Sol}(E)$  we denote the set of all solutions  $\nu \in \mathbb{N}^{V_E}$  of  $E$ . We can view  $\text{Sol}(E)$  as a subset of  $\mathbb{N}^k$ . The *length* of  $E$  is defined as  $|E| = |v_0| + \sum_{i=1}^k |u_i| + |v_i|$ , whereas  $k$  is its *depth*. If the length of a knapsack expression is not needed, we will write an exponent expression over  $G$  also as  $E = h_0 g_1^{x_1} h_1 g_2^{x_2} h_2 \cdots g_k^{x_k} h_k$  where  $g_i, h_i \in G$ . We define *solvability of exponent equations over  $G$* ,  $\text{EXPEQ}(G)$  for short, as the following decision problem:

**Input:** A finite list of exponent expressions  $E_1, \dots, E_n$  over  $G$ .

**Question:** Is  $\bigcap_{i=1}^n \text{Sol}(E_i)$  non-empty?

The knapsack problem for  $G$ ,  $\text{KP}(G)$  for short, is the following decision problem:

**Input:** A single knapsack expression  $E$  over  $G$ .

**Question:** Is  $\text{Sol}(E)$  non-empty?

We also consider the uniform knapsack problem for powers

$$G^m = \underbrace{G \times \cdots \times G}_{m \text{ many}}.$$

We denote this problem with  $\text{KP}(G^*)$ . Formally, it is defined as follows:

**Input:** A number  $m \geq 0$  (represented in unary notation) and a knapsack expression  $E$  over the group  $G^m$ .

**Question:** Is  $\text{Sol}(E)$  non-empty?

It turns out that the problems  $\text{KP}(G^*)$  and  $\text{EXPEQ}(G)$  are interreducible:

**Proposition 3.1.** *For every finitely generated group  $G$ ,  $\text{KP}(G^*)$  is decidable if and only if  $\text{EXPEQ}(G)$  is decidable.*

*Proof.* Clearly, every instance of  $\text{KP}(G^*)$  can be translated to an instance of  $\text{EXPEQ}(G)$  by projecting onto the  $m$  factors of a power  $G^m$ . For the converse direction, assume that  $\text{KP}(G^*)$  is decidable. Then in particular,  $G$  has a decidable word problem. Let  $E_j = h_{0,j} g_{1,j}^{x_{1,j}} h_{1,j} \cdots g_{k,j}^{x_{k,j}} h_{k,j}$  be an exponent expression over  $G$  for every  $j \in [1, m]$ . By adding dummy powers of the form  $1^x$  we may assume that the  $E_j$  have the same depth  $k$ . We distinguish two cases.

*Case 1.*  $G$  is a torsion group. Since  $G$  has a decidable word problem, we can compute  $\ell \in \mathbb{N}$  so that  $g_{i,j}^\ell = 1$  for every  $i \in [1, k]$  and  $j \in [1, m]$ . Then there is a solution to the exponent equation system if and only if there is a solution  $\nu$  with  $0 \leq \nu(x) < \ell$  for every variable  $x$ . Hence, solvability is clearly decidable.

*Case 2.* There is some  $a \in G$  with  $\text{ord}(a) = \infty$ . We first rename the variables in  $E_1, \dots, E_m$  such that every variable occurs at most once in the entire system of expressions. Let  $E'_1, \dots, E'_m$  be the resulting system of knapsack expressions and let  $U$  be the set of variables that occur in  $E'_1, \dots, E'_m$ . We can compute an equivalence relation  $\sim \subseteq U \times U$  such that the system  $E_1 = 1, \dots, E_m = 1$  has a solution if and only if the system  $E'_1 = 1, \dots, E'_m = 1$  has a solution  $\nu$  with  $\nu(x) = \nu(x')$  for  $x \sim x'$ . We can equip  $U$  with a linear order  $\leq$  so that if  $x$  occurs left of  $x'$  in some  $E'_j$ , then  $x < x'$ .

Now for each pair  $(x, x') \in U \times U$  with  $x \sim x'$  and  $x < x'$ , we add the knapsack expression  $a^x (a^{-1})^{x'}$ . This yields knapsack expressions  $E'_1, \dots, E'_{m+\ell}$  for some  $\ell \geq 0$  such that  $E'_1 = 1, \dots, E'_{m+\ell} = 1$  is solvable if and only if  $E_1 = 1, \dots, E_m = 1$  is solvable. Moreover, whenever  $x$  occurs to the left of  $x'$  in some expression, then  $x < x'$ .

By padding the expressions with trivial powers, we turn  $E'_1, \dots, E'_{m+\ell}$  into expressions  $E''_1, \dots, E''_{m+\ell}$  that all exhibit the same variables (in the same order). Now, it is easy to turn  $E''_1, \dots, E''_{m+\ell}$  into a single knapsack expression over  $G^{m+\ell}$ .  $\square$

Note that the equation  $v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k = 1$  is equivalent to

$$(v_0 u_1 v_0^{-1})^{x_1} (v_0 v_1 u_2 v_1^{-1} v_0^{-1})^{x_2} \cdots (v_0 \cdots v_{k-1} u_k v_{k-1}^{-1} \cdots v_0^{-1})^{x_k} (v_0 \cdots v_k) = 1.$$

Hence, it suffices to consider exponent expressions of the form  $u_1^{x_1} u_2^{x_2} \cdots u_k^{x_k} v$ .

The group  $G$  is called *knapsack-semilinear* if for every knapsack expression  $E$  over  $G$ , the set  $\text{Sol}(E)$  is a semilinear set of vectors and a semilinear representation can be effectively computed from  $E$ . The following classes of groups only contain knapsack-semilinear groups:

- virtually special groups [17]: these are finite extensions of subgroups of graph groups (aka right-angled Artin groups). The class of virtually special groups is very rich. It contains all Coxeter groups, one-relator groups with torsion, fully residually free groups, and fundamental groups of hyperbolic 3-manifolds.
- hyperbolic groups: see Appendix A
- co-context-free groups [12], i.e., groups where the set of all words over the generators that do not represent the identity is a context-free language. Lehnert and Schweitzer [14] have shown that the Higman-Thompson groups are co-context-free.

Since the emptiness of the intersection of finitely many semilinear sets is decidable, we have:

**Lemma 3.2.** *If  $G$  is knapsack-semilinear, then  $\text{KP}(G^*)$  and  $\text{EXPEQ}(G)$  are decidable.*

An example of a group  $G$ , where  $\text{KP}(G)$  is decidable but  $\text{KP}(G^*)$  (and hence  $\text{EXPEQ}(G)$ ) are undecidable is the Heisenberg group  $H_3(\mathbb{Z})$ , see [12]. It is the group of all matrices of the following form, where  $a, b, c \in \mathbb{Z}$ :

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

In particular,  $H_3(\mathbb{Z})$  is not knapsack-semilinear.

#### 4. WREATH PRODUCTS

Let  $G$  and  $H$  be groups. Consider the direct sum  $K = \bigoplus_{h \in H} G_h$ , where  $G_h$  is a copy of  $G$ . We view  $K$  as the set  $G^{(H)}$  of all mappings  $f: H \rightarrow G$  such that  $\text{supp}(f) = \{h \in H \mid f(h) \neq 1\}$  is finite, together with pointwise multiplication as the group operation. The set  $\text{supp}(f) \subseteq H$  is called the *support* of  $f$ . The group  $H$  has a natural left action on  $G^{(H)}$  given by  $hf(a) = f(h^{-1}a)$ , where  $f \in G^{(H)}$  and  $h, a \in H$ . The corresponding semidirect product  $G^{(H)} \rtimes H$  is the *wreath product*  $G \wr H$ . In other words:

- Elements of  $G \wr H$  are pairs  $(f, h)$ , where  $h \in H$  and  $f \in G^{(H)}$ .
- The multiplication in  $G \wr H$  is defined as follows: Let  $(f_1, h_1), (f_2, h_2) \in G \wr H$ . Then  $(f_1, h_1)(f_2, h_2) = (f, h_1h_2)$ , where  $f(a) = f_1(a)f_2(h_1^{-1}a)$ .

The following intuition might be helpful: An element  $(f, h) \in G \wr H$  can be thought of as a finite multiset of elements of  $G \setminus \{1_G\}$  that are sitting at certain elements of  $H$  (the mapping  $f$ ) together with the distinguished element  $h \in H$ , which can be thought of as a cursor moving in  $H$ . If we want to compute the product  $(f_1, h_1)(f_2, h_2)$ , we do this as follows: First, we shift the finite collection of  $G$ -elements that corresponds to the mapping  $f_2$  by  $h_1$ : If the element  $g \in G \setminus \{1_G\}$  is sitting at  $a \in H$  (i.e.,  $f_2(a) = g$ ), then we remove  $g$  from  $a$  and put it to the new location  $h_1a \in H$ . This new collection corresponds to the mapping  $f'_2: a \mapsto f_2(h_1^{-1}a)$ . After this shift, we multiply the two collections of  $G$ -elements pointwise: If in  $a \in H$  the elements  $g_1$  and  $g_2$  are sitting (i.e.,  $f_1(a) = g_1$  and  $f'_2(a) = g_2$ ), then we put the product  $g_1g_2$  into the location  $a$ . Finally, the new distinguished  $H$ -element (the new cursor position) becomes  $h_1h_2$ .

By identifying  $f \in G^{(H)}$  with  $(f, 1_H) \in G \wr H$  and  $h \in H$  with  $(1_{G^{(H)}}, h)$ , we regard  $G^{(H)}$  and  $H$  as subgroups of  $G \wr H$ . Hence, for  $f \in G^{(H)}$  and  $h \in H$ , we have  $fh = (f, 1_H)(1_{G^{(H)}}, h) = (f, h)$ . There are two natural projection morphism  $\sigma_{G \wr H}: G \wr H \rightarrow H$  and  $\tau_{G \wr H}: G \wr H \rightarrow G^{(H)}$  with

$$\begin{aligned} (1) \quad \sigma_{G \wr H}(f, h) &= h, \\ (2) \quad \tau_{G \wr H}(f, h) &= f. \end{aligned}$$

If  $G$  (resp.  $H$ ) is generated by the set  $\Sigma$  (resp.  $\Gamma$ ) with  $\Sigma \cap \Gamma = \emptyset$ , then  $G \wr H$  is generated by the set  $\{(f_a, 1_H) \mid a \in \Sigma\} \cup \{(f_{1_G}, b) \mid b \in \Gamma\}$ , where for  $g \in G$ , the mapping  $f_g: H \rightarrow G$  is defined by  $f_g(1_H) = g$  and  $f_g(x) = 1_G$  for  $x \in H \setminus \{1_H\}$ . This generating set can be identified with  $\Sigma \uplus \Gamma$ . We will need the following embedding lemma:

**Lemma 4.1.** *Let  $G, H, K$  be finitely generated groups where  $K$  has a decidable word problem. Then, given  $n \in \mathbb{N}$  with  $n \leq |K|$ , one can compute an embedding of  $G^n \wr H$  into  $G \wr (H \times K)$ .*

*Proof.* Let  $\Sigma$ ,  $\Gamma$ , and  $\Theta$  be finite generating sets of  $G$ ,  $H$ , and  $K$ , respectively. Suppose  $n \in \mathbb{N}$  is given. Since  $K$  has a decidable word problem and  $|K| \geq n$ , we can compute words  $w_1, \dots, w_n \in \Theta^*$  that represent pairwise distinct elements  $k_1, \dots, k_n$  of  $K$ .

Let  $\pi_i: G^n \rightarrow G$  be the projection on the  $i$ -th coordinate. Since the statement of the lemma does not depend on the chosen generating sets of  $G^n \wr H$  and  $G \wr (H \times K)$ , we may

choose one. The group  $G^n$  is generated by the tuples  $s_i := (1, \dots, 1, s, 1, \dots, 1) \in G^n$ , for  $s \in \Sigma$  and  $i \in [1, n]$ , where  $s$  is at the  $i$ -th coordinate. Hence,  $\Delta = \{s_i \mid s \in \Sigma, i \in [1, n]\} \uplus \Gamma$  is a finite generating set of  $G^n \wr H$ .

The embedding  $\iota: \Delta^* \rightarrow (\Sigma \cup \Gamma \cup \Theta)^*$  is defined by  $\iota(s_i) = w_i s w_i^{-1}$  for  $s \in \Sigma, i \in [1, n]$  and  $\iota(t) = t$  for  $t \in \Gamma$ . It remains to be shown that  $\iota$  induces an embedding of  $G^n \wr H$  into  $G \wr (H \times K)$ .

Consider the injective morphism  $\varphi: (G^n)^{(H)} \rightarrow G^{(H \times K)}$  where for  $\zeta \in (G^n)^{(H)}$ , we have

$$[\varphi(\zeta)](h, k) = \begin{cases} \pi_i(\zeta(h)) & \text{if } k = k_i \\ 1 & \text{if } k \notin \{k_1, \dots, k_n\} \end{cases}$$

We claim that  $\varphi$  extends to an injective morphism  $\hat{\varphi}: (G^n)^{(H)} \rtimes H \rightarrow G^{(H \times K)} \rtimes H$  where  $H$  acts on  $G^{(H \times K)}$  by  $(h\zeta)(a, k) = \zeta(h^{-1}a, k)$  for  $h, a \in H, k \in K$ . To show this, it suffices to establish  $\varphi(h\zeta) = h\varphi(\zeta)$  for all  $\zeta \in (G^n)^{(H)}$ ,  $h \in H$ , i.e., the action of  $H$  commutes with the morphism  $\varphi$ . To see this, note that

$$[\varphi(h\zeta)](a, k_i) = \pi_i((h\zeta)(a)) = \pi_i(\zeta(h^{-1}a)) = [\varphi(\zeta)](h^{-1}a, k_i) = [h\varphi(\zeta)](a, k_i)$$

and if  $k \notin \{k_1, \dots, k_n\}$ , we have

$$[\varphi(h\zeta)](a, k) = 1 = [\varphi(\zeta)](h^{-1}a, k) = [h\varphi(\zeta)](a, k).$$

Since the above action of  $H$  on  $G^{(H \times K)}$  is the restriction of the action of  $H \times K$  on  $G^{(H \times K)}$ , we have  $G^{(H \times K)} \rtimes H \leq G^{(H \times K)} \rtimes (H \times K) = G \wr (H \times K)$ . Thus  $\hat{\varphi}$  can be viewed as an embedding  $\hat{\varphi}: G^n \wr H \rightarrow G \wr (H \times K)$ .

We complete the proof by showing that  $\iota$  represents  $\hat{\varphi}$ , i.e.  $\hat{\varphi}(\overline{w}) = \overline{\iota(w)}$  for every  $w \in \Delta^*$ , where  $\overline{w}$  denotes the element of  $(G^n)^{(H)} \rtimes H$  represented by the word  $w$  and similarly for  $\iota(w)$ . It suffices to prove this in the case  $w \in \Delta \subseteq (G^n)^{(H)} \rtimes H$ . If  $w = s_i$  with  $s \in \Sigma, i \in [1, n]$ , we observe that  $\hat{\varphi}(s_i) = k_i s k_i^{-1} = \overline{\iota(s_i)}$ . Moreover, for  $t \in \Gamma \subseteq H$  we have  $\hat{\varphi}(t) = t = \iota(t)$ .  $\square$

## 5. MAIN RESULTS

In this section, we state the main results of the paper. We begin with a general necessary condition for knapsack to be decidable for a wreath product. Note that if  $H$  is finite, then  $G \wr H$  is a finite extension of  $G^{|H|}$  [16, Proposition 1], meaning that  $\text{KP}(G \wr H)$  is decidable if and only if  $\text{KP}(G^{|H|})$  is decidable [18, Theorem 11]<sup>1</sup>. Therefore, we are only interested in the case that  $H$  is infinite.

**Proposition 5.1.** *Suppose  $H$  is infinite. If  $\text{KP}(G \wr H)$  is decidable, then  $\text{KP}(H)$  and  $\text{KP}(G^*)$  are decidable.*

*Proof.* As a subgroup of  $G \wr H$ ,  $H$  inherits decidability of the knapsack problem. According to Lemma 4.1, given  $m \in \mathbb{N}$ , we can compute an embedding of  $G^m$  into  $G \wr H$  and thus solve knapsack instances over  $G^m$  uniformly in  $m$ .  $\square$

Proposition 5.1 shows that  $\text{KP}(H_3(\mathbb{Z}) \wr \mathbb{Z})$  is undecidable: It was shown in [12] that  $\text{KP}(H_3(\mathbb{Z}))$  is decidable, whereas for some  $m > 1$ , the problem  $\text{KP}(H_3(\mathbb{Z})^m)$  is undecidable.

Proposition 5.1 raises the question whether decidability of  $\text{KP}(H)$  and  $\text{KP}(G^*)$  implies decidability of  $\text{KP}(G \wr H)$ . The answer turns out to be negative. Let us first recall the following result from [12]:

**Theorem 5.2** ([12]). *For every  $\ell \in \mathbb{N}$ ,  $\text{KP}(H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$  is decidable.*

Hence, by the following result, which is shown in Section 6, decidability of  $\text{KP}(H)$  and  $\text{KP}(G^*)$  does in general not imply decidability of  $\text{KP}(G \wr H)$ :

<sup>1</sup>Strictly speaking, only preservation of NP-membership was shown there. However, the proof also yields preservation of decidability.

