

A Characterization of Wreath Products Where Knapsack Is Decidable

Pascal Bergsträßer 

Fachbereich Informatik, Technische Universität Kaiserslautern, Germany

Moses Ganardi 

Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern, Germany

Georg Zetsche 

Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern, Germany

Abstract

The knapsack problem for groups was introduced by Miasnikov, Nikolaev, and Ushakov. It is defined for each finitely generated group G and takes as input group elements $g_1, \dots, g_n, g \in G$ and asks whether there are $x_1, \dots, x_n \geq 0$ with $g_1^{x_1} \cdots g_n^{x_n} = g$. We study the knapsack problem for wreath products $G \wr H$ of groups G and H .

Our main result is a characterization of those wreath products $G \wr H$ for which the knapsack problem is decidable. The characterization is in terms of decidability properties of the individual factors G and H . To this end, we introduce two decision problems, the *intersection knapsack problem* and its restriction, the *positive intersection knapsack problem*.

Moreover, we apply our main result to $H_3(\mathbb{Z})$, the discrete Heisenberg group, and to Baumslag-Solitar groups $BS(1, q)$ for $q \geq 1$. First, we show that the knapsack problem is undecidable for $G \wr H_3(\mathbb{Z})$ for any $G \neq 1$. This implies that for $G \neq 1$ and for infinite and virtually nilpotent groups H , the knapsack problem for $G \wr H$ is decidable if and only if H is virtually abelian and solvability of systems of exponent equations is decidable for G . Second, we show that the knapsack problem is decidable for $G \wr BS(1, q)$ if and only if solvability of systems of exponent equations is decidable for G .

2012 ACM Subject Classification Theory of computation \rightarrow Problems, reductions and completeness; Theory of computation \rightarrow Theory and algorithms for application domains

Keywords and phrases knapsack, wreath products, decision problems in group theory, decidability, discrete Heisenberg group, Baumslag-Solitar groups

Digital Object Identifier 10.4230/LIPIcs.STACS.2021.11

Related Version This paper is based on the following technical report:

Full Version: <https://arxiv.org/abs/2101.06132> [5]

1 Introduction

The knapsack problem. The knapsack problem is a decision problem for groups that was introduced by Myasnikov, Nikolaev, and Ushakov [27]. If G is a finitely generated group, then the knapsack problem for G , denoted $KP(G)$, takes group elements $g_1, \dots, g_n, g \in G$ as input (as words over the generators) and it asks whether there are natural numbers $x_1, \dots, x_n \geq 0$ such that $g_1^{x_1} \cdots g_n^{x_n} = g$. Since its introduction, a significant amount of attention has been devoted to understanding for which groups the problem is decidable and what the resulting complexity is [17, 20, 10, 26, 16, 9, 21, 7]. For matrix semigroups, the knapsack problem has been studied implicitly by Bell, Halava, Harju, Karhumäki, and Potapov [3], Bell, Potapov, and Semukhin [4], and for commuting matrices by Babai, Beals, Cai, Ivanyos, and Luks [1].

There are many groups for which knapsack has been shown decidable. For example, knapsack is decidable for virtually special groups [20, Theorem 3.1], co-context-free groups [16, Theorem 8.1], hyperbolic groups [27, Theorem 6.1], the discrete Heisenberg group [16,



© Pascal Bergsträßer, Moses Ganardi, and Georg Zetsche;
licensed under Creative Commons License CC-BY 4.0

38th International Symposium on Theoretical Aspects of Computer Science (STACS 2021).

Editors: Markus Bläser and Benjamin Monmege; Article No. 11; pp. 11:1–11:17

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



Theorem 6.8], and Baumslag-Solitar groups $BS(p, q)$ for co-prime $p, q > 1$ [6, Theorem 2] and for $p = 1$ [21, Theorem 4.1]. Moreover, the class of groups where knapsack is decidable is closed under free products with amalgamation [19, Theorem 14] and HNN extensions [19, Theorem 13] over finite identified subgroups. On the other hand, there are nilpotent groups for which knapsack is undecidable [16, Theorem 6.5].

Wreath products. A prominent construction in group theory and semigroup theory is the wreath product $G \wr H$ of two groups G and H . Wreath products are important algorithmically, because the Magnus embedding theorem [22, Lemma] states that for any free group F of rank r and a normal subgroup N of F , one can find $F/[N, N]$ as a subgroup of $\mathbb{Z}^r \wr (F/N)$, where $[N, N]$ is the commutator subgroup of N . This has been used by several authors to obtain algorithms for groups of the form $F/[N, N]$, and in particular free solvable groups. Examples include the word problem (folklore, see [13]), the conjugacy problem [24, 28, 13, 25], the power problem [13], and the knapsack problem [7, 10].

For groups G and H , their wreath product $G \wr H$ can be roughly described as follows. An element of $G \wr H$ consists of (i) a labeling, which maps each element of H to an element of G and (ii) an element of H , called the *cursor*. Here, the labeling has finite support, meaning all but finitely many elements of H are mapped to the identity of G . Moreover, each element of $G \wr H$ can be written as a product of elements from G and from H . Multiplying an element $g \in G$ will multiply g to the label of the current cursor position. Multiplying an element $h \in H$ will move the cursor by multiplying h .

Understanding the knapsack problem for wreath products is challenging for two reasons. First, the path that the expression $g_1^{x_1} \cdots g_n^{x_n} g^{-1}$ takes through the group H can have complicated interactions with itself: The product can place elements of G at (an *a priori* unbounded number of) positions $h \in H$ that are later revisited. At the end of the path, each position of H must carry the identity of G so as to obtain $g_1^{x_1} \cdots g_k^{x_k} g^{-1} = 1$. The second reason is that the groups G and H play rather different roles: *A priori*, for each group G the class of all H with decidable $\text{KP}(G \wr H)$ could be different, resulting in a plethora of cases.