**Theorem 5.3.** *There is an  $\ell \in \mathbb{N}$  such that for every group  $G \neq 1$ ,  $\text{KP}(G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell))$  is undecidable.*

We therefore need to strengthen the assumptions on  $H$  in order to show decidability of  $\text{KP}(G \wr H)$ . By adding the weak assumption of knapsack-semilinearity for  $H$ , we obtain a partial converse to Proposition 5.1. In Section 7 we prove:

**Theorem 5.4.** *Let  $H$  be knapsack-semilinear. Then  $\text{KP}(G \wr H)$  is decidable if and only if  $\text{KP}(G^*)$  is decidable.*

In fact, in case  $G$  is also knapsack-semilinear, our algorithm constructs a semilinear representation of the solution set. Therefore, we get:

**Theorem 5.5.** *The group  $G \wr H$  is knapsack-semilinear if and only if both  $G$  and  $H$  are knapsack-semilinear.*

Since every free abelian group is clearly knapsack-semilinear, it follows that the iterated wreath products  $G_{1,r} = \mathbb{Z}^r$  and  $G_{d+1,r} = \mathbb{Z}^r \wr G_{d,r}$  are knapsack-semilinear. By the well-known Magnus embedding, the free solvable group  $S_{d,r}$  embeds into  $G_{d,r}$ . Hence, we get:

**Corollary 5.6.** *Every free solvable group is knapsack-semilinear. Hence, solvability of exponent equations is decidable for free solvable groups.*

Finally, we consider the complexity of knapsack for wreath products. We prove NP-completeness for an important special case:

**Theorem 5.7.** *For every non-trivial finitely generated abelian group  $G$ ,  $\text{KP}(G \wr \mathbb{Z})$  is NP-complete.*

## 6. UNDECIDABILITY: PROOF OF THEOREM 5.3

Our proof of Theorem 5.3 employs the undecidability of the knapsack problem for certain powers of  $H_3(\mathbb{Z})$ . In fact, we need a slightly stronger version, which states undecidability already for knapsack instances of bounded depths.

**Theorem 6.1** ([12]). *There is a fixed constant  $m$  and a fixed list of group elements  $g_1, \dots, g_k \in H_3(\mathbb{Z})^m$  such that membership in the product  $\prod_{i=1}^k \langle g_i \rangle$  is undecidable. In particular, there are  $k, m \in \mathbb{N}$  such that solvability of knapsack instances of depth  $k$  is undecidable for  $H_3(\mathbb{Z})^m$ .*

We prove Theorem 5.3 by showing the following.

**Proposition 6.2.** *There are  $m, \ell \in \mathbb{N}$  such that for every non-trivial group  $G$ , the knapsack problem for  $G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$  is undecidable.*

Let  $k$  and  $m$  be the constants from Theorem 6.1. In order to prove Proposition 6.2, consider a knapsack expression

$$(3) \quad E = g_1^{x_1} \cdots g_k^{x_k} g_{k+1}$$

with  $g_1, \dots, g_{k+1} \in H_3(\mathbb{Z})^m$ . We can write  $g_i = (g_{i,1}, \dots, g_{i,m})$  for  $i \in [1, k+1]$ , which leads to the expressions

$$(4) \quad E_j = g_{1,j}^{x_{1,j}} \cdots g_{k,j}^{x_{k,j}} g_{k+1,j}.$$

Let  $\ell = m \cdot k$  and let  $\alpha: H_3(\mathbb{Z}) \times \mathbb{Z}^\ell \rightarrow H_3(\mathbb{Z})$  and  $\beta: H_3(\mathbb{Z}) \times \mathbb{Z}^\ell \rightarrow \mathbb{Z}^\ell$  be the projection onto the left and right component, respectively. For each  $p \in [1, \ell]$ , let  $e_p \in \mathbb{Z}^\ell$  be the  $p$ -th unit vector  $e_p = (0, \dots, 0, 1, 0, \dots, 0)$ . For  $j \in [1, m]$  we define the following knapsack expressions over  $H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$  ( $0$  denotes the zero vector of dimension  $\ell$ ):

$$E'_j = \prod_{i=1}^k (g_{i,j}, e_{(j-1)k+i})^{x_{i,j}} (g_{k+1,j}, 0) \quad \text{and} \quad M_j = \prod_{t=1}^{\ell} (1, -e_t)^{y_{j,t,0}} (1, e_t)^{y_{j,t,1}}.$$

Note that the term  $(j-1)k+i$  assumes all numbers  $1, \dots, m \cdot k$  as  $i$  ranges over  $1, \dots, k$  and  $j$  ranges over  $1, \dots, m$ .

Since  $G$  is non-trivial, there is some  $a \in G \setminus \{1\}$ . For each  $j \in [1, m]$ , let  $a_j = (1, \dots, 1, a, 1, \dots, 1) \in G^m$ , where the  $a$  is in the  $j$ -th coordinate. With this, we define

$$C = \prod_{i=1}^k \left( \prod_{j=1}^m (1, -e_{(j-1)k+i}) \right)^{z_i} \quad \text{and} \quad F = \left( \prod_{j=1}^m a_j E'_j \right) C \left( \prod_{j=1}^m a_j^{-1} M_j \right).$$

Since  $G^m$  and  $H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$  are subgroups of  $G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$ , we can treat  $F$  as a knapsack expression over  $G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$ . We will show that  $\text{Sol}(F) \neq \emptyset$  if and only if  $\text{Sol}(E) \neq \emptyset$ . For this we need another simple lemma:

**Lemma 6.3.** *Let  $G, H$  be groups and let  $a \in G \setminus \{1\}$  and  $f, g, h \in H$ . Regard  $G$  and  $H$  as subsets of  $G \wr H$ . Then  $faga^{-1}h = 1$  if and only if  $g = 1$  and  $fh = 1$ .*

*Proof.* The right-to-left direction is trivial. For the converse, suppose  $faga^{-1}h = 1$  and  $g \neq 1$ . By definition of  $G \wr H$ , we can write  $faga^{-1}h = (\zeta, p)$  with  $\zeta \in G^{(H)}$  and  $p \in H$ , where  $\zeta(f) = a \neq 1$ ,  $\zeta(fg) = a^{-1} \neq 1$ , and  $p = fgh$ . This clearly implies  $faga^{-1}h \neq 1$ , a contradiction. Hence,  $faga^{-1}h = 1$  implies  $g = 1$  and thus  $fh = 1$ .  $\square$

In the proof of the following lemma, we use the simple fact that every morphism  $\varphi: G \rightarrow G'$  extends uniquely to a morphism  $\hat{\varphi}: G \wr H \rightarrow G' \wr H$  such that  $\hat{\varphi}|_G = \varphi$  and  $\hat{\varphi}|_H = \text{id}_H$  (the identity mapping on  $H$ ).

**Lemma 6.4.** *A valuation  $\nu$  for  $F$  satisfies  $\nu(F) = 1$  if and only if for every  $i \in [1, k]$ ,  $j \in [1, m]$ ,  $t \in [1, m-1]$ , we have*

$$(5) \quad \nu(E_j) = 1, \quad \nu(x_{i,j}) = \nu(z_i),$$

$$(6) \quad \nu(M_t) = \nu(E'_t), \quad \nu(M_1 \cdots M_m) = 1.$$

*Proof.* Let  $\pi_j: G^m \rightarrow G$  be the projection morphism onto the  $j$ -th coordinate and let  $\hat{\pi}_j: G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell) \rightarrow G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$  be its extension with  $\hat{\pi}_j|_{H_3(\mathbb{Z}) \times \mathbb{Z}^\ell} = \text{id}_{H_3(\mathbb{Z}) \times \mathbb{Z}^\ell}$ . Of course, for  $g \in G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$ , we have  $g = 1$  if and only if  $\hat{\pi}_j(g) = 1$  for every  $j \in [1, m]$ . Observe that

$$\hat{\pi}_r(\nu(F)) = \nu \left( \left( \prod_{j=1}^{r-1} E'_j \right) a \left( \prod_{j=r}^m E'_j \right) C \left( \prod_{j=1}^{r-1} M_j \right) a^{-1} \left( \prod_{j=r}^m M_j \right) \right)$$

for every  $r \in [1, m]$ . Therefore, according to Lemma 6.3,  $\nu(F) = 1$  holds if and only if for every  $r \in [1, m]$ , we have

$$(7) \quad \nu(E'_1 \cdots E'_m C M_1 \cdots M_m) = 1 \quad \text{and} \quad \nu(E'_r \cdots E'_m C M_1 \cdots M_{r-1}) = 1.$$

We claim that Eq. (7) holds for all  $r \in [1, m]$  if and only if

$$(8) \quad \nu(E'_1 \cdots E'_m C) = 1, \quad \nu(E'_t) = \nu(M_t) \quad \text{and} \quad \nu(M_1 \cdots M_m) = 1$$

for all  $t \in [1, m-1]$ . First assume that Eq. (8) holds for all  $t \in [1, m-1]$ . We clearly get  $\nu(E'_1 \cdots E'_m C M_1 \cdots M_m) = 1$  and  $\nu(E'_r \cdots E'_m C M_1 \cdots M_{r-1}) = 1$  for  $r = 1$ . The equations  $\nu(E'_r \cdots E'_m C M_1 \cdots M_{r-1}) = 1$  for  $r \in [2, m]$  are obtained by conjugating  $\nu(E'_1 \cdots E'_m C) = 1$  with  $\nu(E'_1) = \nu(M_1), \dots, \nu(E'_{r-1}) = \nu(M_{r-1})$ . Now assume that Eq. (7) holds for all  $r \in [1, m]$ . Taking  $r = 1$  yields  $\nu(E'_1 \cdots E'_m C) = 1$  and hence  $\nu(M_1 \cdots M_m) = 1$ . Moreover, we have  $\nu(E'_1 \cdots E'_{r-1}) = \nu(E'_1 \cdots E'_m C M_1 \cdots M_{r-1}) = \nu(M_1 \cdots M_{r-1})$  for all  $r \in [1, m]$ , which implies  $\nu(E'_t) = \nu(M_t)$  for all  $t \in [1, m-1]$ .

Observe that by construction of  $E'_j$  and  $C$ , we have

$$(9) \quad \alpha(\nu(E'_j)) = \nu(E_j), \quad \pi_{(j-1)k+i}(\beta(\nu(E'_1 \cdots E'_m))) = \nu(x_{i,j}),$$

$$(10) \quad \alpha(\nu(C)) = 1, \quad \pi_{(j-1)k+i}(\beta(\nu(C))) = -\nu(z_i).$$

for every  $i \in [1, k]$  and  $j \in [1, m]$ .



Note that the equations in Eq. (8) only involve elements of  $H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$ . Since for elements  $g \in H_3(\mathbb{Z}) \times \mathbb{Z}^\ell$ , we have  $g = 1$  if and only if  $\alpha(g) = 1$  and  $\beta(g) = 1$ , the equation  $\nu(E'_1 \cdots E'_m C) = 1$  is equivalent to  $\alpha(\nu(E'_1 \cdots E'_m C)) = 1$  and  $\beta(\nu(E'_1 \cdots E'_m C)) = 1$ . By Eqs. (9) to (10), this is equivalent to  $\nu(E_1 \cdots E_m) = 1$  and  $\nu(x_{i,j}) = \nu(z_i)$  for all  $i \in [1, k]$  and  $j \in [1, m]$ . Finally,  $\nu(E'_t) = \nu(M_t)$  implies  $\nu(E_t) = \alpha(\nu(E'_t)) = \alpha(\nu(M_t)) = 1$  for all  $t \in [1, m-1]$  and hence also  $\nu(E_m) = 1$ . Thus, Eq. (8) is equivalent to the conditions in the lemma.  $\square$

**Lemma 6.5.**  $\text{Sol}(F) \neq \emptyset$  if and only if  $\text{Sol}(E) \neq \emptyset$ .

*Proof.* If  $\nu(F) = 1$ , then according to Lemma 6.4, the valuation also satisfies  $\nu(E_j) = 1$  and  $\nu(x_{i,j}) = \nu(z_i)$  for  $i \in [1, k]$  and  $j \in [1, m]$ . In particular  $\nu(x_{i,j}) = \nu(x_{i,j'})$  for  $j, j' \in [1, m]$ . Thus, we have

$$g_1^{\nu(x_{1,1})} \cdots g_k^{\nu(x_{k,1})} g_{k+1} = 1$$

and hence  $\text{Sol}(E) \neq \emptyset$ .

Suppose now that  $\text{Sol}(E) \neq \emptyset$ . Then there is a valuation  $\nu$  with  $\nu(E_j) = 1$  and  $\nu(x_{i,j}) = \nu(x_{i,j'})$  for  $i \in [1, k]$  and  $j, j' \in [1, m]$ . We shall prove that we can extend  $\nu$  so as to satisfy the conditions of Lemma 6.4.

The left-hand equation in Eq. (5) is fulfilled already. Since  $\nu(x_{i,j}) = \nu(x_{i,j'})$ , setting  $\nu(z_i) = \nu(x_{i,1})$  will satisfy the right-hand equation of Eq. (5). Finally, observe that by assigning suitable values to the variables  $y_{j,s,b}$  for  $j \in [1, m]$ ,  $s \in [1, \ell]$ , and  $b \in \{0, 1\}$ , we can enforce any value from  $\{1\} \times \mathbb{Z}^\ell$  for  $\nu(M_j)$ . Therefore, we can extend  $\nu$  so that it satisfies Eq. (6) as well.  $\square$

This completes the proof of Proposition 6.2, which allows us to prove Theorem 5.3.

*Proof of Theorem 5.3.* By Proposition 6.2, there are  $\ell, m \in \mathbb{N}$  such that the knapsack problem is undecidable for  $G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$ . According to Lemma 4.1, the group  $G^m \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$  is a subgroup of  $G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^{\ell+1})$ , meaning that the latter also has an undecidable knapsack problem.  $\square$

## 7. DECIDABILITY: PROOF OF THEOREM 5.4 AND THEOREM 5.5

Let us fix a wreath product  $G \wr H$ . Recall the projection homomorphisms  $\sigma = \sigma_{G \wr H} : G \wr H \rightarrow H$  and  $\tau = \tau_{G \wr H} : G \wr H \rightarrow G^{(H)}$  from (1). For  $g \in G \wr H$  we write  $\text{supp}(g)$  for  $\text{supp}(\tau(g))$ .

A knapsack expression  $E = h_0 g_1^{x_1} h_1 \cdots g_k^{x_k} h_k$  over  $G \wr H$  is called *torsion-free* if for each  $i \in [1, k]$ , either  $\sigma(g_i) = 1$  or  $\sigma(g_i)$  has infinite order. A map  $\varphi : \mathbb{N}^a \rightarrow \mathbb{N}^b$  is called *affine* if there is a matrix  $A \in \mathbb{N}^{b \times a}$  and a vector  $\mu \in \mathbb{N}^b$  such that  $\varphi(\nu) = A\nu + \mu$  for every  $\nu \in \mathbb{N}^a$ .

**Proposition 7.1.** *Let knapsack be decidable for  $H$ . For every knapsack expression  $E$  over  $G \wr H$ , one can construct torsion-free expressions  $E_1, \dots, E_r$  and affine maps  $\varphi_1, \dots, \varphi_r$  such that  $\text{Sol}(E) = \bigcup_{i=1}^r \varphi_i(\text{Sol}(E_i))$ .*

*Proof.* First of all, note that since knapsack is decidable for  $H$ , we can decide for which  $i$  the element  $\sigma(g_i) \in H$  has finite or infinite order. For a knapsack expression  $F = h_0 g_1^{x_1} h_1 \cdots g_k^{x_k} h_k$ , let  $t(F)$  be the set of indices of  $i \in [1, k]$  such that  $\sigma(g_i) \neq 1$  and  $\sigma(g_i)$  has finite order. We show that if  $|t(E)| > 0$ , then one can construct expressions  $E_0, \dots, E_{r-1}$  and affine maps  $\varphi_0, \dots, \varphi_{r-1}$  such that  $|t(E_j)| < |t(E)|$  and  $\text{Sol}(E) = \bigcup_{j=0}^{r-1} \varphi_j(\text{Sol}(E_j))$ . This suffices, since the composition of affine maps is again an affine map.

Suppose  $E = h_0 g_1^{x_1} h_1 \cdots g_k^{x_k} h_k$  and  $\sigma(g_i) \neq 1$  has finite order  $r$ . Note that we can compute  $r$ . For every  $j \in [0, r-1]$ , let

$$E_j = h_0 g_1^{x_1} h_1 \cdots g_{i-1}^{x_{i-1}} h_{i-1} (g_i^r)^{x_i} (g_i^j h_i) g_{i+1}^{x_{i+1}} h_{i+1} \cdots g_k^{x_k} h_k.$$

Let  $X = \{x_1, \dots, x_r\}$ . Moreover, let  $\varphi : \mathbb{N}^X \rightarrow \mathbb{N}^X$  be the affine map such that for  $\nu \in \mathbb{N}^X$ , we have  $\varphi_j(\nu)(x_\ell) = \nu(x_\ell)$  for  $\ell \neq i$  and  $\varphi_j(\nu)(x_i) = r \cdot \nu(x_i) + j$ . Note that then

$\sigma(g_i^r) = \sigma(g_i)^r = 1$  and thus  $t(E_j) = t(E) \setminus \{i\}$ . Furthermore, we clearly have  $\text{Sol}(E) = \bigcup_{j=0}^{r-1} \varphi_j(\text{Sol}(E_j))$ .  $\square$

Since the image of a semilinear set under an affine map is again semilinear, Proposition 7.1 tells us that it suffices to prove Theorems 5.4 and 5.5 for torsion-free knapsack expressions. For the rest of this section let us fix a torsion-free knapsack expression  $E$  over  $G \wr H$ . We can assume that  $E = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k} g_{k+1}$  (note that if  $g$  has infinite order then also  $c^{-1}gc$  has infinite order). We partition the set  $V_E = \{x_1, \dots, x_k\}$  of variables in  $E$  as  $V_E = S \uplus M$ , where  $S = \{x_i \in V_E \mid \sigma(g_i) = 1\}$  and  $M = \{x_i \in V_E \mid \text{ord}(\sigma(g_i)) = \infty\}$ . In this situation, the following notation will be useful. If  $U = A \uplus B$  for a set of variables  $U \subseteq V$  and  $\mu \in \mathbb{N}^A$  and  $\kappa \in \mathbb{N}^B$ , then we write  $\mu \oplus \kappa \in \mathbb{N}^U$  for the valuation with  $(\mu \oplus \kappa)(x) = \mu(x)$  for  $x \in A$  and  $(\mu \oplus \kappa)(x) = \kappa(x)$  for  $x \in B$ .

**Computing powers.** A key observation in our proof is that in order to compute the group element  $\tau(g^m)(h)$  (in the cursor intuition, this is the element labelling the point  $h \in H$  in the wreath product element  $g^m$ ) for  $h \in H$  and  $g \in G \wr H$ , where  $\sigma(g)$  has infinite order, one only has to perform at most  $|\text{supp}(g)|$  many multiplications in  $G$ , yielding a bound independent of  $m$ . Let us make this precise. Suppose  $h \in H$  has infinite order. For  $h', h'' \in H$ , we write  $h' \preceq_h h''$  if there is an  $n \geq 0$  with  $h' = h^n h''$ . Then,  $\preceq_h$  is transitive. Moreover, since  $h$  has infinite order,  $\preceq_h$  is also anti-symmetric and thus a partial order. Observe that if knapsack is decidable for  $H$ , given  $h, h', h'' \in H$ , we can decide whether  $h$  has infinite order and whether  $h' \preceq_h h''$ . It turns out that for  $g \in G \wr H$ , the order  $\preceq_{\sigma(g)}$  tells us how to evaluate the mapping  $\tau(g^m)$  at a certain element of  $H$ . Before we make this precise, we need some notation.

We will sometimes want to multiply all elements  $a_i$  for  $i \in I$  such that the order in which we multiply is specified by some linear order on  $I$ . If  $(I, \leq)$  is a finite linearly ordered set with  $I = \{i_1, \dots, i_n\}$ ,  $i_1 < i_2 < \dots < i_n$ , then we write  $\prod_{i \in I}^{\leq} a_i$  for  $\prod_{j=1}^n a_{i_j}$ . If the order  $\leq$  is clear from the context, we just write  $\prod_{i \in I} a_i$ .

**Lemma 7.2.** *Let  $g \in G \wr H$  such that  $\text{ord}(\sigma(g)) = \infty$  and let  $h \in H$ ,  $m \in \mathbb{N}$ . Moreover let  $F = \text{supp}(g) \cap \{\sigma(g)^{-i}h \mid i \in [0, m-1]\}$ . Then  $F$  is linearly ordered by  $\preceq_{\sigma(g)}$  and*

$$\tau(g^m)(h) = \prod_{h' \in F}^{\preceq_{\sigma(g)}} \tau(g)(h').$$

*Proof.* By definition of  $G \wr H$ , we have  $\tau(g_1 g_2)(h) = \tau(g_1)(h) \cdot \tau(g_2)(\sigma(g_1)^{-1}h)$ . By induction, this implies

$$\tau(g^m)(h) = \prod_{i=0}^{m-1} \tau(g)(\sigma(g)^{-i}h) = \prod_{j=1}^n \tau(g)(\sigma(g)^{-i_j}h),$$

where  $\{i_1, \dots, i_n\} = \{i \in [0, m-1] \mid \sigma(g)^{-i}h \in \text{supp}(g)\}$  with  $i_1 < \dots < i_n$ . Note that then  $F = \{\sigma(g)^{-i_j}h \mid j \in [1, n]\}$ . Since  $\sigma(g)^{-i_j}h = \sigma(g)^{i_{j+1}-i_j} \sigma(g)^{-i_{j+1}}h$ , we have  $\sigma(g)^{-i_1}h \preceq_{\sigma(g)} \dots \preceq_{\sigma(g)} \sigma(g)^{-i_n}h$ .  $\square$

**Lemma 7.3.** *Let  $g \in G \wr H$  with  $\sigma(g) = 1$  and  $h \in H$ . Then  $\tau(g^m)(h) = (\tau(g)(h))^m$ .*

*Proof.* Recall that for  $g_1, g_2 \in G \wr H$ , we have  $\tau(g_1 g_2)(f) = \tau(g_1)(h) \cdot \tau(g_2)(\sigma(g_1)^{-1}h)$ . Therefore, if  $\sigma(g) = 1$ , then  $\tau(g^m)(h) = \prod_{i=0}^{m-1} \tau(g)(\sigma(g)^{-i}h) = (\tau(g)(h))^m$ .  $\square$

**Addresses.** A central concept in our proof is that of an address. Intuitively, a solution to the equation  $E = 1$  can be thought of as a sequence of instructions on how to walk through the Cayley graph of  $H$  and place elements of  $G$  at those nodes. Here, being a solution means that in the end, all the nodes contain the identity of  $G$ . In order to express that every node carries 1 in the end, we want to talk about at which points in the product  $E = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k} g_{k+1}$  a particular node is visited. An address is a datum that contains just

enough information about such a point to determine which element of  $G$  has been placed during that visit.

A pair  $(i, h)$  with  $i \in [1, k+1]$ , and  $h \in H$  is called an *address* if  $h \in \text{supp}(g_i)$ . The set of addresses of the expression  $E$  is denoted by  $A$ . Note that  $A$  is finite and computable. To each address  $(i, h)$ , we associate the group element  $\gamma(i, h) = g_i$  of the expression  $E$ .

**A linear order on addresses.** We will see that if a node is visited more than once, then (i) each time<sup>2</sup> it does so at a different address and (ii) the order of these visits only depends on the addresses. To capture the order of these visits, we define a linear order on addresses.

We partition  $A = \bigcup_{i \in [1, k+1]} A_i$ , where  $A_i = \{(i, h) \mid h \in \text{supp}(g_i)\}$  for  $i \in [1, k+1]$ . Then, for  $a \in A_i$  and  $a' \in A_j$ , we let  $a < a'$  if and only if  $i < j$ . It remains to order addresses within each  $A_i$ . Within  $A_{k+1}$ , we pick an arbitrary order. If  $i \in [1, k]$  and  $\sigma(g_i) = 1$ , we also order  $A_i$  arbitrarily. Finally, if  $i \in [1, k]$  and  $\sigma(g_i)$  has infinite order, then we pick a linear order  $\leq$  on  $A_i$  so that for  $h, h' \in \text{supp}(g_i)$ ,  $h \preccurlyeq_{\sigma(g_i)} h'$  implies  $(i, h) \leq (i, h')$ . Note that this is possible since  $\preccurlyeq_{\sigma(g_i)}$  is a partial order on  $H$ .

**Cancelling profiles.** In order to express that a solution for  $E$  yields the identity at every node of the Cayley graph of  $H$ , we need to compute the element of  $G$  that is placed after the various visits at a particular node. We therefore, associate to each address an expression over  $G$  that yields the element placed during a visit at this address  $a \in A$ . In analogy to  $\tau(g)$  for  $g \in G \wr H$ , we denote this expression by  $\tau(a)$ . If  $a = (k+1, h)$ , then we set  $\tau(a) = \tau(g_{k+1})(h)$ . Now, let  $a = (i, h)$  for  $i \in [1, k]$ . If  $\sigma(g_i) = 1$ , then  $\tau(a) = \tau(g_i)(h)^{x_i}$ . Finally, if  $\sigma(g_i)$  has infinite order, then  $\tau(a) = \tau(g_i)(h)$ .

This allows us to express the element of  $G$  that is placed at a node  $h \in H$  if  $h$  has been visited with a particular set of addresses. To each subset  $C \subseteq A$ , we assign the expression  $E_C = \prod_{a \in C} \tau(a)$ , where the order of multiplication is given by the linear order on  $A$ . Observe that only variables in  $S \subseteq \{x_1, \dots, x_k\}$  occur in  $E_C$ . Therefore, given  $\kappa \in \mathbb{N}^S$ , we can evaluate  $\kappa(E_C) \in G$ . We say that  $C \subseteq A$  is  $\kappa$ -*cancelling* if  $\kappa(E_C) = 1$ .

In order to record which sets of addresses can cancel simultaneously (meaning: for the same valuation), we use profiles. A *profile* is a subset of  $\mathcal{P}(A)$  (the power set of  $A$ ). A profile  $P \subseteq \mathcal{P}(A)$  is said to be  $\kappa$ -*cancelling* if every  $C \in P$  is  $\kappa$ -cancelling. A profile is *cancelling* if it is  $\kappa$ -cancelling for some  $\kappa \in \mathbb{N}^S$ .

**Clusters.** We also need to express that there is a node  $h \in H$  that is visited with a particular set of addresses. To this end, we associate to each address  $a \in A$  another expression  $\sigma(a)$ . As opposed to  $\tau(a)$ , the expression  $\sigma(a)$  is over  $H$  and variables  $M' = M \cup \{y_i \mid x_i \in M\}$ . Let  $a = (i, h) \in A$ . When we define  $\sigma(a)$ , we will also include factors  $\sigma(g_j)^{x_j}$  and  $\sigma(g_j)^{y_j}$  where  $\sigma(g_j) = 1$ . However, since these factors do not affect the evaluation of the expression, this should be interpreted as leaving out such factors.

- (1) If  $i = k+1$  then  $\sigma(a) = \sigma(g_1)^{x_1} \dots \sigma(g_k)^{x_k} h$ .
- (2) If  $i \in [1, k]$  then  $\sigma(a) = \sigma(g_1)^{x_1} \dots \sigma(g_{i-1})^{x_{i-1}} \sigma(g_i)^{y_i} h$ .

We now want to express that when multiplying  $g_1^{\nu(x_1)} \dots g_k^{\nu(x_k)} g_{k+1}$ , there is a node  $h \in H$  such that the set of addresses with which one visits  $h$  is precisely  $C \subseteq A$ . In this case, we will call  $C$  a cluster.

Let  $\mu \in \mathbb{N}^M$  and  $\mu' \in \mathbb{N}^{M'}$ . We write  $\mu' \sqsubset \mu$  if  $\mu'(x_i) = \mu(x_i)$  for  $x_i \in M$  and  $\mu'(y_i) \in [0, \mu(x_i) - 1]$  for every  $y_i \in M'$ . We can now define the set of addresses at which one visits  $h \in H$ : For  $h \in H$ , let

$$A_{\mu, h} = \{a \in A \mid \mu'(\sigma(a)) = h \text{ for some } \mu' \in \mathbb{N}^{M'} \text{ with } \mu' \sqsubset \mu\}.$$

A subset  $C \subseteq A$  is called a  $\mu$ -*cluster* if  $C \neq \emptyset$  and there is an  $h \in H$  such that  $C = A_{\mu, h}$ .

<sup>2</sup>Here, we count two visits inside the same factor  $g_i$ ,  $i \in [1, k]$ , with  $\sigma(g_i) = 1$  as one visit.

**Lemma 7.4.** *Let  $\nu \in \mathbb{N}^{V_E}$  with  $\nu = \mu \oplus \kappa$  for  $\mu \in \mathbb{N}^M$  and  $\kappa \in \mathbb{N}^S$ . Moreover, let  $h \in H$  and  $C = A_{\mu,h}$ . Then  $\tau(\nu(E))(h) = \kappa(E_C)$ .*

*Proof.* Recall that for  $k_1, k_2 \in G \setminus H$  and  $h \in H$ , we have  $\tau(k_1 k_2)(h) = \tau(k_1)(h) \cdot \tau(\sigma(k_1)^{-1}h)$ . Therefore, we can calculate  $\tau(\nu(E))(h)$  as

$$\tau(\nu(E))(h) = \prod_{i=1}^k \tau\left(g_i^{\nu(x_i)}\right) (\sigma(p_{i-1})^{-1}h) \cdot \tau(g_{k+1}) (\sigma(p_k)^{-1}h),$$

where  $p_i = g_1^{\nu(x_1)} \cdots g_i^{\nu(x_i)}$  for  $i \in [0, k]$ . On the other hand, by definition of the linear order on  $A$ , we have

$$\kappa(E_C) = \prod_{a \in C} \kappa(\tau(a)) = \left( \prod_{a \in C \cap A_1} \kappa(\tau(a)) \right) \cdots \left( \prod_{a \in C \cap A_k} \kappa(\tau(a)) \right) \left( \prod_{a \in C \cap A_{k+1}} \kappa(\tau(a)) \right).$$

Therefore, it suffices to show that

$$(11) \quad \tau\left(g_i^{\nu(x_i)}\right) (\sigma(p_{i-1})^{-1}h) = \prod_{a \in C \cap A_i} \kappa(\tau(a))$$

$$(12) \quad \tau(g_{k+1}) (\sigma(p_k)^{-1}h) = \prod_{a \in C \cap A_{k+1}} \kappa(\tau(a)),$$

for  $i \in [1, k]$ .

We begin with Eq. (12). Note that by definition of  $C = A_{\mu,h}$ , if  $a \in C \cap A_{k+1} = A_{\mu,h} \cap A_{k+1}$  with  $a = (k+1, t)$ , then there is a  $\mu' \in \mathbb{N}^{M'}$  with  $\mu' \sqsubset \mu$  such that  $\mu'(\sigma(a)) = h$ . Moreover, since  $a \in A_{k+1}$ ,  $\sigma(a)$  contains only variables in  $M$  and thus  $\mu'(\sigma(a)) = \mu(\sigma(a)) = \nu(\sigma(a))$ . Note that then

$$h = \mu'(\sigma(a)) = \nu(\sigma(a)) = \nu(\sigma(g_1)^{x_1} \cdots \sigma(g_k)^{x_k} t) = \sigma(p_k) t,$$

meaning that there is only one such  $t$ , namely  $t = \sigma(p_k)^{-1}h$ . Moreover, recall that if  $a = (k+1, t)$ , then  $\tau(a) = \tau(g_{k+1})(t) \in G$ . Therefore, the right-hand side of Eq. (12) is

$$\kappa(\tau(a)) = \tau(g_{k+1})(t) = \tau(g_{k+1}) (\sigma(p_k)^{-1}h),$$

which is the left-hand side of Eq. (12).

It remains to verify Eq. (11). Let us analyze the addresses in  $C \cap A_i$  for  $i \in [1, k]$ . Consider  $a \in C \cap A_i = A_{\mu,h} \cap A_i$  with  $a = (i, t)$ . Since  $a \in A_{\mu,h}$ , there is a  $\mu' \sqsubset \mu$  with  $\mu'(\sigma(a)) = h$ . Since  $i \in [1, k]$  we have

$$(13) \quad h = \mu'(\sigma(a)) = \mu'(\sigma(g_1)^{x_1} \cdots \sigma(g_{i-1})^{x_{i-1}} \sigma(g_i)^{y_i} t) \\ = \sigma(g_1)^{\nu(x_1)} \cdots \sigma(g_{i-1})^{\nu(x_{i-1})} \sigma(g_i)^{\mu'(y_i)} t = \sigma(p_{i-1}) \sigma(g_i)^{\mu'(y_i)} t.$$

Here again, if  $\sigma(g_j) = 1$ , we mean that the factor  $\sigma(g_j)^{\nu(x_j)}$  (resp.,  $\sigma(g_i)^{\mu'(y_i)}$ ) does not appear. We now distinguish two cases.

*Case 1.*  $\sigma(g_i) = 1$ . In this case, Eq. (13) tells us that  $h = \sigma(p_{i-1})t$ , i.e.,  $t = \sigma(p_{i-1})^{-1}h$ . Thus,  $C \cap A_i = \{(i, \sigma(p_{i-1})^{-1}h)\}$ . Moreover, since  $\sigma(g_i) = 1$ ,  $\tau(a)$  is defined as  $(\tau(g_i)(t))^{x_i}$ . Therefore, the right-hand side of Eq. (11) reads

$$(\tau(g_i)(t))^{\kappa(x_i)} = (\tau(g_i)(t))^{\nu(x_i)} = (\tau(g_i^{\nu(x_i)}))(t) = \tau\left(g_i^{\nu(x_i)}\right) (\sigma(p_{i-1})^{-1}h),$$

where the second equality is due to Lemma 7.3. This is precisely the left-hand side of Eq. (11).

*Case 2.*  $\sigma(g_i)$  has infinite order. Let

$$F = \text{supp}(g_i) \cap \{\sigma(g_i)^{-j} \sigma(p_{i-1})^{-1}h \mid j \in [0, \nu(x_i) - 1]\}.$$

We claim that  $t \in F$  if and only if  $(i, t) \in C$ . If  $(i, t) \in C$  then Equation (13) directly implies that  $t \in F$ . Conversely, assume that  $t \in F$  and let  $t = \sigma(g_i)^{-j} \sigma(p_{i-1})^{-1} h$  for  $j \in [0, \nu(x_i) - 1]$ . Then, according to Eq. (13), setting  $\mu'(y_i) := j$  guarantees  $\mu'(\sigma(a)) = h$  for  $a = (i, t)$ , i.e.,  $(i, t) \in C$ .

Observe that  $F$  is linearly ordered by  $\preccurlyeq_{\sigma(g_i)}$ : If  $j < j'$ , then

$$\sigma(g_i)^{-j} \sigma(p_{i-1})^{-1} h = \sigma(g_i)^{j'-j} \sigma(g_i)^{-j'} \sigma(p_{i-1})^{-1} h.$$

Therefore, we can compute the right-hand side of Eq. (11) as

$$\prod_{a \in C \cap A_i} \kappa(\tau(a)) = \prod_{a \in C \cap A_i} \tau(a) = \prod_{t \in F} \tau(g_i)(t).$$

According to Lemma 7.2, this equals the left-hand side of Eq. (11).  $\square$

**Proposition 7.5.** *Let  $\nu \in \mathbb{N}^{V_E}$  with  $\nu = \mu \oplus \kappa$  for  $\mu \in \mathbb{N}^M$  and  $\kappa \in \mathbb{N}^S$ . Then  $\nu(E) = 1$  if and only if  $\sigma(\nu(E)) = 1$  and there is a  $\kappa$ -cancelling profile  $P$  such that every  $\mu$ -cluster is contained in  $P$ .*

*Proof.* Note that  $\nu(E) = 1$  if and only if  $\tau(\nu(E)) = 1$  and  $\sigma(\nu(E)) = 1$ . Therefore, we show that  $\tau(\nu(E)) = 1$  if and only if there is a  $\kappa$ -cancelling profile  $P$  such that every  $\mu$ -cluster is contained in  $P$ .