Decidability of the knapsack problem for wreath products has been studied by Ganardi, König, Lohrey, and Zetsche [10]. They focus on the case that H is knapsack-semilinear, which means that the solution sets of equations $g_1^{x_1} \cdots g_n^{x_n} = g$ are (effectively) semilinear. A set $S \subseteq \mathbb{N}^n$ is *semilinear* if it is a finite union of *linear* sets $\{u_0 + \lambda_1 u_1 + \cdots + \lambda_k u_k \mid \lambda_1, \dots, \lambda_k \in \mathbb{N}\}$ for some vectors $u_0, \dots, u_k \in \mathbb{N}^n$. Under this assumption, they show that $\text{KP}(G \wr H)$ is decidable if and only if solvability of systems of exponent equations is decidable for G [10, Theorem 5.3]. Here, an exponent equation is one of the form $g_1^{x_1} \cdots g_n^{x_n} = g$, where variables x_i are allowed to repeat. The problem of solvability of systems of exponent equations is denoted $\text{ExpEq}(G)$. Moreover, it is shown there that for some number $\ell \in \mathbb{N}$, knapsack is undecidable for $G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$, where $H_3(\mathbb{Z})$ denotes the discrete Heisenberg group and G is any non-trivial group [10, Theorem 5.2]. Since $\text{KP}(H_3(\mathbb{Z}) \times \mathbb{Z}^\ell)$ is decidable for any $\ell \geq 0$ [16, Theorem 6.8], this implies that wreath products do not preserve decidability of knapsack in general. However, apart from the latter undecidability result, little is known about wreath products $G \wr H$ where H is not knapsack-semilinear. As notable examples of this, knapsack is decidable for solvable Baumslag-Solitar groups $BS(1, q)$ [21, Theorem 4.1] and for the discrete Heisenberg group $H_3(\mathbb{Z})$ [16, Theorem 6.8], but it is not known for which G the knapsack problem is decidable for $G \wr H_3(\mathbb{Z})$ or for $G \wr BS(1, q)$.

The only other paper which studies the knapsack problem over wreath products is [7]. It is concerned with complexity results (for knapsack-semilinear groups) whereas in this paper we are concerned with decidability results.

Contribution. Our main result is a characterization of the groups G and H for which $\text{KP}(G \wr H)$ is decidable. Specifically, we introduce two problems, *intersection knapsack* $\text{KP}^\pm(H)$ and the variant *positive intersection knapsack* $\text{KP}^+(H)$ and show the following. Let G and H be finitely generated, with G non-trivial and H infinite. Then knapsack for $G \wr H$ is decidable if and only if $\text{ExpEq}(G)$ is decidable and either (i) G is abelian and $\text{KP}^+(H)$ is decidable or (ii) G is not abelian and $\text{KP}^\pm(H)$ is decidable. Note that the case of finite H is not interesting: For $|H| = m$, $\text{KP}(G \wr H)$ is equivalent to $\text{KP}(G^m)$ (see Section 3).

Thus, our result relieves us from considering every pair (G, H) of groups and allows us to study the factors separately. It is not hard to see that decidability of $\text{ExpEq}(G)$ is necessary for decidability of $\text{KP}(G \wr H)$ if H is infinite. It is surprising that the only other property of G that is relevant for decidability of $\text{KP}(G \wr H)$ is whether G is abelian or not. This is in contrast to the effect of other structural properties of G on the complexity of $\text{KP}(G \wr \mathbb{Z})$: If $G \neq 1$ is a finite nilpotent group, then $\text{KP}(G \wr \mathbb{Z})$ is NP-complete [7, Theorem 2], whereas for finite and non-solvable G , the problem $\text{KP}(G \wr \mathbb{Z})$ is Σ_2^p -complete [7, Corollary 25].

Applications. We also obtain two applications. First, we deduce that $\text{KP}(G \wr H_3(\mathbb{Z}))$ is undecidable for every $G \neq 1$. This implies that if $G \neq 1$ and H is virtually nilpotent and infinite, then $\text{KP}(G \wr H)$ is decidable if and only if H is virtually abelian and $\text{ExpEq}(G)$ is decidable. Moreover, we show that $\text{KP}(G \wr \text{BS}(1, q))$ is decidable if and only if $\text{ExpEq}(G)$ is.

Ingredients. For the “if” direction of our main result, we reduce $\text{KP}(G \wr H)$ to $\text{ExpEq}(G)$ and $\text{KP}^\pm(H)$ (respectively $\text{KP}^+(H)$) using extensions of techniques used by Figelius, Ganardi, Lohrey, and Zetsche [7]. Roughly speaking, the problem $\text{KP}^\pm(H)$ takes as input an expression $h_0 g_1^{x_1} h_1 \cdots g_n^{x_n} h_n$ and looks for numbers $x_1, \dots, x_n \geq 0$ such that the walk defined by the product $h_0 g_1^{x_1} h_1 \cdots g_n^{x_n} h_n$ meets specified constraints about self-intersections. Such a constraint can be either (i) a *loop constraint*, meaning the walk visits the same point after two specified factors or (ii) a *disjointness constraint* saying that the $(x_i + 1)$ -many points visited when multiplying $g_i^{x_i}$ do not intersect the $(x_j + 1)$ -many points visited while multiplying $g_j^{x_j}$.

The “only if” reductions in our main result involve substantially new ideas. The challenge is to guarantee that the constructed instances of $\text{KP}(G \wr H)$ will leave an element $\neq 1$ somewhere, as soon as any constraint is violated. In particular, the loop constraints have to be checked independently of the disjointness constraints. Moreover, if several constraints are violated, the resulting elements $\neq 1$ should not cancel each other. Furthermore, this has to be achieved despite almost no information on the structure of G and H . This requires an intricate construction that uses various patterns in the Cayley graph of H for which we show that only very specific arrangements permit cancellation. To this end, we introduce the notion of *periodic complexity*, which measures how many periodic sequences are needed to cancel out a sequence of elements of a group. Roughly speaking, for the loop constraints we use patterns of high periodic complexity, whereas for the disjointness constraints we use patterns with low periodic complexity but many large gaps. This ensures that the disjointness patterns cannot cancel the loop patterns or vice versa.

2 Preliminaries

Knapsack problems. For a group G and a subset $S \subseteq G$ we write S^* for the submonoid generated by S , i.e. the set of products of elements from S . Let G be a group with a finite (*monoid*) *generating set* $\Sigma \subseteq G$, i.e. $G = \Sigma^*$. Such groups are called *finitely generated*. An *exponent expression* over G is an expression $E = e_1 \dots e_n$ consisting of *atoms* e_i where each

atom e_i is either a *constant* $e_i = g_i \in G$ or a *power* $e_i = g_i^{x_i}$ for some $g_i \in G$ and variable x_i . Here the group elements g_i are given as words over Σ . We write $\gamma(e_i) = g_i$ for the constant or the base of the power. Furthermore let $P_E \subseteq [1, n]$ be the set of indices of the powers in E and $Q_E = [1, n] \setminus P_E$ be the set of indices of the constants in E . If $\nu \in \mathbb{N}^X$ is a valuation of the variables X that occur in E , then for each $i \in [1, n]$, we define $\nu(e_i) = \gamma(e_i)^{\nu(x_i)}$ if $i \in P_E$; and $\nu(e_i) = e_i$ if $i \in Q_E$. Moreover, $\nu(E) := \nu(e_1) \cdots \nu(e_n)$ and the set of G -solutions of E as $\text{sol}_G(E) := \{\nu \in \mathbb{N}^X \mid \nu(E) = 1\}$.

For a group G , the problem of *solvability of exponent equations* $\text{ExpEq}(G)$ is defined as:

Given a finite list of exponent expression E_1, \dots, E_k over G .

Question Is $\bigcap_{i=1}^k \text{sol}_G(E_i)$ non-empty?

An exponent expression is called a *knapsack expression* if all variables occur at most once. The *knapsack problem* $\text{KP}(G)$ over G is defined as follows:

Given a knapsack expression E over G .

Question Is there a valuation ν such that $\nu(E) = 1$?

The definition from [27] asks whether $g_1^{x_1} \cdots g_n^{x_n} = g$ has a solution for given $g_1, \dots, g_n, g \in G$. The two versions are inter-reducible in polynomial time [16, Proposition 7.1].

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 ${}^h f(a) = f(h^{-1}a)$, where $f \in G^{(H)}$ and $h, a \in H$. The corresponding semidirect product $G^{(H)} \rtimes H$ is the (restricted) *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 $(f_1, h_1)(f_2, h_2) = (f, h_1 h_2)$, where $f(a) = f_1(a) f_2(h_1^{-1}a)$.

There are canonical mappings $\sigma: G \wr H \rightarrow H$ with $\sigma(f, h) = h$ and $\tau: G \wr H \rightarrow G^{(H)}$ with $\tau(f, h) = f$ for $f \in G^{(H)}$, $h \in H$. In other words: $g = (\tau(g), \sigma(g))$ for $g \in G \wr H$. Note that σ is a homomorphism whereas τ is in general not a homomorphism. Throughout this paper, the letters σ and τ will have the above meaning (the groups G, H will be always clear from the context). We also define $\text{supp}(g) = \text{supp}(\tau(g))$ for all $g \in G \wr H$.

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 . We can compute the product $(f_1, h_1)(f_2, h_2)$ 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 $h_1 a \in H$. 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 $g_1 \in G$ and $g_2 \in G$ are sitting at $a \in H$ (i.e., $f_1(a) = g_1$ and $f'_2(a) = g_2$), then we put $g_1 g_2$ into the location a . The new distinguished H -element (the new cursor position) becomes $h_1 h_2$.

Clearly, H is a subgroup of $G \wr H$. We also regard G as a subgroup of $G \wr H$ by identifying G with the set of all $f \in G^{(H)}$ with $\text{supp}(f) \subseteq \{1\}$. This copy of G together with H generates $G \wr H$. In particular, if $G = \langle \Sigma \rangle$ and $H = \langle \Gamma \rangle$ with $\Sigma \cap \Gamma = \emptyset$ then $G \wr H$ is generated by $\Sigma \cup \Gamma$. With these embeddings, GH is the set of $(f, h) \in G \wr H$ with $\text{supp}(f) \subseteq \{1\}$ and $h \in H$.

Groups. Our applications will involve two well-known types of groups: the *discrete Heisenberg group* $H_3(\mathbb{Z})$, which consists of the matrices $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ with $a, b, c \in \mathbb{Z}$, and the *Baumslag-Solitar groups* [2] $\text{BS}(p, q)$ for $p, q \in \mathbb{N}$, where $\text{BS}(p, q) = \langle a, t \mid ta^pt^{-1} = a^q \rangle$.