First, let suppose that there is a  $\kappa$ -cancelling profile  $P$  such that every  $\mu$ -cluster is contained in  $P$ . We need to show that then  $\tau(\nu(E)) = 1$ , meaning  $\tau(\nu(E))(h) = 1$  for every  $h \in H$ . Consider the set  $C = A_{\mu, h}$ . If  $C = \emptyset$ , then by definition, we have  $E_C = 1$ . Thus,  $\kappa(E_C) = 1$ , which by Lemma 7.4 implies  $\tau(\nu(E))(h) = 1$ . If  $C \neq \emptyset$ , then  $C$  is a  $\mu$ -cluster and hence  $\kappa$ -cancelling. Therefore, by Lemma 7.4,  $\tau(\nu(E))(h) = \kappa(E_C) = 1$ . This shows that  $\tau(\nu(E)) = 1$ .

Now suppose  $\tau(\nu(E)) = 1$  and let  $P \subseteq \mathcal{P}(A)$  be the profile consisting of all sets  $A_{\mu, h}$  with  $h \in H$ . Then  $P$  is  $\kappa$ -cancelling, because if  $C \in P$  with  $C = A_{\mu, h}$ , then by Lemma 7.4, we have  $\kappa(E_C) = \tau(\nu(E))(h) = 1$ .  $\square$

**Lemma 7.6.** *Suppose  $\text{KP}(G^*)$  is decidable. Given an instance of knapsack for  $G \wr H$ , we can compute the set of cancelling profiles. If  $G$  is knapsack-semilinear, then for each profile  $P$ , the set of  $\kappa$  such that  $P$  is  $\kappa$ -cancelling is semilinear.*

*Proof.* A profile  $P \subseteq \mathcal{P}(A)$  is  $\kappa$ -cancelling if and only if  $\kappa(E_C) = 1$  for every  $C \in P$ . Together, the expressions  $E_C$  for  $C \in P$  constitute an instance of  $\text{EXPEQ}(G)$  (and according to Proposition 3.1,  $\text{EXPEQ}(G)$  is decidable if  $\text{KP}(G^*)$  is decidable) and this instance is solvable if and only if  $P$  is cancelling. This proves the first statement of the lemma. The second statement holds because the set of  $\kappa \in \mathbb{N}^S$  such that  $P$  is  $\kappa$ -cancelling is precisely  $\bigcap_{C \in P} \text{Sol}(E_C)$  and because the class of semilinear sets is closed under Boolean operations.  $\square$

Let  $L_P \subseteq \mathbb{N}^M$  be the set of all  $\mu \in \mathbb{N}^M$  such that every  $\mu$ -cluster belongs to  $P$ .

**Lemma 7.7.** *Let  $H$  be knapsack-semilinear. For every profile  $P \subseteq \mathcal{P}(A)$ , the set  $L_P$  is effectively semilinear.*

*Proof.* We claim that the fact that every  $\mu$ -cluster belongs to  $P$  can be expressed in Presburger arithmetic. This implies the lemma.

In addition to the variables in  $M'$ , we will use the variables in  $\overline{M'} = \{\overline{x} \mid x \in M'\}$ . For a knapsack expression  $F = r_0 s_1^{z_1} r_1 \cdots s_m^{z_m} r_m$  with variables in  $M'$ , let  $F^{-1} = r_m^{-1} (s_m^{-1})^{z_m} \cdots r_1^{-1} (s_1^{-1})^{z_1} r_0^{-1}$ . Moreover, let  $\overline{F} = r_0 \overline{s}_1^{z_1} r_1 \cdots \overline{s}_m^{z_m} r_m$ . For  $\mu \in \mathbb{N}^{M'}$ , the valuation  $\overline{\mu} \in \mathbb{N}^{\overline{M'}}$  is defined as  $\overline{\mu}(\overline{x}) = \mu(x)$  for all  $x \in M'$ . Furthermore, for  $\mu \in \mathbb{N}^{\overline{M'}}$ , we define the valuation  $\overline{\mu} \in \mathbb{N}^{M'}$  by  $\overline{\mu}(x) = \mu(\overline{x})$  for  $x \in M'$ . Thus if  $\mu \in \mathbb{N}^{M'}$  or  $\mu \in \mathbb{N}^{\overline{M'}}$ , then  $\overline{\overline{\mu}} = \mu$ .

As a first step, for each pair  $a, b \in A$ , we construct a Presburger formula  $\eta_{a,b}$  with free variables  $M' \cup \overline{M'}$  such that for  $\mu_a \in \mathbb{N}^{M'}$  and  $\mu_b \in \mathbb{N}^{\overline{M'}}$ , we have  $\mu_a \oplus \mu_b \models \eta_{a,b}$  if and

only if  $\mu_a(\sigma(a)) = \overline{\mu}_b(\sigma(b))$ . This is possible because  $\mu_a(\sigma(a)) = \overline{\mu}_b(\sigma(b))$  is equivalent to  $(\mu_a \oplus \mu_b)(\sigma(a)\sigma(b)^{-1}) = 1$  and the solution set of the knapsack expression  $\sigma(a)\sigma(b)^{-1}$  is effectively semilinear by assumption.

Next, for each non-empty subset  $C \subseteq A$ , we construct a formula  $\gamma_C$  with free variables in  $M'$  such that  $\mu \models \gamma_C$  if and only if  $C$  is a  $\mu$ -cluster. Since  $C \neq \emptyset$ , we can pick a fixed  $a \in C$  and let  $\gamma_C$  express the following:

$$(14) \quad \begin{aligned} \exists \mu' \in \mathbb{N}^{M'} : \mu' \sqsubset \mu \wedge \bigwedge_{b \in C} \left( \exists \mu'' \in \mathbb{N}^{M'} : \overline{\mu''} \sqsubset \mu \wedge \mu'(\sigma(a)) = \overline{\mu''}(\sigma(b)) \right) \\ \wedge \bigwedge_{b \in A \setminus C} \left( \forall \mu'' \in \mathbb{N}^{M'} : \overline{\mu''} \sqsubset \mu \rightarrow \neg (\mu'(\sigma(a)) = \overline{\mu''}(\sigma(b))) \right). \end{aligned}$$

Observe that  $\mu' \sqsubset \mu$  and  $\overline{\mu''} \sqsubset \mu$  are easily expressible in Presburger arithmetic.

Let us show that in fact  $\mu \models \gamma_C$  if and only if  $C$  is a  $\mu$ -cluster. Consider some  $C \subseteq A$  and let  $a \in C$  be the element picked to define  $\gamma_C$ . If  $\mu \models \gamma_C$ , then there is a  $\mu' \in \mathbb{N}^{M'}$  with the properties stated in Eq. (14). We claim that with  $h := \mu'(\sigma(a))$ , we have  $C = A_{\mu,h}$ . The second of the three conjuncts in Eq. (14) states that for every  $b \in C$  there is a  $\mu'' \in \mathbb{N}^{M'}$  such that  $\mu'' \sqsubset \mu$  and  $\mu''(\sigma(b)) = \mu'(\sigma(a)) = h$ . Thus,  $b \in A_{\mu,h}$ , proving  $C \subseteq A_{\mu,h}$ . The third conjunct states that the opposite is true for every  $b \in A \setminus C$ , so that  $b \notin A_{\mu,h}$  for all  $b \in A \setminus C$ . In other words, we have  $A_{\mu,h} \subseteq C$  and thus  $A_{\mu,h} = C$ .

Conversely, suppose  $C \neq \emptyset$  and  $C = A_{\mu,h}$ . Let  $a \in C$  be the element chosen to define  $\gamma_C$ . Since  $a \in A_{\mu,h}$ , there is a  $\mu' \sqsubset \mu$  with  $h = \mu'(\sigma(a))$ . Moreover, for every  $b \in C$ , there is a  $\mu'' \sqsubset \mu$  with  $\mu''(\sigma(b)) = h = \mu'(\sigma(a))$ . Hence, the second conjunct is satisfied. Furthermore, for every  $b \in A \setminus A_{\mu,h}$ , there is no  $\mu'' \sqsubset \mu$  with  $\mu''(\sigma(b)) = h$ , meaning that the third conjunct is satisfied as well. Hence,  $C = A_{\mu,h}$  and thus we have  $\mu \models \gamma_C$  if and only if  $C$  is a  $\mu$ -cluster.

Finally, we get a formula with free variables  $M$  that expresses that every  $\mu$ -cluster belongs to  $P$  by writing  $\bigwedge_{C \in \mathcal{P}(A) \setminus P, C \neq \emptyset} \neg \gamma_C$ .  $\square$

We are now ready to prove Theorems 5.4 and 5.5. Let  $H$  be knapsack-semilinear and let  $\text{KP}(G^*)$  be decidable. For each profile  $P \subseteq \mathcal{P}(A)$ , let  $K_P \subseteq \mathbb{N}^S$  be the set of all  $\kappa \in \mathbb{N}^S$  such that  $P$  is  $\kappa$ -cancelling.

Observe that for  $\nu = \mu \oplus \kappa$ , where  $\mu \in \mathbb{N}^M$  and  $\kappa \in \mathbb{N}^S$ , the value of  $\sigma(\nu(E))$  only depends on  $\mu$ . Moreover, the set  $T \subseteq \mathbb{N}^M$  of all  $\mu$  such that  $\sigma(\nu(E)) = 1$  is effectively semilinear because  $H$  is knapsack-semilinear. Proposition 7.5 tells us that  $\text{Sol}(E) = \bigcup_{P \subseteq \mathcal{P}(A)} K_P \oplus (L_P \cap T)$  and Lemma 7.7 states that  $L_P$  is effectively semilinear. This implies Theorem 5.4: We can decide solvability of  $E$  by checking, for each of the finitely many profiles  $P$ , whether  $K_P \neq \emptyset$  (which is decidable by Lemma 7.6) and whether  $L_P \cap T \neq \emptyset$ . Moreover, if  $G$  is knapsack-semilinear, then Lemma 7.6 tells us that  $K_P$  and thus  $\text{Sol}(E)$  is semilinear as well. This proves Theorem 5.5.

## 8. COMPLEXITY: PROOF OF THEOREM 5.7

Throughout the section we fix a finitely generated group  $G$ . The goal of this section is to show that if  $G$  is abelian and non-trivial, then  $\text{KP}(G \wr \mathbb{Z})$  is NP-complete.

**8.1. Periodic words over groups.** In this section we define a countable subgroup of  $G^\omega$  (the direct product of  $\aleph_0$  many copies of  $G$ ) that consists of all periodic sequences over  $G$ . We show that the membership problem for certain subgroups of this group can be solved in polynomial time if  $G$  is abelian. We believe that this is a result of independent interest which might have other applications. Therefore, we prove the best possible complexity bound, which is  $\text{TC}^0$ .<sup>3</sup> This is the class of all problems that can be solved with uniform threshold circuits of polynomial size and constant depth. Here, uniformity means

<sup>3</sup>Alternatively, the reader can always replace  $\text{TC}^0$  by polynomial time in the further arguments.

DLOGTIME-uniformity, see e.g. [10] for more details. Complete problems for  $\text{TC}^0$  are multiplication and division of binary encoded integers (or, more precisely, the question whether a certain bit in the output number is 1) [10].  $\text{TC}^0$ -complete problems in the context of group theory are the word problem for any infinite finitely generated solvable linear group [13], the subgroup membership problem for finitely generated nilpotent groups [25], the conjugacy problem for free solvable groups and wreath products of abelian groups [21], and the knapsack problem for finitely generated abelian groups [19].

With  $G^+$  we denote the set of all tuples  $(g_0, \dots, g_{q-1})$  over  $G$  of arbitrary length  $q \geq 1$ . With  $G^\omega$  we denote the set of all mappings  $f : \mathbb{N} \rightarrow G$ . Elements of  $G^\omega$  can be seen as infinite sequences (or words) over the set  $G$ . We define the binary operation  $\circ$  on  $G^\omega$  by pointwise multiplication:  $(f \circ g)(n) = f(n)g(n)$ . In fact,  $G^\omega$  together with the multiplication  $\circ$  is the direct product of  $\aleph_0$  many copies of  $G$ . The identity element is the mapping  $\text{id}$  with  $\text{id}(n) = 1$  for all  $n \in \mathbb{N}$ . For  $f_1, f_2, \dots, f_n \in G^\omega$  we write  $\bigcirc_{i=1}^n f_i$  for  $f_1 \circ f_2 \circ \dots \circ f_n$ . If  $G$  is abelian, we write  $\sum_{i=1}^n f_i$  for  $\bigcirc_{i=1}^n f_i$ . A function  $f \in G^\omega$  is *periodic with period*  $q \geq 1$  if  $f(k) = f(k+q)$  for all  $k \geq 0$ . Note that in this situation,  $f$  might also be periodic with a smaller period  $q' < q$ . Of course, a periodic function  $f$  with period  $q$  can be specified by the tuple  $(f(0), \dots, f(q-1))$ . Vice versa, a tuple  $u = (g_0, \dots, g_{q-1}) \in G^+$  defines the periodic function  $f_u \in G^\omega$  with

$$f_u(n \cdot q + r) = g_r \text{ for } n \geq 0 \text{ and } 0 \leq r < q.$$

One can view this mapping as the sequence  $u^\omega$  obtained by taking infinitely many repetitions of  $u$ . Let  $G^\rho$  be the set of all periodic functions from  $G^\omega$ . If  $f_1$  is periodic with period  $q_1$  and  $f_2$  is periodic with period  $q_2$ , then  $f_1 \circ f_2$  is periodic with period  $q_1 q_2$  (in fact,  $\text{lcm}(q_1, q_2)$ ). Hence,  $G^\rho$  forms a countable subgroup of  $G^\omega$ . Note that  $G^\rho$  is not finitely generated: The subgroup generated by elements  $f_i \in G^\rho$  with period  $q_i$  ( $1 \leq i \leq n$ ) contains only functions with period  $\text{lcm}(q_1, \dots, q_n)$ . Nevertheless, using the representation of periodic functions by elements of  $G^+$  we can define the word problem for  $G^\rho$ ,  $\text{WP}(G^\rho)$  for short:

**Input:** Tuples  $u_1, \dots, u_n \in G^+$  (elements of  $G$  are represented by finite words over  $\Sigma$ ).

**Question:** Does  $\bigcirc_{i=1}^n f_{u_i} = \text{id}$  hold?

For  $n \geq 0$  we define the subgroup  $G_n^\rho$  of all  $f \in G^\rho$  with  $f(k) = 1$  for all  $0 \leq k \leq n-1$ . We also consider the uniform membership problem for subgroups  $G_n^\rho$ ,  $\text{MEMBERSHIP}(G_n^\rho)$  for short:

**Input:** Tuples  $u_1, \dots, u_n \in G^+$  (elements of  $G$  are represented by finite words over  $\Sigma$ ) and a binary encoded number  $m$ .

**Question:** Does  $\bigcirc_{i=1}^n f_{u_i}$  belong to  $G_m^\rho$ ?

**Lemma 8.1.**  $\text{WP}(G^\rho)$  is  $\text{TC}^0$ -reducible to  $\text{MEMBERSHIP}(G_*^\rho)$

*Proof.* Let  $u_1, \dots, u_n \in G^+$  and let  $q_i$  be the length of  $u_i$ . Let  $m = \text{lcm}(q_1, \dots, q_n)$ . We have  $\bigcirc_{i=1}^n f_{u_i} = \text{id}$  if and only if  $\bigcirc_{i=1}^n f_{u_i}$  belongs to  $G_m^\rho$ .  $\square$

**Theorem 8.2.** For every finitely generated abelian group  $G$ ,  $\text{MEMBERSHIP}(G_*^\rho)$  belongs to  $\text{TC}^0$ .

*Proof.* Since the word problem for a finitely generated abelian group belongs to  $\text{TC}^0$ , it suffices to show the following claim:

*Claim:* Let  $u_1, \dots, u_n \in G^+$  and let  $q_i$  be the length of  $u_i$ . Let  $f = \sum_{i=1}^n f_{u_i}$ . If there exists a position  $m$  such that  $f(m) \neq 0$ , then there exists a position  $m < \sum_{i=1}^n q_i$  such that  $f(m) \neq 0$ .

Let  $m \geq \sum_{i=1}^n q_i$ . We show that if  $f(j) = 0$  for all  $j$  with  $m - \sum_{i=1}^n q_i \leq j < m$ , then also  $f(m) = 0$ , which proves the above claim.

Hence, let us assume that  $f(j) = 0$  for all  $j$  with  $m - \sum_{i=1}^n q_i \leq j < m$ . Note that  $f_{u_i}(j) = f_{u_i}(j - q_i)$  for all  $j \geq q_i$  and  $1 \leq i \leq n$ . For  $M \subseteq [1, n]$  let  $q_M = \sum_{i \in M} q_i$ .

Moreover, for  $1 \leq k \leq n$  let  $\mathcal{M}_k = \{M \subseteq [1, n], |M| = k\}$ . For all  $1 \leq k \leq n-1$  we get

$$\begin{aligned}
\sum_{M \in \mathcal{M}_k} \sum_{i \in M} f_{u_i}(m - q_M) &= - \sum_{M \in \mathcal{M}_k} \sum_{i \in [1, n] \setminus M} f_{u_i}(m - q_M) \\
&= - \sum_{M \in \mathcal{M}_k} \sum_{i \in [1, n] \setminus M} f_{u_i}(m - q_M - q_i) \\
&= - \sum_{i=1}^n \sum_{M \in \mathcal{M}_k, i \notin M} f_{u_i}(m - q_{M \cup \{i\}}) \\
&= - \sum_{i=1}^n \sum_{M \in \mathcal{M}_{k+1}, i \in M} f_{u_i}(m - q_M) \\
&= - \sum_{M \in \mathcal{M}_{k+1}} \sum_{i \in M} f_{u_i}(m - q_M).
\end{aligned}$$

We can write

$$f(m) = \sum_{i=1}^n f_{u_i}(m) = \sum_{i=1}^n f_{u_i}(m - q_i) = \sum_{M \in \mathcal{M}_1} \sum_{i \in M} f_{u_i}(m - q_M).$$

From the above identities we get by induction:

$$\begin{aligned}
f(m) &= (-1)^{n+1} \sum_{M \in \mathcal{M}_n} \sum_{i \in M} f_{u_i}(m - q_M) \\
&= (-1)^{n+1} \sum_{i \in [1, n]} f_{u_i}(m - q_{[1, n]}) \\
&= (-1)^{n+1} f(m - \sum_{i=1}^n q_i) = 0.
\end{aligned}$$

This proves the claim and hence the theorem.  $\square$

**8.2. Automata for Cayley representations.** The goal of this section is to show that if  $\text{EXPEQ}(G)$  and  $\text{MEMBERSHIP}(G_*^p)$  both belong to NP, then also  $\text{KP}(G \wr \mathbb{Z})$  belongs to NP.