A subgroup H of G is called *finite-index* if there are finitely many cosets gH . If $ab = ba$ for every $a, b \in G$, then G is *abelian*. A group has a property *virtually* if it has a finite-index subgroup H with that property. For example, a group is *virtually abelian* if it has a finite-index abelian subgroup. For two elements $a, b \in G$, we write $[a, b] = aba^{-1}b^{-1}$ and call this the *commutator* of a, b . If A, B are subgroups of G , then $[A, B]$ is the subgroup generated by all $[a, b]$ with $a \in A$ and $b \in B$. For $g, h \in G$, we write ${}^hg = hgh^{-1}$. In particular, if $g \in G$ and $h \in H$, then hg is the element $(f, 1) \in G \wr H$ with $f(h) = g$ and $f(h') = 1$ for $h' \neq h$.

3 Main results

We first introduce the new (positive) intersection knapsack problem. A solution to a knapsack expression E describes a walk in the Cayley graph that starts and ends in the group identity. Whereas the ordinary knapsack problem only asks for the expression to yield the identity, our extended version can impose constraints on how this walk intersects itself.

A *walk* over G is a nonempty sequence $\pi = (g_1, \dots, g_n)$ over G . Its support is $\text{supp}(\pi) = \{g_1, \dots, g_n\}$. It is a *loop* if $g_1 = g_n$. Two walks are *disjoint* if their supports are disjoint. We define a partial concatenation on walks: If $\pi = (g_1, \dots, g_n)$ and $\rho = (h_1, \dots, h_m)$ with $g_n = h_1$ then $\pi\rho = (g_1, \dots, g_n, h_2, \dots, h_m)$. A *progression* with period $h \in G$ over G is a walk of the form $\pi = (g, gh, gh^2, \dots, gh^\ell)$ for some $g \in G$ and $\ell \geq 0$. We also call the set $\text{supp}(\pi)$ a progression, whose period may not be unique. If $h \neq 1$ we also call π a *ray*.

A *factorized walk* is a walk π equipped with a *factorization* (π_1, \dots, π_n) , i.e. $\pi = \pi_1 \dots \pi_n$. One also defines the concatenation of factorized walks in the straightforward fashion. If $E = e_1 \dots e_n$ is an exponent expression and ν is a valuation over E we define the factorized walk $\pi_{\nu, E} = \pi_1 \dots \pi_n$ induced by ν on E where

$$\pi_i = \begin{cases} (\nu(e_1 \dots e_{i-1}) g_i^k)_{0 \leq k \leq \nu(x_i)}, & \text{if } e_i = g_i^{x_i} \\ (\nu(e_1 \dots e_{i-1}), \nu(e_1 \dots e_{i-1}) g_i), & \text{if } e_i = g_i. \end{cases}$$

The *intersection knapsack problem* $\text{KP}^\pm(G)$ over G is defined as follows:

Given a knapsack expression E over G , a set $L \subseteq [0, n]^2$ of loop constraints, and a set $D \subseteq [1, n]^2$ of disjointness constraints.

Question Is there a valuation ν such that $\nu(E) = 1$ and the factorized walk $\pi_{\nu, E} = \pi_1 \dots \pi_n$ induced by ν on E satisfies the following conditions:

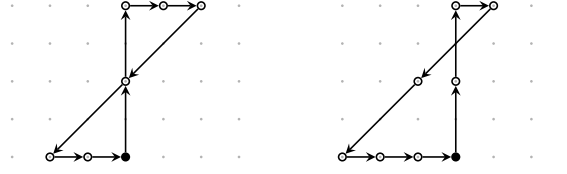
- $\pi_{i+1} \dots \pi_j$ is a loop for every $(i, j) \in L$
- π_i and π_j are disjoint for every $(i, j) \in D$.

The *positive intersection knapsack problem* $\text{KP}^+(G)$ over G is the restriction of $\text{KP}^\pm(G)$ to instances where $D = \emptyset$. We denote the set of solutions of a $\text{KP}^\pm(G)$ -instance (resp. $\text{KP}^+(G)$ -instance) (E, I, D) (resp. (E, I)) as $\text{sol}_G(E, I, D)$ (resp. $\text{sol}_G(E, I)$). Figure 1 shows an example for the intersection knapsack problem over \mathbb{Z}^2 .

The following is our main result.

► **Theorem 3.1.** *Let G and H be f.g. groups such that G is non-trivial and H is infinite. Then $\text{KP}(G \wr H)$ is decidable if and only if $\text{ExpEq}(G)$ is decidable and either*

1. G is abelian and $\text{KP}^+(H)$ is decidable or
2. G is not abelian and $\text{KP}^\pm(H)$ is decidable.



■ **Figure 1** Consider the knapsack equation $g_1^{x_1} g_2^{x_2} g_3^{x_3} g_4^{x_4} = 1$ over \mathbb{Z}^2 written multiplicatively, where $g_1 = (0, 2)$, $g_2 = (1, 0)$, $g_3 = (-2, -2)$ and $g_4 = (1, 0)$ and the disjointness condition $D = \{(1, 3)\}$. The solid dot represents the origin $(0, 0)$. The knapsack equation is satisfied by $(x_1, x_2, x_3, x_4) = (2, 2, 2, 2)$ but it violates D , as illustrated on the left. On the right the solution $(x_1, x_2, x_3, x_4) = (2, 1, 2, 3)$ is depicted, which satisfies D .

Here, we assume H to be infinite, because the case of finite H is not interesting: If $|H| = m$, then $G \wr H$ has G^m as a finite-index subgroup [18, Proposition 1], meaning $\text{KP}(G \wr H)$ is decidable if and only if $\text{KP}(G^m)$ is [16, Theorem 7.3].

If H is knapsack-semilinear, it is easy to see that both $\text{KP}^+(H)$ and $\text{KP}^\pm(H)$ are decidable via an encoding in Presburger arithmetic. Hence, the main decidability result of [10], saying that for knapsack-semilinear H , $\text{KP}(G \wr H)$ is decidable if and only if $\text{ExpEq}(G)$ is decidable, is generalized by Theorem 3.1.

Logical version of KP^+ and KP^\pm . For our applications of Theorem 3.1, it is often convenient to use a formulation of $\text{KP}^+(G)$ and $\text{KP}^\pm(G)$ in terms of logics over an extended Cayley graph of G . The *Cayley graph of G* is the logical structure $\mathcal{C}(G) = (G, (\xrightarrow{g})_{g \in G})$, with domain G and with the relation \xrightarrow{g} for each¹ $g \in G$, where $g_1 \xrightarrow{g} g_2$ if and only if $g_1 g = g_2$. We define the extension $\mathcal{C}^+(G) = (G, (\xrightarrow{g})_{g \in G}, (\xrightarrow{g^*})_{g \in G})$ where $\xrightarrow{g^*}$ is the reflexive transitive closure of \xrightarrow{g} . Finally, we define a further extension $\mathcal{C}^\pm(G) = (G, (\xrightarrow{g})_{g \in G}, (\xrightarrow{g^*})_{g \in G}, (\perp_{g,h})_{g,h \in G})$ with *disjointness relations* $\perp_{g,h}$, which are binary relations on pairs G^2 : For any $g, h \in G$ and $(g_1, g_2), (h_1, h_2) \in G^2$ we have that $(g_1, g_2) \perp_{g,h} (h_1, h_2)$ if and only if for some $k, \ell \in \mathbb{N}$, we have $g_1 g^k = g_2$, $h_1 h^\ell = h_2$, and the walks $(g_1, g_1 g, \dots, g_1 g^k)$ and $(h_1, h_1 h, \dots, h_1 h^\ell)$ are disjoint. We denote by \mathcal{F}^\pm the set of positive existential first-order formulas over $\mathcal{C}^\pm(G)$, i.e. formulas $\exists y_1 \dots \exists y_m \varphi(y_1, \dots, y_m)$ where $\varphi(y_1, \dots, y_m)$ is a positive Boolean combination of atomic formulas. Then $\text{SAT}^\pm(G)$ is the decision problem that asks if a closed formula in \mathcal{F}^\pm holds in $\mathcal{C}^\pm(G)$. The fragment \mathcal{F}^+ and the problem $\text{SAT}^+(G)$ are defined similarly. Clearly, $\text{KP}^\pm(G)$ (resp. $\text{KP}^+(G)$) reduces to $\text{SAT}^\pm(G)$ (resp. $\text{SAT}^+(G)$). In the full version [5], we show:

▶ **Theorem 3.2.** *For any finitely generated group G , the problem $\text{SAT}^\pm(G)$ (resp. $\text{SAT}^+(G)$) is decidable if and only if $\text{KP}^\pm(G)$ (resp. $\text{KP}^+(G)$) is decidable.*

Virtually nilpotent groups. It was shown by Ganardi, König, Lohrey, and Zetsche that for some number $\ell \in \mathbb{N}$ and all groups $G \neq 1$, $\text{KP}(G \wr (H_3(\mathbb{Z}) \times \mathbb{Z}^\ell))$ is undecidable [10, Theorem 5.2], but essentially nothing is known so far about the groups G for which the problem $\text{KP}(G \wr H_3(\mathbb{Z}))$ is decidable. Using Theorem 3.1, this can be settled.

▶ **Theorem 3.3.** *For every non-trivial G , the problem $\text{KP}(G \wr H_3(\mathbb{Z}))$ is undecidable.*

¹ Customarily, one only includes the edge relations $(\xrightarrow{s})_{s \in S}$ for some finite generating set S of G . We choose $S = G$ to make the presentation in the following cleaner.

This is in contrast to decidability of $\text{KP}(H_3(\mathbb{Z}))$ [16, Theorem 6.8]. We show Theorem 3.3 by proving in Section 6 that $\text{SAT}^+(H_3(\mathbb{Z}))$ (and thus $\text{KP}^+(H_3(\mathbb{Z}))$) is undecidable.

The interest in the Heisenberg group stems from its special role inside the class of virtually nilpotent groups. This class, in turn, consists exactly of the finite extensions of groups of unitriangular integer matrices (see, for example, [14, Theorem 17.2.5]). Furthermore, a celebrated result of Gromov [12] states that the f.g. virtually nilpotent groups are precisely the f.g. groups with polynomial growth. In some sense, the discrete Heisenberg group is the smallest f.g. virtually nilpotent group that is not virtually abelian. Therefore, Theorem 3.3 implies the following characterization of all wreath products $G \wr H$ with decidable $\text{KP}(G \wr H)$ where H is infinite and virtually nilpotent. See the full version [5] for details.

► **Corollary 3.4.** *Let G, H be f.g. non-trivial groups. If H is virtually nilpotent and infinite, then $\text{KP}(G \wr H)$ is decidable if and only if H is virtually abelian and $\text{ExpEq}(G)$ is decidable.*

By undecidability of $\text{ExpEq}(H_3(\mathbb{Z}))$, this implies: If $G \neq 1$ and H are f.g. virtually nilpotent and H is infinite, then $\text{KP}(G \wr H)$ is decidable if and only if G and H are virtually abelian.

Solvable Baumslag-Solitar groups. Our second application of Theorem 3.1 concerns wreath products $G \wr \text{BS}(1, q)$. It is known that knapsack is decidable for $\text{BS}(1, q)$ [21, Theorem 4.1], but again, essentially nothing is known about $\text{KP}(G \wr \text{BS}(1, q))$ for any G .