An interval  $[a, b] \subseteq \mathbb{Z}$  *supports* an element  $(f, d) \in G \wr \mathbb{Z}$  if  $\{0, d\} \cup \text{supp}(f) \subseteq [a, b]$ . If  $(f, d) \in G \wr \mathbb{Z}$  is a product of length  $n$  over the generators, then the minimal interval  $[a, b]$  which supports  $(f, d)$  satisfies  $b - a \leq n$ . A knapsack expression  $E = v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k$  is called *rigid* if each  $u_i$  evaluates to an element  $(f_i, 0) \in G \wr \mathbb{Z}$ . Intuitively, the movement of the cursor is independent from the values of the variables  $x_i$  up to repetition of loops. In particular, every variable-free expression is rigid.

In the following we define so called Cayley representations of rigid knapsack expressions. This is a finite word, where every symbol is a marked knapsack expression over  $G$ . A marked knapsack expression over  $G$  is of the form  $E, \overline{E}, \underline{E}$ , or  $\underline{\overline{E}}$ , where  $E$  is a knapsack expression over  $G$ . We say that  $\overline{E}$  and  $\underline{\overline{E}}$  (resp.,  $\underline{E}$  and  $\underline{\overline{E}}$ ) are top-marked (resp., bottom-marked).

Let  $E = v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k$  be a rigid knapsack expression over  $G \wr \mathbb{Z}$ . For an assignment  $\nu$  let  $(f_\nu, d) \in G \wr \mathbb{Z}$  be the element to which  $\nu(E)$  evaluates, i.e.  $(f_\nu, d) = \nu(E)$ . Note that  $d$  does not depend on  $\nu$ . Because of the rigidity of  $E$ , there is an interval  $[a, b] \subseteq \mathbb{Z}$  that supports  $(f_\nu, d)$  for all assignments  $\nu$ . For each  $j \in [a, b]$  let  $E_j$  be a knapsack expression over  $G$  with the variables  $x_1, \dots, x_k$  such that  $f_\nu(j) = \nu(E_j)$  for all assignments  $\nu$ . Then we call the formal expression

$$r = \begin{cases} E_a E_{a+1} \cdots E_{-1} \overline{E_0} E_1 \cdots E_{d-1} \underline{E_d} E_{d+1} \cdots E_b & \text{if } d > 0 \\ E_a E_{a+1} \cdots E_{-1} \overline{E_0} E_1 \cdots E_b & \text{if } d = 0 \\ E_a E_{a+1} \cdots E_{d-1} \underline{E_d} E_{d+1} \cdots E_{-1} \overline{E_0} E_1 \cdots E_b & \text{if } d < 0 \end{cases}$$



-1	0	1	2	3	4	5	6	7	8	9	10	11	12
$a^x$	$\frac{a^x}{1}$	$b^x$											
	$b$	$\frac{1}{b^y}$	$b^y$	$b^y$	$\frac{a}{a}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{a}$
		$\frac{1}{a}$	$b^{-1}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{b^{-1}}$	$\frac{a}{a}$	$\frac{a}{a}$
$a^x$	$a^x b$	$b^x b^y a$	$b^y$	$b^y a^2$	$a$	$a^2$	$a$	$a^2$	$a$	$a^2$	$ab^{-1}$	$\frac{a}{a}$	$a$

FIGURE 1. Cayley representation

a *Cayley representation* of  $E$  (or  $E$  is *represented* by  $r$ ). Formally, a Cayley representation is a sequence of marked knapsack expressions. For a Cayley representation  $r$ , we denote by  $|r|$  the number of knapsack expressions in the sequence. If necessary, we separate consecutive marked knapsack expressions in  $r$  by commas. For instance, if  $a_1$  and  $a_2$  are generators of  $G$ , then  $\overline{a_1}, a_2 a_1, \underline{a_2}$  is a Cayley representation of length 3, whereas  $\overline{a_1}, a_2, a_1, \underline{a_2}$  is a Cayley representation of length 4. By this definition,  $r$  depends on the chosen supporting interval  $[a, b]$ . However, compared to the representation of the minimal supporting interval, any other Cayley representation differs only by adding 1's (i.e., trivial knapsack expressions over  $G$ ) at the left and right end of  $r$ .

A Cayley representation of  $E$  records for each point in  $\mathbb{Z}$  an expression that describes which element will be placed at that point. Multiplying an element of  $G \wr \mathbb{Z}$  always begins at a particular cursor position; in a Cayley representation, the marker on top specifies the expression that is placed at the cursor position in the beginning. Moreover, a Cayley representation describes how the cursor changes when multiplying  $\nu(E)$ : The marker on the bottom specifies where the cursor is located in the end.

**Example 8.3.** Let us consider the wreath product  $F_2 \wr \mathbb{Z}$  where  $F_2$  is the free group generated by  $\{a, b\}$  and  $\mathbb{Z}$  is generated by  $t$ . Consider the rigid knapsack expression  $E = u_1^x u_2^y u_3^y u_4^5$  where

- $u_1 = at^{-1}at^2bt^{-1}$ , represented by  $a\overline{a}b$ ,
- $u_2 = t$ , represented by  $\overline{1}1$ ,
- $u_3 = btbttb^{-2}$ , represented by  $\overline{b}bb$ ,
- $u_4 = at^{-1}bt^2b^{-1}tatat^{-1}$ , represented by  $b\overline{a}b^{-1}\underline{a}a$ .

A Cayley representation of  $u_1^x$  is  $a^x \overline{a^x} b^{-1}$  and a Cayley representation of  $u_3^y$  is  $\overline{b^y} b^y b^y$ . The diagram in Fig. 1 illustrates how to compute a Cayley representation  $r$  of  $E$ , which is shown in the bottom line. Here, we have chosen the supporting interval minimal. Note that if we replace the exponents 5 in  $u_4^5$  by a larger number, then we only increase the number of repetitions of the factor  $a, a^2$  in the Cayley representation.

Example 8.3 also illustrates the concept of so called consistent tuples, which will be used later. A tuple  $(\gamma_1, \dots, \gamma_n)$ , where every  $\gamma_i$  is a marked knapsack expression over  $G$  is *consistent* if, whenever  $\gamma_i$  is bottom-marked and  $i < n$ , then  $\gamma_{i+1}$  is top-marked. Every column in Fig. 1 is a consistent tuple.

Let  $E$  be an arbitrary knapsack expression over  $G \wr \mathbb{Z}$ . We can assume that  $E$  has the form  $u_1^{x_1} \dots u_k^{x_k} u_{k+1}$ . We partition the set of variables  $X = \{x_1, \dots, x_k\}$  as  $X = X_0 \cup X_1$ , where  $X_0$  contains all variables  $x_i$  where  $u_i$  evaluates to an element  $(f, 0) \in G \wr \mathbb{Z}$ , and  $X_1$  contains all other variables. For a partial assignment  $\nu: X_1 \rightarrow \mathbb{N}$  we obtain a rigid knapsack expression  $E_\nu$  by replacing in  $E$  every variable  $x_i \in X_1$  by  $\nu(x_i)$ . A set  $R$  of Cayley representations is a *set representation* of  $E$  if

- for each assignment  $\nu: X_1 \rightarrow \mathbb{N}$  there exists  $r \in R$  such that  $r$  represents  $E_\nu$ ,

- for each  $r \in R$  there exists an assignment  $\nu: X_1 \rightarrow \mathbb{N}$  such that  $r$  represents  $E_\nu$  and  $\nu(x) \leq |r|$  for all  $x \in X_1$ .

**Example 8.4.** Let us consider again the wreath product  $F_2 \wr \mathbb{Z}$  and consider the (non-rigid) knapsack expression  $E' = u_1^x u_2^y u_3^z u_4^z$  where  $u_1, u_2, u_3, u_4$  are taken from Example 8.3. We have  $X_0 = \{x, y\}$  and  $X_1 = \{z\}$ . For  $z = 5$  we obtained in Example 8.3 the Cayley representation

$$a^x, \overline{a^x b}, b^x b^y a, b^y, b^y a^2, a, a^2, a, a^2, a, a^2, ab^{-1}, \underline{a}, a.$$

A set representation  $R$  of  $E'$  consists of the following Cayley representations:

- $a^x, \overline{a^x}, \underline{b^x b^y}, b^y, b^y$  for  $\nu(z) = 0$ ,
- $a^x, \overline{a^x b}, b^x b^y a, b^y b^{-1}, \underline{b^y a}, a$  for  $\nu(z) = 1$ ,
- $a^x, \overline{a^x b}, b^x b^y a, b^y, b^y a^2, \underbrace{a, a^2, \dots, a, a^2}_{\nu(z) - 2 \text{ times}}, ab^{-1}, \underline{a}, a$  for  $\nu(z) \geq 2$ .

Only finitely many different marked knapsack expressions appear in this set representation  $R$ , and  $R$  is clearly a regular language over the finite alphabet consisting of this finitely many marked knapsack expressions.

In the following, we will show that for every knapsack expression  $E = u_1^{x_1} \dots u_k^{x_k} u_{k+1}$  there exists a non-deterministic finite automaton (NFA) that accepts a set representation of  $E$ , whose size is exponential in  $n = |E|$ . First, we consider the blocks  $u_1^{x_1}, \dots, u_k^{x_k}, u_{k+1}$ .

**Lemma 8.5.** *One can compute in polynomial time for each  $1 \leq i \leq k+1$  an NFA  $\mathcal{A}_i$  of size  $|u_i|^{O(1)}$  that recognizes a set representation of  $u_i^{x_i}$  or  $u_{k+1}$ .*

*Proof.* Let us do a case distinction.

*Case 1.* Consider an expression  $u_i^{x_i}$  where  $x_i \in X_0$ , i.e.  $u_i$  evaluates to some element  $(f, 0) \in G \wr \mathbb{Z}$ . Let  $[a, b]$  be the minimal interval which supports  $(f, 0)$ . Thus,  $b - a \leq |u_i|$ . Then

$$r_i = f(a)^{x_i} \dots f(-1)^{x_i} \overline{f(0)^{x_i}} f(1)^{x_i} \dots f(b)^{x_i}$$

is a Cayley representation of  $u_i^{x_i}$  where  $|r_i| = b - a + 1 \leq |u_i| + 1$ . Clearly,  $\{r_i\}$  is a set representation of  $u_i^{x_i}$ , which is recognized by an NFA  $\mathcal{A}_i$  of size  $|r_i| + 1 \leq |u_i| + 2$ .

*Case 2.* Similarly, for the word  $u_{k+1}$  we obtain a Cayley representation  $r_{k+1}$  as above except that the exponents  $x_i$  are not present. Again,  $\{r_{k+1}\}$  is a set representation of  $u_{k+1}$ , which is recognized by an NFA  $\mathcal{A}_{k+1}$  of size  $|u_{k+1}| + 2$ .

*Case 3.* Consider an expression  $u_i^{x_i}$  where  $x_i \in X_1$ , i.e.,  $u_i$  evaluates to some element  $(f, d) \in G \wr \mathbb{Z}$  where  $d \neq 0$ . Let  $[a, b]$  be a minimal interval which supports  $(f, d)$ , hence  $b - a \leq |u_i|$ .

We only consider the case  $d > 0$ ; at the end we say how to modify the construction for  $d < 0$ . Consider the word

$$r_i = f(a) \dots f(-1) \overline{f(0)} \dots \underline{f(d)} f(1) \dots f(b),$$

which is a Cayley representation of  $(f, d)$ . We will prove that there is an NFA  $\mathcal{A}_i$  with  $\varepsilon$ -transitions of size  $O(|r_i|^2) = O(|u_i|^2)$  which recognizes a set representation of  $u_i^{x_i}$ . This set representation has to contain a Cayley representation of every  $u_i^m$  (a variable-free knapsack expression over  $G$ ) for  $m \geq 0$ .

First we define an auxiliary automaton  $\mathcal{B}$ . Example 8.6 shows an example of the following construction. Let  $\Gamma$  be the alphabet of  $r_i$  (a set of possibly marked elements of  $G$ ) and define  $g: [a, b] \rightarrow \Gamma$  by

$$g(c) = \begin{cases} \overline{f(0)} & \text{if } c = 0 \\ \underline{f(d)} & \text{if } c = d \\ f(c) & \text{otherwise.} \end{cases}$$

$b$	$\bar{a}$	$b^{-1}$ $b$	$\underline{a}$ $\bar{a}$	$a$ $b^{-1}$ $b$	$\underline{a}$ $\bar{a}$	$a$ $b^{-1}$ $b$	$\underline{a}$ $\bar{a}$	$a$ $b^{-1}$ $b$	$\underline{a}$ $\bar{a}$	$a$ $b^{-1}$ $b$	$\underline{a}$ $\bar{a}$	$a$
$b$	$\bar{a}$	1	$a^2$	$a$	$a^2$	$a$	$a^2$	$a$	$a^2$	$ab^{-1}$	$\underline{a}$	$a$
(-1)	(0)	(1,-1)	(2,0)	(3,1,-1)	(2,0)	(3,1,-1)	(2,0)	(3,1,-1)	(2,0)	(3,1)	(2)	(3)

FIGURE 2. A run of the automaton for  $(at^{-1}bt^2b^{-1}atat^{-1})^x$ 

The state set of  $\mathcal{B}$  is the set  $Q$  of all decreasing arithmetic progressions  $(s, s-d, s-2d, \dots, s-\ell d)$  in the interval  $[a, b]$  where  $\ell \geq 0$  together with a unique final state  $\top$ . It is not hard to see that  $|Q| = O(|r_i|^2)$ . For each state  $(s_0, \dots, s_\ell) \in Q$  we define the marked  $G$ -element

$$\alpha(s_0, \dots, s_\ell) = \begin{cases} f(s_0) \cdots f(s_\ell) & \text{if neither } g(s_0) \text{ is top-marked nor } g(s_\ell) \text{ is bottom-marked} \\ \overline{f(s_0) \cdots f(s_\ell)} & \text{if } g(s_0) \text{ is top-marked} \\ \underline{f(s_0) \cdots f(s_\ell)} & \text{if } g(s_\ell) \text{ is bottom-marked} \end{cases}$$

Since  $d > 0$  it cannot happen that  $g(s_0)$  is top-marked and at the same time  $g(s_\ell)$  is bottom-marked. The initial state is the 1-tuple  $(a)$ . For each state  $(s_0, \dots, s_\ell) \in Q$  and  $\gamma = \alpha(s_0, \dots, s_\ell)$  the automaton has the following transitions:

- $(s_0, \dots, s_\ell) \xrightarrow{\varepsilon} (s_0, \dots, s_\ell, a)$  if  $s_\ell = a + d$
- $(s_0, \dots, s_\ell) \xrightarrow{\gamma} (s_0 + 1, \dots, s_\ell + 1)$  if  $s_0 < b$
- $(s_0, \dots, s_\ell) \xrightarrow{\gamma} (s_1 + 1, \dots, s_\ell + 1)$  if  $s_0 = b$  and  $\ell \geq 1$
- $(s_0, \dots, s_\ell) \xrightarrow{\gamma} \top$  if  $s_0 = b$  and  $\ell = 0$

Finally we take the union with another automaton which accepts the singleton  $\{\bar{1}\}$ . This yields the desired automaton  $\mathcal{A}_i$ .

If  $d < 0$  we can consider the group element  $(f', -d)$  with  $f': [-b, -a] \rightarrow G$ ,  $f'(c) = f(-c)$  for  $-b \leq c \leq -a$ . We then do the above automaton construction for  $(f', -d)$ . From the resulting NFA we finally construct an automaton for the reversed language. This proves the lemma.  $\square$

**Example 8.6.** Below is a run of the automaton for  $(at^{-1}bt^2b^{-1}atat^{-1})^x$  on the word

$$b, \bar{a}, 1, (a^2, a)^3, a^2, ab^{-1}, \underline{a}, a.$$

Fig. 2 shows how this word is produced from  $(at^{-1}bt^2b^{-1}atat^{-1})^5$ . The last line shows the tuple of relative positions in the currently “active” copies of  $b, a, b^{-1}, a, a$ . The positions are  $-1, 0, 1, 2, 3$ . For instance, the tuple  $(3, 1, -1)$  means that currently three copies of  $b, a, b^{-1}, a, a$  are active. The current position in the first copy is 3, the current position in the second copy is 1, and the current position in the third copy is -1. These tuples are states in the run below. The only additional states (1) and (3, 1) in the run are origins of  $\varepsilon$ -transitions, which add new copies of  $b, a, b^{-1}, a, a$ .

$$\begin{aligned} (-1) &\xrightarrow{b} (0) \xrightarrow{\bar{a}} (1) \xrightarrow{\varepsilon} (1, -1) \xrightarrow{1} \\ (2, 0) &\xrightarrow{a^2} (3, 1) \xrightarrow{\varepsilon} (3, 1, -1) \xrightarrow{a} \\ (2, 0) &\xrightarrow{a^2} (3, 1) \xrightarrow{\varepsilon} (3, 1, -1) \xrightarrow{a} \\ (2, 0) &\xrightarrow{a^2} (3, 1) \xrightarrow{\varepsilon} (3, 1, -1) \xrightarrow{a} \\ (2, 0) &\xrightarrow{a^2} (3, 1) \xrightarrow{ab^{-1}} (2) \xrightarrow{a} (3) \xrightarrow{a} \top \end{aligned}$$

A language  $L \subseteq \Sigma^*$  is *bounded* if there exist words  $\beta_1, \dots, \beta_n \in \Sigma^*$  such that  $L \subseteq \beta_1^* \cdots \beta_n^*$ . It will be convenient to use the following characterization. For states  $p, q$  of an automaton  $\mathcal{B}$ , let  $L_{p,q}(\mathcal{B})$  be the set of all words read on a path from  $p$  to  $q$ . An NFA  $\mathcal{B}$  recognizes a bounded language if and only if for every state  $q$ , the language  $L_{q,q}(\mathcal{B})$  is commutative, meaning that  $uv = vu$  for any  $u, v \in L_{q,q}(\mathcal{B})$  [5].