► **Theorem 3.5.** *For any f.g. group G and $q \geq 1$, the problem $\text{KP}(G \wr \text{BS}(1, q))$ is decidable if and only if $\text{ExpEq}(G)$ is decidable.*

Extending methods from Lohrey and Zetsche [21], we show that $\text{KP}^\pm(\text{BS}(1, q))$ is decidable for any $q \geq 1$ and thus obtain Theorem 3.5 in Section 6.

Magnus embedding. Another corollary concerns groups of the form $F/[N, N]$, where F is a f.g. free group and N is a normal subgroup. Recall that any f.g. group can be written as F/N , where F is an f.g. free group and N is a normal subgroup of F . Dividing by $[N, N]$ instead of N yields $F/[N, N]$, which is subject to the Magnus embedding [22, Lemma] of $F/[N, N]$ into $\mathbb{Z}^r \wr (F/N)$, where r is the rank of F . We show in the full version [5]:

► **Corollary 3.6.** *Let F be a finitely generated free group and N be a normal subgroup of F . If $\text{KP}^+(F/N)$ is decidable, then so is $\text{KP}(F/[N, N])$.*

Knapsack vs. intersection knapsack. Introducing the problems KP^+ and KP^\pm raises the question of whether they are substantially different from the similar problems KP and ExpEq : Is $\text{KP}^+(G)$ or $\text{KP}^\pm(G)$ perhaps inter-reducible with $\text{KP}(G)$ or $\text{ExpEq}(G)$? Our applications show that this is not the case. Since $\text{KP}(H_3(\mathbb{Z}))$ is decidable [16, Theorem 6.8], but $\text{KP}^+(H_3(\mathbb{Z}))$ is not, neither $\text{KP}^+(G)$ nor $\text{KP}^\pm(G)$ can be inter-reducible with $\text{KP}(G)$ in general. Moreover, one can show² that $\text{ExpEq}(\text{BS}(1, 2))$ is undecidable [11], whereas $\text{KP}^\pm(\text{BS}(1, q))$ is decidable for any $q \geq 1$. Hence, neither $\text{KP}^+(G)$ nor $\text{KP}^\pm(G)$ can be inter-reducible with $\text{ExpEq}(G)$ in general. However, we leave open whether there is a f.g. group G for which $\text{KP}^+(G)$ is decidable, but $\text{KP}^\pm(G)$ is undecidable (see Section 7).

² Since there is no published proof available, we include a proof in the full version [5], with kind permission of Moses Ganardi and Markus Lohrey.

4 From wreath products to intersection knapsack

In this section, we prove the “if” direction of Theorem 3.1 by deciding $\text{KP}(G \wr H)$ using $\text{ExpEq}(G)$ and either $\text{KP}^\pm(H)$ or $\text{KP}^+(H)$ (depending on whether G is abelian).

Normalization. We fix a wreath product $G \wr H$ with G and H finitely generated groups. Note that we may assume that $\text{KP}(H)$ is decidable. In our reduction, we will augment the $\text{KP}(G \wr H)$ -instance with positive intersection constraints regarding the cursor in H . This results in instances of the *hybrid intersection knapsack problem* $\text{HKP}^\pm(G \wr H)$ over $G \wr H$: It is defined as $\text{KP}^\pm(G \wr H)$ but the loop and disjointness constraints consider the σ -image of elements. Let us make this more precise. If $E = \alpha_1 \cdots \alpha_n$ is a knapsack expression over $G \wr H$, then we define for all $i \in [1, n]$ and $\nu \in \mathbb{N}^X$ the set

$$\text{supp}_E^\nu(i) := \{\sigma(\nu(\alpha_1 \cdots \alpha_{i-1})\gamma(\alpha_i)^k) \mid 0 \leq k \leq \nu(x_i) - 1\}$$

if $i \in P_E$ and

$$\text{supp}_E^\nu(i) := \{\sigma(\nu(\alpha_1 \cdots \alpha_{i-1}))\}$$

if $i \in Q_E$. For a walk $w = (w_1, \dots, w_k)$ over $G \wr H$ we write $\sigma(w) := (\sigma(w_1), \dots, \sigma(w_k))$. Then the *hybrid intersection knapsack problem* $\text{HKP}^\pm(G \wr H)$ over $G \wr H$ is defined as follows:

Given a knapsack expression E over G , a set $L \subseteq [0, n]^2$ of loop constraints, and a set $D \subseteq [1, n]^2$ of disjointness constraints.

Question Is there a valuation $\nu \in \mathbb{N}^X$ with factorized walk $\pi_{\nu, E} = \pi_1 \dots \pi_n$ induced by ν on E such that the following conditions are fulfilled:

- $\nu(E) = 1$
- $\sigma(\pi_{i+1} \dots \pi_j)$ is a loop for all $(i, j) \in L$
- $\text{supp}_E^\nu(i) \cap \text{supp}_E^\nu(j) = \emptyset$ for all $(i, j) \in D$.

Its *positive* version $\text{HKP}^+(G \wr H)$ is again defined by having no disjointness constraints. The set $\text{sol}_{G \wr H}$ is defined accordingly. Note that to simplify the constructions in the proofs, the disjointness constraints in an $\text{HKP}^\pm(G \wr H)$ -instance disregard the last point of walks.

In the following, when we write a knapsack expression as $E = \alpha_1 \cdots \alpha_n \alpha_{n+1}$, we assume w.l.o.g. that α_{n+1} is a constant. Two elements $g, h \in H$ are called *commensurable* if $g^x = h^y$ for some $x, y \in \mathbb{Z} \setminus \{0\}$. It is known that if g_1, g_2 have infinite order and are not commensurable, then there is at most one solution $(x_1, x_2) \in \mathbb{Z}^2$ for the equations $g_1^{x_1} g_2^{x_2} = g$ [7, Lemma 9].