**Lemma 8.7.** *Given an NFA  $\mathcal{B}$  that recognizes a bounded language, one can compute in polynomial time words  $\beta_1, \dots, \beta_n$  with  $L(\mathcal{B}) \subseteq \beta_1^* \cdots \beta_n^*$ .*

*Proof.* For any two states  $p, q$  with  $L_{p,q}(\mathcal{B}) \neq \emptyset$ , compute a shortest word  $w_{p,q} \in L_{p,q}(\mathcal{B})$  and let  $P_q = u_1^* \cdots u_m^*$ , where  $w_{q,q} = u_1 \cdots u_m$  and  $u_1, \dots, u_m$  are letters.

We first prove the lemma for the languages  $L_{p,q} = L_{p,q}(\mathcal{B})$  if  $p, q$  lie in the same strongly connected component. Any two words in  $L_{p,q}$  have to be comparable in the prefix order: Otherwise we could construct two distinct words of equal length in  $L_{p,p}$ , contradicting the commutativity of  $L_{p,p}$ . Since  $w_{p,q}w_{q,q}^* \subseteq L_{p,q}$ , this means that every word in  $L_{p,q}$  must be a prefix of a word in  $w_{p,q}w_{q,q}^*$ . In particular, we have  $L_{p,q} \subseteq w_{p,q}^*w_{q,q}P_q$ .

In the general case, we assume that  $\mathcal{B}$  has only one initial state  $s$ . We decompose  $\mathcal{B}$  into strongly connected components, yielding a directed acyclic graph  $\Gamma$  with vertices  $V$ . For  $i \leq |V|$ , let  $D_i = \{v \in V \mid v \text{ has distance } i \text{ from } [s] \text{ in } \Gamma\}$ , where  $[s]$  denotes the strongly connected component of  $s$ . Observe that  $L(\mathcal{B}) \subseteq \prod_{i=0}^{|V|} \prod_{v \in D_i} \prod_{p,q \in v} L_{p,q}$ , where the two innermost products are carried out in an arbitrary order. Since we have established the lemma in the case of the  $L_{p,q}$ , this tells us how to perform the computation for  $L(\mathcal{B})$ .  $\square$

**Lemma 8.8.** *The NFAs  $\mathcal{A}_i$  from Lemma 8.5 recognize bounded languages.*

*Proof.* The statement is clear for the automata which recognize singleton languages in cases 1. and 2. Consider the constructed automaton  $\mathcal{B}$  from case 3. It is almost deterministic in the following sense: Every state in  $\mathcal{B}$  has at most one outgoing transition labelled by a symbol from the alphabet and at most one outgoing  $\varepsilon$ -transition.

We partition its state set as  $Q = Q_0 \uplus Q_1$ , where  $Q_0$  consists of those states  $(s_0, \dots, s_\ell)$  where  $s_\ell \leq a + d$ . Since there is no transition from  $Q_1$  to  $Q_0$ , every strongly connected component is either entirely within  $Q_0$  or entirely within  $Q_1$ . If a state  $q$  has an outgoing  $\varepsilon$ -transition, then  $q \in Q_0$  and all non- $\varepsilon$ -transitions from  $q$  lead into  $Q_1$ . Therefore, every state in  $\mathcal{B}$  has at most one outgoing transition that leads into the same strongly connected component. Thus, every strongly connected component is a directed cycle, meaning that  $L_{q,q}(\mathcal{B}) = w^*$ , where  $w$  is the word read on that cycle. Hence,  $\mathcal{B}$  recognizes a bounded language. Hence also  $L(\mathcal{A}_i) = L(\mathcal{B}) \cup \{\bar{1}\}$  is bounded.  $\square$

**Lemma 8.9.** *There exists an NFA  $\mathcal{A}$  of size  $\prod_{i=1}^{k+1} O(|u_i|) \leq 2^{O(n \log n)}$  which recognizes a set representation of  $E$ , where  $n = |E|$ .*

*Proof.* Reconsider the automata  $\mathcal{A}_i$  from Lemma 8.5. We first ensure that for all  $1 \leq i \leq k+1$  we have  $L(\mathcal{A}_i) = 1^* L(\mathcal{A}_i) 1^*$ , which can be achieved using two new states in  $\mathcal{A}_i$ . Let  $\mathcal{E}_i$  be the finite alphabet of marked knapsack expressions that occur as labels in  $\mathcal{A}_i$  and let  $\mathcal{E}$  be the set of consistent tuples in the cartesian product  $\mathcal{E}_1 \times \cdots \times \mathcal{E}_{k+1}$ .

Let  $\mathcal{A}'$  be the following product NFA over the alphabet  $\mathcal{E}$ . It stores a  $(k+1)$ -tuple of states (one for each NFA  $\mathcal{A}_i$ ). On input of a consistent tuple  $(\gamma_1, \dots, \gamma_{k+1}) \in \mathcal{E}$  it reads  $\gamma_i$  into  $\mathcal{A}_i$ . The size of  $\mathcal{A}'$  is  $\prod_{i=1}^{k+1} O(|u_i|) \leq 2^{O(n \log n)}$ . To obtain the NFA  $\mathcal{A}$  we project the transition labels of  $\mathcal{A}'$  as follows: Let  $(\gamma_1, \dots, \gamma_{k+1}) \in \mathcal{E}$  and let  $(\chi_1, \dots, \chi_{k+1})$  obtained by removing all markings from the  $\gamma_i$ . We then replace the transition label  $(\chi_1, \dots, \chi_{k+1})$  by

- $\chi_1 \cdots \chi_{k+1}$  if neither  $\chi_1$  is top-marked nor  $\chi_{k+1}$  is bottom-marked,
- $\overline{\chi_1 \cdots \chi_{k+1}}$  if  $\chi_1$  is top-marked and  $\chi_{k+1}$  is not bottom-marked,
- $\underline{\chi_1 \cdots \chi_{k+1}}$  if  $\chi_1$  is not top-marked and  $\chi_{k+1}$  is bottom-marked,
- $\overline{\underline{\chi_1 \cdots \chi_{k+1}}}$  if  $\chi_1$  is top-marked and  $\chi_{k+1}$  is bottom-marked.

One can verify that  $\mathcal{A}$  recognizes a set representation of  $E$ .  $\square$

**Proposition 8.10.** *Let  $G$  be a finitely generated abelian group. If  $\text{EXPEQ}(G) \in \text{NP}$  and  $\text{MEMBERSHIP}(G_*^\rho) \in \text{NP}$ , then also  $\text{KP}(G \wr \mathbb{Z}) \in \text{NP}$ .*

*Proof.* We first claim that, if  $E = 1$  is solvable, then there exists a solution  $\nu$  such that  $\nu(x)$  is exponentially bounded in  $n$  for all  $x \in X_1$ . Assume that  $\nu$  is a solution for  $E = 1$ . From the NFA  $\mathcal{A}$ , we obtain an automaton  $\mathcal{A}'$  by replacing each knapsack expression in the alphabet of  $\mathcal{A}$  by its value under  $\nu$  in  $G$ . Then,  $\mathcal{A}'$  has the same number of states as  $\mathcal{A}$ , hence at most  $2^{O(n \log n)}$ . Moreover,  $\mathcal{A}'$  accepts a Cayley representation of the identity of  $G \wr \mathbb{Z}$  (which is just a sequence of 1's). Due to the size bound,  $\mathcal{A}'$  accepts such a representation of length  $2^{O(n \log n)}$ . Since  $\mathcal{A}$  accepts a set representation of  $E$ , this short computation corresponds to a solution  $\nu'$ . By definition of a set representation, for each  $x \in X_1$ ,  $\mathcal{A}'$  makes at least  $\nu'(x)$  steps. Therefore,  $\nu'(x)$  is bounded exponentially for  $x \in X_1$ .

Since each  $\mathcal{A}_i$  accepts a set representation of  $u_i^{x_i}$ ,  $i \in [1, k]$  or of  $u_{k+1}$ , this implies that solvability of  $E$  is witnessed by words  $\alpha_1, \dots, \alpha_{k+1}$  with  $\alpha_i \in L(\mathcal{A}_i)$  for  $i \in [1, k+1]$  whose length is bounded exponentially.

In the following we will encode exponentially long words as follows: A *cycle compression* of a word  $w$  is a sequence  $(\beta_1, \ell_1, \dots, \beta_m, \ell_m)$  where each  $\beta_i$  is a word and each  $\ell_i \geq 0$  is a binary encoded integer such that there exists a factorization  $w = w_1 \cdots w_m$  and each factor  $w_i$  is the prefix of  $\beta_i^\omega$  of length  $\ell_i$ . Each  $w_i$  is called a *cycle factor* in  $w$ .

We need the following simple observation. Let  $(\beta_1, \ell_1, \dots, \beta_m, \ell_m)$  be a cycle compression of a word  $w$  with the corresponding factorization  $w = w_1 \cdots w_m$ . Given a position  $p$  in  $w$  which yields factorizations  $w = uv$ ,  $u = w_1 \cdots w_{i-1}w'_i$ ,  $v = w''_i w_{i+1} \cdots w_m$  and  $w_i = w'_i w''_i$ . *Splitting*  $(\beta_1, \ell_1, \dots, \beta_m, \ell_m)$  at position  $p$  yields the unique cycle compression of  $w$  of the form

$$(\beta_1, \ell_1, \dots, \beta_{i-1}, \ell_{i-1}, \beta'_i, \ell'_i, \beta''_i, \ell''_i, \dots, \beta_m, \ell_m)$$

where  $|w'_i| = \ell'_i$  and  $|w''_i| = \ell''_i$ . Clearly, splitting can be performed in polynomial time. With the help of splitting operations we can also remove a given set of positions from a cycle compressed word in polynomial time.

This leads us to our NP-algorithm: First we construct the NFAs  $\mathcal{A}_i$  as above. By Lemma 8.8 each NFA  $\mathcal{A}_i$  recognizes a bounded language. Hence for each  $i \in [1, k+1]$ , Lemma 8.7 allows us to compute in polynomial time words  $\beta_{i,1}, \dots, \beta_{i,m_i}$  such that  $L(\mathcal{A}_i) \subseteq \beta_{i,1}^* \cdots \beta_{i,m_i}^*$ . For each  $\mathcal{A}_i$  we guess a cycle compression  $(\beta_{i,1}, \ell_{i,1}, \dots, \beta_{i,m_i}, \ell_{i,m_i})$  of a word  $\alpha_i$  such that the words  $\alpha_1, \dots, \alpha_{k+1}$  have equal length  $\ell$ . Then, we test in polynomial time whether  $\alpha_i$  is accepted by  $\mathcal{A}_i$  (this is a restricted case of the *compressed membership problem* of a regular language [15]). Next we verify in polynomial time whether the markers of the  $\alpha_i$  are consistent and whether the position of the origin in  $\alpha_1$  coincides with the position of the cursor in  $\alpha_{k+1}$ . If so, we remove all markers from the words  $\alpha_i$ .

Finally we reduce to instances of  $\text{EXPEQ}(G)$  and  $\text{MEMBERSHIP}(G_*^\rho)$ . Denote with  $P = \{p_1, \dots, p_r\} \subseteq [1, \ell]$  the set of positions  $p$  such that there exists a variable  $x_i \in X_0$  occurring in  $\alpha_i[p]$ , which is the expression at position  $p$  in  $\alpha_i$ . Note that if a variable  $x_i \in X_0$  occurs in  $\alpha_i$ , then by definition of  $X_0$  and set representations,  $\alpha_i$  contains at most  $|u_i|^{O(1)}$  positions with an expression  $\neq 1$ . We can therefore compute  $P$  in polynomial time and obtain an instance of  $\text{EXPEQ}(G)$  containing the expression  $\alpha_1[p_j] \cdots \alpha_{k+1}[p_j]$  for each  $j \in [1, r]$ . We then remove the positions in  $P$  from the words  $\alpha_i$  and compute cycle compressions  $(\beta_{i,1}, \ell_{i,1}, \dots, \beta_{i,m_i}, \ell_{i,m_i})$  of the new words  $\alpha_i$  in polynomial time.

The remaining words reduce to instances of  $\text{MEMBERSHIP}(G_*^\rho)$  as follows: Consider the set of at most  $\sum_{i=1}^{k+1} m_i$  positions at which some cycle factor begins in  $\alpha_i$ . By splitting all words  $\alpha_i$  along these positions we obtain new cycle compressions of the form  $(\beta_{i,1}, \ell_1, \dots, \beta_{i,m}, \ell_m)$  of  $\alpha_i$ , i.e., the  $j$ -th cycle factor has uniform length across all  $\alpha_i$ . From this representation one easily obtains  $m$  instances of  $\text{MEMBERSHIP}(G_*^\rho)$ .  $\square$

Proposition 8.10 yields the NP upper bound for Theorem 5.7: If  $G$  is a finitely generated abelian group, then  $G \cong \mathbb{Z}^n \oplus \bigoplus_{i=1}^m (\mathbb{Z}/r_i\mathbb{Z})$  for some  $n, r_1, \dots, r_m \in \mathbb{N}$ , so that  $\text{EXPEQ}(G)$

corresponds to the solvability problem for linear equation systems over the integers, possibly with modulo-constraints (if  $m > 0$ ). This is a well known problem in NP. Moreover,  $\text{MEMBERSHIP}(G_*^\rho)$  belongs to  $\text{TC}^0$  by Theorem 8.2.

It remains to prove the NP-hardness part of Theorem 5.7, which is the content of the next section.

### 8.3. NP-hardness.

**Theorem 8.11.** *If  $G$  is non-trivial, then  $\text{KP}(G \wr \mathbb{Z})$  is NP-hard.*

*Proof.* Since every non-trivial group contains a non-trivial cyclic group, we may assume that  $G$  is non-trivial and abelian. We reduce from 3-dimensional matching, 3DM for short. In this problem, we have a set of triples  $T = \{e_1, \dots, e_t\} \subseteq [1, q] \times [1, q] \times [1, q]$  for some  $q \geq 1$ , and the question whether there is a subset  $M \subseteq T$  such that  $|M| = q$  and all pairs  $(i, j, k), (i', j', k') \in M$  with  $(i, j, k) \neq (i', j', k')$  satisfy  $i \neq i', j \neq j'$  and  $k \neq k'$ ; such a set  $M$  is called a matching. Since we will write all group operations multiplicatively, we denote the generator of  $\mathbb{Z}$  by  $a$ .

Let  $G$  be a non-trivial group and  $g \in G \setminus \{1\}$ . We reduce 3DM to  $\text{KP}(G \wr \mathbb{Z})$  in the following way: for every  $e_l = (i, j, k) \in T$  let

$$\begin{aligned} w_l &= a^i g a^{q-i+j} g a^{q-j+k} g a^{-2q-k+(3q+1)l} g a^{-(3q+1)l} \\ &= \underbrace{a^i g a^{q-i+j} g a^{q-j+k} g a^{-2q-k}}_{u_l} \underbrace{a^{(3q+1)l} g a^{-(3q+1)l}}_{v_l}. \end{aligned}$$

Intuitively,  $u_l$  is the word that puts  $g$  on positions  $i$ ,  $q+j$  and  $2q+k$ , and  $v_l$  puts  $g$  on position  $(3q+1)l$  and then moves the cursor back to 0. Hence,  $v_l$  is contained in  $G^{(\mathbb{Z})}$  and thus commutes with every element of  $G \wr \mathbb{Z}$  (recall that  $G$  is abelian).

We define the knapsack expression

$$E = w_1^{x_1} \dots w_t^{x_t} (ag^{-1})^{3q} a^{-3q} \prod_{i=1}^q (a^{(3q+1)y_i} g^{-1}) a^{-(3q+1)y_{q+1}}$$

with variables  $x_1, \dots, x_t, y_1, \dots, y_{q+1}$ . For all values of these variables, the following equivalences hold.

$$\begin{aligned} w_1^{x_1} \dots w_t^{x_t} (ag^{-1})^{3q} a^{-3q} \prod_{i=1}^q (a^{(3q+1)y_i} g^{-1}) a^{-(3q+1)y_{q+1}} &= 1 \quad \Leftrightarrow \\ u_1^{x_1} \dots u_t^{x_t} (ag^{-1})^{3q} a^{-3q} v_1^{x_1} \dots v_t^{x_t} \prod_{i=1}^q (a^{(3q+1)y_i} g^{-1}) a^{-(3q+1)y_{q+1}} &= 1 \quad \Leftrightarrow \\ \underbrace{u_1^{x_1} \dots u_t^{x_t} (ag^{-1})^{3q} a^{-3q}}_{E_1} = 1 \text{ and } \underbrace{v_1^{x_1} \dots v_t^{x_t} \prod_{i=1}^q (a^{(3q+1)y_i} g^{-1}) a^{-(3q+1)y_{q+1}}}_{E_2} &= 1 \end{aligned}$$

The second equivalence holds because (i) for all values of the variables, the word  $E_1$  only affects positions from the interval  $[1, 3q]$ , whereas the word  $E_2$  only affects positions that are multiples of  $3q+1$  and (ii)  $E_2$  represents a word in  $G^{(\mathbb{Z})}$ .

First assume that there is a matching  $M \subseteq T$ . We define a valuation  $\nu$  for  $E$  by  $\nu(x_i) = 1$  if  $e_i \in M$  and  $\nu(x_i) = 0$  if  $e_i \notin M$ . Let  $M = \{e_{m_1}, \dots, e_{m_q}\}$  such that  $m_i < m_j$  for  $i < j$  and let  $m_0 = 0$ . Then we set  $\nu(y_i) = m_i - m_{i-1}$  for  $1 \leq i \leq q$ , and  $\nu(y_{q+1}) = m_q$ . Since  $M$  is a matching, we have

$$\nu(u_{e_1}^{x_1} \dots u_{e_t}^{x_t}) = \prod_{e_l \in M} u_l = (ag)^{3q} a^{-3q}$$

and thus  $\nu(E_1) = 1$ . Furthermore, we have

$$\nu(v_{e_1}^{x_1} \cdots v_{e_t}^{x_t}) = \prod_{i=1}^q a^{(3q+1)m_i} g a^{-(3q+1)m_i} = \prod_{i=1}^q (a^{(3q+1)(m_i-m_{i-1})} g) a^{-(3q+1)m_q}$$

and thus  $\nu(E_2) = 1$ .

Now assume that there is a valuation  $\nu$  for  $E$  with  $\nu(E_1) = \nu(E_2) = 1$ . Let  $n_i = \nu(x_i)$  and  $m_i = \nu(y_i)$ . For every  $1 \leq l \leq t$ , we must have  $g^{n_l} \in \{1, g\}$ , i.e.,  $n_l \equiv 0 \pmod{\text{ord}(g)}$  or  $n_l \equiv 1 \pmod{\text{ord}(g)}$ . We first show that  $q' := \#\{l \mid n_l \equiv 1 \pmod{\text{ord}(g)}\} = q$ . This follows from  $\nu(E_2) = 1$  and the fact that the effect of  $\prod_{i=1}^q a^{(3q+1)m_i} g^{-1}$  is to multiply the  $G$ -elements at exactly  $q$  many positions  $p$  ( $p \equiv 0 \pmod{3q+1}$ ) with  $g^{-1}$ . Hence, the effect of  $v_1^{n_1} \cdots v_t^{n_t}$  must be to multiply the  $G$ -elements at exactly  $q$  many positions  $p$  ( $p \equiv 0 \pmod{3q+1}$ ) with  $g$ . But this means that  $q' = q$ .

So we can assume that  $q' = q$ . We finally show that  $M = \{e_l \mid n_l \equiv 1 \pmod{\text{ord}(g)}\} \subseteq T$  is a matching: Assume that there are  $e = (i, j, k) \in M$  and  $e' = (i', j', k') \in M$  with  $i = i', j = j'$  or  $k = k'$ . Since  $q' = q$  this would imply that at most  $3q - 1$  positions  $p$  with  $1 \leq p \leq 3q$  can be set to  $g$  by the word  $u_{e_1}^{n_1} \cdots u_{e_t}^{n_t}$ . But then,  $(ag^{-1})^{3q} a^{-3q}$  would leave a position with value  $g^{-1}$ , and hence  $\nu(E_1) \neq 1$ . Hence,  $M$  must be a matching. Notice that the argumentation of the whole proof still works in the case that we allow the variables  $x_1, \dots, x_t, y_1, \dots, y_{q+1}$  to be integers instead of naturals.  $\square$

Note that the above NP-hardness proof also works for the subset sum problem, where the range of the valuation is restricted to  $\{0, 1\}$ . Moreover, if the word problems for two groups  $G$  and  $H$  can be solved in polynomial time, then word problem for  $G \wr H$  can be solved in polynomial time as well [21]. This implies that subset sum for  $G \wr H$  belongs to NP. Thus, we obtain:

**Theorem 8.12.** *Let  $G$  and  $H$  be non-trivial finitely generated groups and assume that  $H$  contains an element of infinite order. Then, the subset sum problem for  $G \wr H$  is NP-hard. If moreover, the word problem for  $G$  and  $H$  can be solved in polynomial time, then the subset sum problem for  $G \wr H$  is NP-complete.*

## 9. OPEN PROBLEMS

Our results yield decidability of  $\text{KP}(G \wr H)$  for almost all groups  $G$  and  $H$  that are known to satisfy the necessary conditions. However, we currently have no complete characterization of those  $G$  and  $H$  for which  $\text{KP}(G \wr H)$  is decidable.

Several interesting open problems concerning the complexity of knapsack for wreath products remain. We are confident that our NP upper bound for  $\text{KP}(G \wr \mathbb{Z})$ , where  $G$  is finitely generated abelian, can be extended to  $\text{KP}(G \wr F)$  for a finitely generated free group  $G$  as well as to  $\text{KP}(G \wr \mathbb{Z}^k)$ . Another question is whether the assumption on  $G$  being abelian can be weakened. In particular, we want to investigate whether polynomial time algorithms exist for  $\text{MEMBERSHIP}(G_*^p)$  for certain non-abelian groups  $G$ .

The complexity of knapsack for free solvable groups is open as well. Our decidability proof uses the preservation of knapsack-semilinearity under wreath products (Theorem 5.5). Our construction in the proof of Theorem 5.5 adds for every application of the wreath product a  $\forall^* \exists^*$ -quantifier prefix in the formula describing the solution set. Since a free solvable group of class  $d$  and rank  $r$  is embedded into a  $d$ -fold iterated wreath product of  $\mathbb{Z}^r$ , this leads to a  $\Pi_{2(d-1)}$ -formula (for  $d = 1$ , we clearly have a  $\Pi_0$ -formula). The existence of a solution is then expressed by a  $\Sigma_{2d-1}$ -formula. Haase [9] has shown that the  $\Sigma_{i+1}$ -fragment of Presburger arithmetic is complete for the  $i$ -th level of the so-called weak EXP hierarchy. In addition to the complexity resulting from the quantifier alternations in Presburger arithmetic, our algorithm incurs a doubly exponential increase in the formula size for each application of the wreath product. This leads to the question whether there is a more efficient algorithm for knapsack over free solvable groups.

Finally, we are confident that with our techniques from [18] one can also show preservation of knapsack-semilinearity under graph products.

## REFERENCES

- [1] Tara C. Davis and Alexander Yu. Olshanskii. Subgroup distortion in wreath products of cyclic groups. *Journal of Pure and Applied Algebra*, 215(12):2987–3004, 2011.
- [2] Samuel Eilenberg and Marcel P. Schützenberger. Rational sets in commutative monoids. *Journal of Algebra*, 13:173–191, 1969.
- [3] Michael Elberfeld, Andreas Jakoby, and Till Tantau. Algorithmic meta theorems for circuit classes of constant and logarithmic depth. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:128, 2011.
- [4] Elizaveta Frenkel, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016.
- [5] Paweł Gawrychowski, Dalia Krieger, and Jeffrey Shallit Narad Rampersad. Finding the growth rate of a regular or context-free language in polynomial time. *International Journal of Foundations of Computer Science*, 21(04):597–618, 2010.
- [6] Etienne Ghys and Pierre de la Harpe. *Sur les groupes hyperboliques d’après Mikhael Gromov*. Progress in mathematics. Birkhäuser, 1990.
- [7] Seymour Ginsburg and Edwin H. Spanier. Semigroups, Presburger formulas, and languages. *Pacific Journal of Mathematics*, 16(2):285–296, 1966.
- [8] Christoph Haase. *On the complexity of model checking counter automata*. PhD thesis, University of Oxford, St Catherine’s College, 2011.
- [9] Christoph Haase. Subclasses of presburger arithmetic and the weak EXP hierarchy. In *Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS 2014*, pages 47:1–47:10. ACM, 2014.
- [10] William Hesse, Eric Allender, and David A. Mix Barrington. Uniform constant-depth threshold circuits for division and iterated multiplication. *Journal of Computer and System Sciences*, 65:695–716, 2002.
- [11] Richard M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.
- [12] Daniel König, Markus Lohrey, and Georg Zetsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. In *Algebra and Computer Science*, volume 677 of *Contemporary Mathematics*, pages 138–153. American Mathematical Society, 2016.
- [13] Daniel König and Markus Lohrey. Evaluation of circuits over nilpotent and polycyclic groups. *Algorithmica*, 2017.
- [14] Jörg Lehnert and Pascal 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] Markus Lohrey. Algorithmics on SLP-compressed strings: A survey. *Groups Complexity Cryptology*, 4(2):241–299, 2012.
- [16] Markus Lohrey, Benjamin Steinberg, and Georg Zetsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015.
- [17] Markus Lohrey and Georg Zetsche. Knapsack in graph groups, HNN-extensions and amalgamated products. *CoRR*, abs/1509.05957, 2015.
- [18] Markus Lohrey and Georg Zetsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In Nicolas Ollinger and Heribert Vollmer, editors, *Proc. of the 33rd International Symposium on Theoretical Aspects of Computer Science (STACS 2016)*, volume 47 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 50:1–50:14, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [19] Markus Lohrey and Georg Zetsche. The complexity of knapsack in graph groups. In *Proceedings of the 34th Symposium on Theoretical Aspects of Computer Science, STACS 2017*, volume 66 of *LIPIcs*, pages 52:1–52:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.
- [20] Wilhelm Magnus. On a theorem of Marshall Hall. *Annals of Mathematics. Second Series*, 40:764–768, 1939.
- [21] Alexei Miasnikov, Svetla Vassileva, and Armin Weiß. The conjugacy problem in free solvable groups and wreath products of abelian groups is in  $TC^0$ . In *Computer Science – Theory and Applications – 12th International Computer Science Symposium in Russia, CSR 2017, Proceedings*, volume 10304 of *Lecture Notes in Computer Science*, pages 217–231. Springer, 2017.
- [22] Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017.
- [23] Alexei Myasnikov, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015.



- [24] Alexei Myasnikov and Andrey Nikolaev. Verbal subgroups of hyperbolic groups have infinite width. *Journal of the London Mathematical Society*, 90(2):573–591, 2014.
- [25] Alexei Myasnikov and Armin Weiß.  $TC^0$  circuits for algorithmic problems in nilpotent groups. *CoRR*, abs/1702.06616, 2017.
- [26] Andrey Nikolaev and Alexander Ushakov. Subset sum problem in polycyclic groups. *Journal of Symbolic Computation*, 84:84–94, 2018.
- [27] Charles Sims. *Computation with finitely presented groups*. Cambridge University Press, 1994.

## APPENDIX A. HYPERBOLIC GROUPS

Let  $G$  be a finitely generated group with the finite symmetric generating set  $\Sigma$ . The Cayley-graph of  $G$  (with respect to  $\Sigma$ ) is the undirected graph  $\Gamma = \Gamma(G)$  with node set  $G$  and all edges  $(g, ga)$  for  $g \in G$  and  $a \in \Sigma$ . We view  $\Gamma$  as a geodesic metric space, where every edge  $(g, ga)$  is identified with a unit-length interval. It is convenient to label the directed edge from  $g$  to  $ga$  with the generator  $a$ . The distance between two points  $p, q$  is denoted with  $d_\Gamma(p, q)$ . For  $g \in G$  let  $|g| = d_\Gamma(1, g)$ . For  $r \geq 0$ , let  $B_r(1) = \{g \in G \mid d_\Gamma(1, g) \leq r\}$ .

Given a word  $w \in \Sigma^*$ , one obtains a unique path  $P[w]$  that starts in 1 and is labelled with the word  $w$ . This path ends in the group element represented by  $w$ . More generally, for  $g \in G$  we denote with  $g \cdot P[w]$  the path that starts in  $g$  and is labelled with  $w$ . We will only consider paths of the form  $g \cdot P[w]$ . One views  $g \cdot P[w]$  as a continuous mapping from the real interval  $[0, |w|]$  to  $\Gamma$ . Such a path  $P : [0, n] \rightarrow \Gamma$  is geodesic if  $d_\Gamma(P(0), P(n)) = n$ ; it is a  $(\lambda, \epsilon)$ -quasigeodesic if for all points  $p = P(a)$  and  $q = P(b)$  we have  $|a - b| \leq \lambda \cdot d_\Gamma(p, q) + \epsilon$ . We say that a path  $P : [0, n] \rightarrow \Gamma$  is path from  $P(0)$  to  $P(n)$ . A word  $w \in \Sigma^*$  is geodesic if the path  $P[w]$  is geodesic.

A geodesic triangle consists of three points  $p, q, r \in G$  and geodesic paths  $P_{p,q}, P_{p,r}, P_{q,r}$  (the three sides of the triangle), where  $P_{x,y}$  is a path from  $x$  to  $y$ . For  $\delta \geq 0$ , the group  $G$  is  $\delta$ -hyperbolic, if for every geodesic triangle, every point  $p$  on one of the three sides has distance at most  $\delta$  from a point belonging to one of the two sides that are opposite of  $p$ . Finally,  $G$  is hyperbolic, if it is  $\delta$ -hyperbolic for some  $\delta \geq 0$ . Finitely generated free groups are for instance 0-hyperbolic. The property of being hyperbolic is independent of the chosen generating set. The word problem for every hyperbolic group is decidable in linear time. This allows to compute for a given word  $w$  an equivalent geodesic word; the best known algorithm is quadratic.

Let us fix a  $\delta$ -hyperbolic group  $G$  with the finite symmetric generating set  $\Sigma$  for the further discussion.

**Lemma A.1** (c.f. [6, 8.21]). *Let  $g \in G$  be of infinite order and let  $n \geq 1$ . Let  $u$  be a geodesic word representing  $g$ . Then the path  $P[u^n]$  is a  $(\lambda, \epsilon)$ -quasigeodesic, where  $\lambda = |g|N$ ,  $\epsilon = 2|g|^2N^2 + 2|g|N$  and  $N = |B_{2\delta}(1)|$ .*

Consider two paths  $P_1 : [0, n_1] \rightarrow \Gamma$ ,  $P_2 : [0, n_2] \rightarrow \Gamma$  and let  $K$  be a positive real number. We say that  $P_1$  and  $P_2$  asynchronously  $K$ -fellow travel if there exist two continuous non-decreasing mappings  $\varphi_1 : [0, 1] \rightarrow [0, n_1]$  and  $\varphi_2 : [0, 1] \rightarrow [0, n_2]$  such that  $\varphi_1(0) = \varphi_2(0) = 0$ ,  $\varphi_1(1) = n_1$ ,  $\varphi_2(1) = n_2$  and for all  $0 \leq t \leq 1$ ,  $d_\Gamma(P_1(\varphi_1(t)), P_2(\varphi_2(t))) \leq K$ . Intuitively, this means that one can travel along the paths  $P_1$  and  $P_2$  asynchronously with variable speeds such that at any time instant the current points have distance at most  $K$ .

**Lemma A.2** (c.f. [24]). *Let  $P_1$  and  $P_2$  be  $(\lambda, \epsilon)$ -quasigeodesic paths in  $\Gamma_G$  and assume that  $P_i$  starts in  $g_i$  and ends in  $h_i$ . Assume that  $d_\Gamma(g_1, h_1), d_\Gamma(g_2, h_2) \leq h$ . Then there exists a computable bound  $K = K(\delta, \lambda, \epsilon, h) \geq h$  such that  $P_1$  and  $P_2$  asynchronously  $K$ -fellow travel.*

**A.1. Hyperbolic groups are knapsack-semilinear.** In this section, we prove the following result:

**Theorem A.3.** *Every hyperbolic group is knapsack-semilinear.*

Let us fix a  $\delta$ -hyperbolic group  $G$  and let  $\Sigma$  be a finite symmetric generating set for  $G$ . We first consider knapsack instances of depth 2.

**Lemma A.4.** *For all  $g_1, h_1, g_2, h_2 \in G$  such that  $g_1$  and  $g_2$  have infinite order, the set  $\{(x_1, x_2) \mid h_1 g_1^{x_1} = g_2^{x_2} h_2 \text{ in } G\}$  is effectively semilinear.*

*Proof.* The semilinear subsets of  $\mathbb{N}^k$  are exactly the rational subsets of  $\mathbb{N}^k$  [2]. A subset  $A \subseteq \mathbb{N}^k$  is rational if it is a homomorphic image of a regular set of words. In other words, there exists a finite automaton with transitions labeled by elements of  $\mathbb{N}^k$  such that  $A$  is the set of  $v \in \mathbb{N}^k$  that are obtained by summing the transition labels along a path from the initial state to a final state. We prove that the set  $\{(x_1, x_2) \mid h_1 g_1^{x_1} = g_2^{x_2} h_2 \text{ in } G\}$  is effectively rational.

Let  $u_i$  be a geodesic word representing  $g_i$  and let  $\ell_i = |u_i|$ . Assume that  $n_1, n_2 \geq 1$  are such that  $h_1 g_1^{n_1} = g_2^{n_2} h_2$ . Let  $P_1 = h_1 \cdot P[u_1^{n_1}]$  and let  $P_2 = P[u_2^{n_2}]$ . By Lemma A.1,  $P_1$  and  $P_2$  are  $(\lambda, \epsilon)$ -quasigeodesics, where  $\lambda$  and  $\epsilon$  only depend on  $\delta$ ,  $|u_1|$  and  $|u_2|$ . By Lemma A.2, the paths  $P_1$  and  $P_2$  asynchronously  $K$ -fellow travel, where  $K$  is a computable bound that only depends on  $\delta$ ,  $\lambda$ ,  $\epsilon$ ,  $|g_1|$ ,  $|h_1|$ ,  $|g_2|$ ,  $|h_2|$ . Let  $\varphi_1 : [0, 1] \rightarrow [0, n_1 \cdot \ell_1]$  and  $\varphi_2 : [0, 1] \rightarrow [0, n_2 \cdot \ell_2]$  be the corresponding continuous non-decreasing mappings.