Let $E = \alpha_1 \cdots \alpha_n \alpha_{n+1}$ be a knapsack expression and write $g_i = \gamma(\alpha_i)$ for $i \in [1, n+1]$. The expression (resp. the corresponding $\text{HKP}^\pm(G \wr H)$ -instance) is *c-simplified* if for any $i, j \in P_E$ with $g_i \notin H$ and $g_j \notin H$, we have that commensurability of $\sigma(g_i)$ and $\sigma(g_j)$ implies $\sigma(g_i) = \sigma(g_j)$. We call the expression (resp. the corresponding $\text{HKP}^\pm(G \wr H)$ -instance) *normalized* if it is c-simplified and each atom α_i with $i \in [1, n]$ is of one of the following types: We either have (a) $i \in Q_E$ and $g_i \in H$ or (b) $i \in P_E$ and $\sigma(g_i) = 1$ or (c) $i \in P_E$, $g_i \in GH$ and $\sigma(g_i)$ has infinite order. Using generalizations of ideas from [10] and [7], we show:

► **Theorem 4.1.** *Given an instance of $\text{KP}(G \wr H)$, one can effectively construct an equivalent finite set of normalized $\text{HKP}^+(G \wr H)$ -instances.*

Here, a problem instance I is *equivalent* to a set \mathcal{I} of problem instances if I has a solution if and only if at least one of the instances in \mathcal{I} has a solution.

Non-abelian case. Note that in a normalized knapsack expression, atoms of type (b) and (c) and the last atom α_{n+1} may place non-trivial elements of G . Our next step is to transform the input instance further so that only the atoms of type (c) can place non-trivial elements of G , which leads to the notion of stacking-freeness.

Let $E = \alpha_1 \cdots \alpha_n \alpha_{n+1}$ be a knapsack expression over $G \wr H$ and let $g_i := \gamma(\alpha_i)$ for all $i \in [1, n+1]$. We call an index $i \in [1, n+1]$ *stacking* if either $i \in P_E$ and $\sigma(g_i) = 1$, or $i = n+1$ and $g_{n+1} \notin H$. We say that E is *stacking-free* if it has no stacking indices. Thus, a normalized expression E is stacking-free if each atom is either of type (c) or a constant in H .

► **Lemma 4.2.** *Given a normalized $\text{HKP}^\pm(G \wr H)$ -instance, one can effectively construct an equivalent finite set of stacking-free, normalized $\text{HKP}^\pm(G \wr H)$ -instances.*

Let us sketch the proof of Lemma 4.2. We use the notion of an address from [10]. An *address* of E is a pair (i, h) with $i \in [1, n+1]$ and $h \in H$ such that $h \in \text{supp}(\gamma(\alpha_i))$. The set of addresses A_E of E is finite and can be computed. Intuitively, an address represents a position in a knapsack expression where a point in H can be visited.

Intuitively, instead of placing elements of G by atoms of type (b) and by α_{n+1} , we introduce loop and disjointness constraints guaranteeing that in points visited by these atoms, a solution would have placed elements that multiply to $1 \in G$. To this end, we pick an address $(i, h) \in A$ of a stacking index i and then guess a set $C \subseteq A$ of addresses such that the point $h' \in H$ visited at (i, h) is visited by exactly the addresses in C . The latter condition is formulated using loop and disjointness constraints in an $\text{HKP}^\pm(G \wr H)$ -instance I_C . In I_C , we do not place elements at C anymore; instead, we construct a set S_C of exponent equations over G that express that indeed the point h' carries $1 \in G$ in the end. Note that this eliminates one address with stacking index. We repeat this until we are left with a set of stacking-free instances of $\text{HKP}^\pm(G \wr H)$, each together with an accumulated set of exponent equations over G . We then take the subset \mathcal{I} of $\text{HKP}^\pm(G \wr H)$ -instances whose associated $\text{ExpEq}(G)$ -instance has a solution. This will be our set for Lemma 4.2.

The last step of the non-abelian case is to construct $\text{KP}^\pm(H)$ -instances.

► **Lemma 4.3.** *Given a stacking-free, normalized $\text{HKP}^\pm(G \wr H)$ -instance, one can effectively construct an equivalent finite set of $\text{KP}^\pm(H)$ -instances.*

We are given an instance (E, L, D) with $E = \alpha_1 \cdots \alpha_n$ and write $g_i = \gamma(\alpha_i)$ for $i \in [1, n]$. As (E, L, D) is normalized and stacking-free, only atoms of type (c) with $g_i \notin H$ can place non-trivial elements of G . Moreover, if α_i and α_j are such atoms, then the elements $\sigma(g_i)$ and $\sigma(g_j)$ are either non-commensurable or equal. In the first case, the two rays produced by α_i and α_j can intersect in at most one point; in the second case, they intersect along subrays corresponding to intervals $I_i \subseteq [0, \nu(x_i)]$ and $I_j \subseteq [0, \nu(x_j)]$.

Thus, the idea is to split up each ray wherever the intersection with another ray starts or ends: We guess for each ray as above the number $m \leq 2 \cdot |A_E| - 1$ of subrays it will be split into and replace $g_i^{x_i}$ with $g_i^{y_1} \cdots g_i^{y_m}$. After the splitting, subrays are either equal or disjoint. We guess an equivalence relation on the subrays; using loop constraints, we ensure that subrays in the same class are equal; using disjointness constraints, we ensure disjointness of subrays in distinct classes. Finally, we have to check that for each equivalence class C , the element of G produced by the rays in C does indeed multiply to $1 \in G$. This can be checked because $\text{ExpEq}(G)$ (and thus the word problem for G) is decidable.