Let  $p_{1,i} = h_1 g_1^i = P_1(i \cdot \ell_1)$  for  $0 \leq i \leq n_1$  and  $p_{2,j} = g_2^j = P_2(j \cdot \ell_2)$  for  $0 \leq j \leq n_2$ . Thus,  $p_{1,i}$  is a point on  $P_1$  and  $p_{2,j}$  is a point on  $P_2$ . We define the binary relation  $R \subseteq \{p_{1,i} \mid 0 \leq i \leq n_1\} \times \{p_{2,j} \mid 0 \leq j \leq n_2\}$  by

$$R = \{(p_{1,i}, p_{2,j}) \mid \exists r \in [0, 1] : \varphi_1(r) \in [i \cdot \ell_1, (i+1) \cdot \ell_1), \varphi_2(r) \in [j \cdot \ell_2, (j+1) \cdot \ell_2)\}.$$

Thus, we take all pairs  $(P_1(\varphi_1(r)), P_2(\varphi_2(r)))$ , and push the first (resp., second) point in this pair back along  $P_1$  (resp.,  $P_2$ ) to the next point  $p_{1,i}$  (resp.,  $p_{2,j}$ ). Then  $R$  has the following properties:

- $(0, 0), (n_1, n_2) \in R$
- If  $(p_{1,i}, p_{2,j}) \in R$  and  $(i, j) \neq (n_1, n_2)$  then one of the following pairs also belongs to  $R$ :  $(p_{1,i+1}, p_{2,j})$ ,  $(p_{1,i}, p_{2,j+1})$ ,  $(p_{1,i+1}, p_{2,j+1})$ .
- If  $(p_{1,i}, p_{2,j}) \in R$ , then  $d_\Gamma(p_{1,i}, p_{2,j}) \leq K + \ell_1 + \ell_2$ .

Let  $r = K + \ell_1 + \ell_2$ . We can now construct a finite automaton over  $\mathbb{N} \times \mathbb{N}$  that accepts the set  $\{(x_1, x_2) \mid h_1 g_1^{x_1} = g_2^{x_2} h_2 \text{ in } G\}$ . The set of states consists of  $B_r(1)$ . The initial state is  $h_1$ , the final state is  $h_2$ . Finally, the transitions are the following:

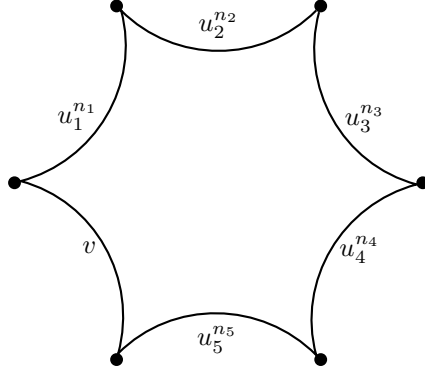
- $p \xrightarrow{(0,1)} q$  for  $p, q \in B_r(1)$  if  $p = g_2 q$
- $p \xrightarrow{(1,0)} q$  for  $p, q \in B_r(1)$  if  $p g_1 = q$
- $p \xrightarrow{(1,1)} q$  for  $p, q \in B_r(1)$  if  $p g_1 = g_2 q$

By the above consideration, it is clear that this automaton accepts the set  $\{(x_1, x_2) \mid h_1 g_1^{x_1} = g_2^{x_2} h_2 \text{ in } G\}$ .  $\square$

We can now prove Theorem A.3.

*Proof of Theorem A.3.* Consider a knapsack expression  $E = v_1 u_1^{x_1} v_2 u_2^{x_2} v_3 \cdots u_k^{x_k} v_{k+1}$ . We want to show that the set of all solutions of  $E = 1$  is a semilinear subset of  $\mathbb{N}^k$ . For this we construct a Presburger formula with free variables  $x_1, \dots, x_k$  that is equivalent to  $E = 1$ . We do this by induction on the depth  $k$ . Therefore, we can use in our Presburger formula also knapsack equations of the form  $F = 1$ , where  $F$  has depth at most  $k - 1$ .

Let  $g_i \in G$  be the group element represented by the word  $u_i$ . In a hyperbolic group the order of torsion elements is bounded by a fixed constant that only depends on the group, see also the proof of [23, Theorem 6.7]. This allows to check for each  $g_i$  whether it has finite order, and to compute the order in the positive case. Assume that  $g_i$  has finite order  $m_i$ . We then produce for every number  $0 \leq d \leq m_i - 1$  a knapsack instance of depth  $k - 1$  by replacing  $u_i^{x_i}$  by  $u_i^d$ , which by induction can be transformed into an equivalent Presburger formula. We then take the disjunction of all these Presburger formulae for all  $0 \leq d \leq m_i - 1$ . A similar argument shows that it suffices to construct a Presburger formula describing all solutions in  $\mathbb{N}_+^k$  (where  $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$ ).

FIGURE 3. The  $(k+1)$ -gon for  $k=5$  from the proof of Theorem A.3

By the above discussion, we can assume that all  $u_i$  represent group elements of infinite order. The case that  $k \leq 2$  is covered by Lemma A.4. Hence, we assume that  $k \geq 3$ . By the above remark, we only need to consider valuations  $\nu$  such that  $\nu(x_i) > 0$  for all  $i \in [1, k]$ . Moreover, we can assume that  $E$  has the form  $u_1^{x_1} \cdots u_k^{x_k} v$ , where all  $u_i$  and  $v$  are geodesic words. By Lemma A.1 for every valuation  $\nu$ , all words  $u_i^{\nu(x_i)}$  are  $(\lambda, \epsilon)$ -quasigeodesics for certain constants  $\lambda$  and  $\epsilon$ .

Consider a solution  $\nu$  and let  $n_i = \nu(x_i)$  for  $i \in [1, k]$ . Consider the polygon obtained by traversing the closed path labelled with  $u_1^{x_1} \cdots u_k^{x_k} v$ . We partition this path into segments  $P_1, \dots, P_k, Q$ , where  $P_i$  is the subpath labelled with  $u_i^{n_i}$  and  $Q$  is the subpath labelled with  $v$ . We consider these subpaths as the sides of a  $(k+1)$ -gon, see Fig. 3. Since all sides of this  $(k+1)$ -gon are  $(\lambda, \epsilon)$ -quasigeodesics, we can apply [23, Lemma 6.4]: Every side of the  $(k+1)$ -gon is contained in the  $h$ -neighborhoods of the other sides, where  $h = (\kappa + \kappa \log(k+1))$  for a constant  $\kappa$  that only depends on the constants  $\delta, \lambda, \epsilon$ .

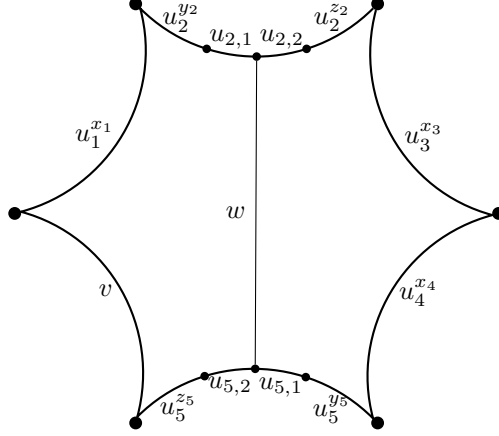
Let us now consider the side  $P_2$  of the quasigeodesic  $(k+1)$ -gon. It is labelled with  $u_2^{x_2}$ . Its neighboring sides are  $P_1$  and  $P_3$  (recall that  $k \geq 3$ ) and are labelled with  $u_1^{x_1}$  and  $u_3^{x_3}$ .<sup>4</sup> We now distinguish the following cases. In each case we cut the  $(k+1)$ -gon into smaller pieces along paths of length  $\leq h$ , and these smaller pieces will correspond to knapsack instances of smaller depth. When we speak of a point on the  $(k+1)$ -gon, we mean a node of the Cayley graph (i.e., an element of the group  $G$ ) and not a point in the interior of an edge. Moreover, when we speak of the successor point of a point  $p$ , we refer to the clockwise order on the  $(k+1)$ -gon, where the sides are traversed in the order  $P_1, \dots, P_k, Q$ .

*Case 1:* There is a point on  $p \in P_2$  that has distance at most  $h$  from a node  $q \in P_4 \cdots P_k$ . Let us assume that  $q \in P_i$  where  $i \in [4, k]$ . We now construct two new knapsack instances  $F_t$  and  $G_t$  for all words  $w \in \Sigma^*$  of length at most  $h$  and all factorizations  $u_2 = u_{2,1}u_{2,2}$  and  $u_i = u_{i,1}u_{i,2}$ , where  $t = (i, w, u_{2,1}, u_{2,2}, u_{i,1}, u_{i,2})$ :

$$\begin{aligned} F_t &= u_1^{x_1} u_2^{y_2} (u_{2,1} w u_{i,2}) u_i^{z_i} u_{i+1}^{x_{i+1}} \cdots u_k^{x_k} v \quad \text{and} \\ G_t &= u_{2,2} u_2^{z_2} u_3^{x_3} \cdots u_{i-1}^{x_{i-1}} u_i^{y_i} (u_{i,1} w^{-1}) \end{aligned}$$

Here  $y_2, z_2, y_i, z_i$  are new variables. The situation looks as follows, where the case  $i = k = 5$  is shown:

<sup>4</sup>We take the side  $P_2$  since  $Q$  is not a neighboring side of  $P_2$ . This avoids some additional cases in the following case distinction.



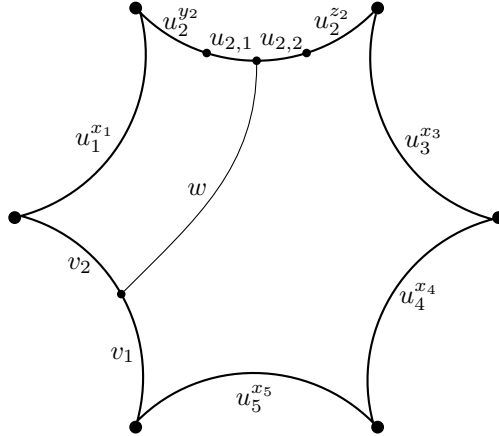
Note that  $F_t$  and  $G_t$  have depth at most  $k-1$ . Lets say that a tuple  $t = (i, w, u_{2,1}, u_{2,2}, u_{i,1}, u_{i,2})$  is valid for case 1 if  $i \in [4, k]$ ,  $w \in \Sigma^*$ ,  $|w| \leq h$ ,  $u_2 = u_{2,1}u_{2,2}$  and  $u_i = u_{i,1}u_{i,2}$ . Moreover, let  $A_1$  be the following formula, where  $t$  ranges over all tuples that are valid for case 1, and  $i$  is the first component of the tuple  $t$ :

$$A_1 = \bigvee_t \exists y_2, z_2, y_i, z_i : x_2 = y_2 + 1 + z_2 \wedge x_i = y_i + 1 + z_i \wedge F_t = 1 \wedge G_t = 1$$

*Case 2:* There is a point on  $p \in P_2$  that has distance at most  $h$  from a node  $q \in Q$ . We construct two new knapsack instances  $F_t$  and  $G_t$  for all words  $w \in \Sigma^*$  of length at most  $h$  and all factorizations  $u_2 = u_{2,1}u_{2,2}$  and  $v = v_1v_2$ , where  $t = (w, u_{2,1}, u_{2,2}, v_1, v_2)$ :

$$\begin{aligned} F_t &= u_1^{x_1} u_2^{y_2} (u_{2,1} w v_2) \text{ and} \\ G_t &= u_{2,2} u_2^{z_2} u_3^{x_3} \cdots u_k^{x_k} (v_1 w^{-1}) \end{aligned}$$

As in case 1,  $y_2, z_2$  are new variables and  $F_t$  and  $G_t$  have depth at most  $k-1$ . The situation looks as follows:



We say that a tuple  $t = (w, u_{2,1}, u_{2,2}, v_1, v_2)$  is valid for case 2 if  $w \in \Sigma^*$ ,  $|w| \leq h$ ,  $u_2 = u_{2,1}u_{2,2}$  and  $v = v_1v_2$ . Moreover, let  $A_2$  be the following formula, where  $t$  ranges over all tuples that are valid for case 2:

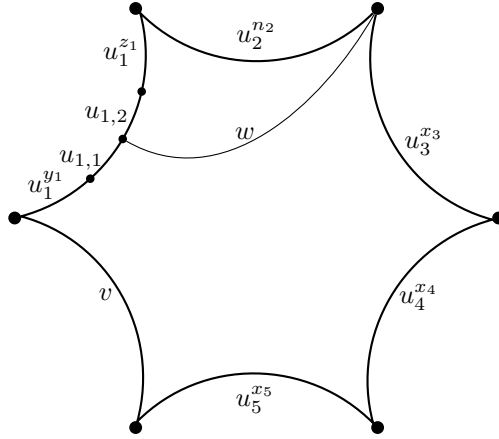
$$A_2 = \bigvee_t \exists y_2, z_2 : x_2 = y_2 + 1 + z_2 \wedge F_t = 1 \wedge G_t = 1$$

*Case 3:* Every point  $p \in P_2$  has distance at most  $h$  from a point on  $P_1$ . Let  $q$  be the unique point in  $P_2 \cap P_3$  and let  $p \in P_1$  be a point with  $d_\Gamma(p, q) \leq h$ . We construct two new

knapsack instances  $F_t$  and  $G_t$  for all words  $w \in \Sigma^*$  of length at most  $h$  and all factorizations  $u_1 = u_{1,1}u_{1,2}$ , where  $t = (w, u_{1,1}, u_{1,2})$ :

$$\begin{aligned} F_t &= u_1^{y_1}(u_{1,1}w)u_3^{x_3} \cdots u_k^{x_k}v \quad \text{and} \\ G_t &= u_{1,2}u_1^{z_1}u_2^{x_2}w^{-1} \end{aligned}$$

Since  $k \geq 3$ ,  $F_t$  and  $G_t$  have depth at most  $k - 1$ . The situation looks as follows:



We say that a triple  $t = (w, u_{1,1}, u_{1,2})$  is valid for case 3 if  $w \in \Sigma^*$ ,  $|w| \leq h$  and  $u_1 = u_{1,1}u_{1,2}$ . Moreover, let  $A_3$  be the following formula, where  $t$  ranges over all tuples that are valid for case 3:

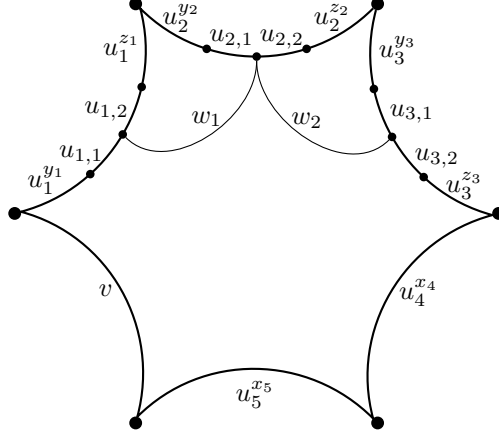
$$A_3 = \bigvee_t \exists y_1, z_1 : x_1 = y_1 + 1 + z_1 \wedge F_t = 1 \wedge G_t = 1$$

*Case 4:* Every point  $p \in P_2$  has distance at most  $h$  from a point on  $P_3$ . This case is of course completely analogous to case 3 and yields a corresponding formula  $A_4$ .

*Case 5:* Every point  $p \in P_2$  has distance at most  $h$  from a point on  $P_1 \cup P_3$  but  $P_2$  is neither contained in the  $h$ -neighborhood of  $P_1$  nor in the  $h$ -neighborhood of  $P_3$ . Hence there exists points  $p_1, p_3 \in P_2$  which are connected by an edge and such that  $p_1$  has distance at most  $h$  from  $P_1$  and  $p_3$  has distance at most  $h$  from  $P_3$ . Therefore,  $p_1$  has distance at most  $h+1$  from  $P_1$  as well as distance at most  $h+1$  from  $P_3$ . We construct three new knapsack instances  $F_t$ ,  $G_t$ ,  $H_t$  for all words  $w_1, w_2 \in \Sigma^*$  with  $|w_1|, |w_2| \leq h+1$  and all factorizations  $u_1 = u_{1,1}u_{1,2}$ ,  $u_2 = u_{2,1}u_{2,2}$ , and  $u_3 = u_{3,1}u_{3,2}$ , where  $t = (w_1, w_2, u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2}, u_{3,1}, u_{3,2})$ :

$$\begin{aligned} F_t &= u_1^{y_1}(u_{1,1}w_1w_2u_{3,2})u_3^{z_3}u_4^{x_4} \cdots u_k^{x_k}v, \\ G_t &= u_{1,2}u_1^{z_1}u_2^{y_2}u_{2,1}w_1^{-1}, \\ H_t &= u_{2,2}u_2^{z_2}u_3^{y_3}u_{3,1}w_2^{-1} \end{aligned}$$

Since  $k \geq 3$ ,  $F_t$ ,  $G_t$  and  $H_t$  have depth at most  $k - 1$ . The situation looks as follows:



We say that a tuple  $t = (w_1, w_2, u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2}, u_{3,1}, u_{3,2})$  is valid for case 5 if  $w_1, w_2 \in \Sigma^*$ ,  $|w_1|, |w_2| \leq h + 1$ ,  $u_1 = u_{1,1}u_{1,2}$ ,  $u_2 = u_{2,1}u_{2,2}$ , and  $u_3 = u_{3,1}u_{3,2}$ . Moreover, let  $A_5$  be the following formula, where  $t$  ranges over all tuples that are valid for case 5:

$$A_5 = \bigvee_t \exists y_1, z_1, y_2, z_2, y_3, z_3 : x_1 = y_1 + 1 + z_1 \wedge x_2 = y_2 + 1 + z_2 \wedge x_3 = y_3 + 1 + z_3 \wedge \\ F_t = 1 \wedge G_t = 1 \wedge H_t = 1.$$

Our final formula is  $A_1 \vee A_2 \vee A_3 \vee A_4 \vee A_5$ . It is easy to check that a valuation  $\nu : \{x_1, \dots, x_k\}$  satisfies  $\nu(E) = 1$  if and only if  $\nu$  makes  $A_1 \vee A_2 \vee A_3 \vee A_4 \vee A_5$  true. If  $\nu(E) = 1$  holds, then one of the above five cases holds, in which case  $\nu$  makes the corresponding formula  $A_i$  true. Vice versa, if  $\nu$  makes one of the formulas  $A_i$  true then  $\nu(E) = 1$  holds.  $\square$

UNIVERSITÄT SIEGEN, GERMANY, {GANARDI,KOENIG,LOHREY}@ETI.UNI-SIEGEN.DE

LSV, CNRS & ENS PARIS-SACLAY, FRANCE, ZETZSCHE@LSV.FR