Abelian case. We now come to the case of abelian G : We show that $\text{KP}(G \wr H)$ is decidable, but only using instances of $\text{KP}^+(H)$ instead of $\text{KP}^\pm(H)$. Here, the key insight is that we can use the same reduction, except that we just do not impose the disjointness constraints. In

the above reduction, we use disjointness constraints to control exactly which positions in our walk visit the same point in H . Then we can check that in the end, each point in H carries $1 \in G$. However, if G is abelian, it suffices to make sure that the set of positions in our walk decomposes into subsets, each of which produces $1 \in G$: If several of these subsets do visit the same point in H , the end result will still be $1 \in G$.

We illustrate this in a slightly simpler setting. Suppose we have a product $g = h_1 a_1 \dots h_n a_n$ with $h_1, \dots, h_n \in H$ and $a_1, \dots, a_n \in G$. Then g is obtained by placing a_1 at $h_1 \in H$, then a_2 at $h_2 \in H$, etc. For a subset $S = \{s_1, \dots, s_k\} \subseteq [1, n]$ with $s_1 < \dots < s_k$, we define $g_S = h_{s_1} a_{s_1} \dots h_{s_k} a_{s_k}$. Hence, we only multiply those factors from S . An equivalence relation \equiv on $[1, n]$ is called *cancelling* if $g_C = 1$ for every class C of \equiv . Moreover, \equiv is called *equilocal* if $i \equiv j$ if and only if $h_i = h_j$. It is called *weakly equilocal* if $i \equiv j$ implies $h_i = h_j$. Now observe that for any G , we have $g = 1$ if and only if there is an equilocal cancelling equivalence on $[1, n]$. However, if G is abelian, then $g = 1$ if and only if there is a *weakly equilocal* equivalence on $[1, n]$. Since weak equilocality can be expressed using only equalities (and no disequalities), it suffices to impose loop conditions in our instances.

Comparison to previous approach in [7]. The reduction from $\text{KP}(G \wr H)$ to $\text{ExpEq}(G)$ and $\text{KP}^\pm(H)$ ($\text{KP}^+(H)$ respectively) uses similar ideas as the proof of [7, Theorem 4], where it is shown $\text{ExpEq}(K)$ is in NP if K is an iterated wreath product of \mathbb{Z}^r for some $r \in \mathbb{N}$.

Let us compare our reduction with the proof of [7, Theorem 4]. In [7], one solves $\text{ExpEq}(K)$ by writing $K = G \wr H$ where G is abelian and H is orderable and knapsack-semilinear. In both proofs, solvability of an instance (of $\text{ExpEq}(G \wr H)$ in [7] and $\text{KP}(G \wr H)$ here) is translated into a set of conditions by using similar decomposition arguments. Then, the two proofs differ in how satisfiability of these conditions is checked.

In [7], this set of conditions is expressed in Presburger arithmetic, which is possible due to knapsack-semilinearity of H . In our reduction, we have to translate the conditions in $\text{ExpEq}(G)$ and $\text{KP}^+(H)$ ($\text{KP}^\pm(H)$) instances. Here, we use loop constraints where in Presburger arithmetic, one can compare variables directly. Moreover, our reduction uses disjointness constraints to express solvability in the case that G is non-abelian. This case does not occur in [7, Theorem 4]. Finally, we have to check whether the elements from G written at the same point of H multiply to 1. The reduction of [7] can express this directly in Presburger arithmetic since G is abelian. Here, we use instances of $\text{ExpEq}(G)$.

5 From intersection knapsack to wreath products

In this section, we prove the “only if” direction of Theorem 3.1. Since it is known that for infinite H , decidability of $\text{KP}(G \wr H)$ implies decidability of $\text{ExpEq}(G)$ [10, Proposition. 3.1, Proposition 5.1], it remains to reduce (i) $\text{KP}^+(H)$ to $\text{KP}(G \wr H)$ for any group $G \neq 1$, and (ii) $\text{KP}^\pm(H)$ to $\text{KP}(G \wr H)$ for any non-abelian group G . In the following, let G be a non-trivial group and H be any group and suppose $\text{KP}(G \wr H)$ is decidable.

First let us illustrate how to reduce $\text{KP}^+(H)$ to $\text{KP}(G \wr H)$. Suppose we want to verify whether a product $h_1 \dots h_m = 1$ over H satisfies a set of loop constraints $L \subseteq [0, m]^2$, i.e. $h_{i+1} \dots h_j = 1$ for all $(i, j) \in L$. To do so we insert into the product for each $(i, j) \in L$ a function $f \in G^{(H)}$ after the element h_i and its inverse f^{-1} after the element h_j . We call these functions *loop words* since their supports are contained in a cyclic subgroup $\langle t \rangle$ of H . We can choose the loop words such that this modified product evaluates to 1 if and only if the loop constraints are satisfied. For the reduction from $\text{KP}^\pm(H)$ we need to make the construction more robust since we simultaneously need to simulate disjointness constraints.

If H is a torsion group then $\text{KP}^+(H)$ and $\text{KP}^\pm(H)$ are decidable if the word problem of H is decidable: For each exponent, we only have to check finitely many candidates. Since $\text{KP}(G \wr H)$ is decidable, we know that $\text{KP}(H)$ is decidable and hence also the word problem. Thus, we assume H not to be a torsion group and may fix an element $t \in H$ of infinite order.

Periodic complexity. Let K be a group. The following definitions will be employed with $K = \mathbb{Z}$ or $K = H$. For any subset $D \subseteq K$, let $G^{(D)}$ be the group of all functions $u: K \rightarrow G$ whose support $\text{supp}(u) = \{h \in K \mid u(h) \neq 1\}$ is finite and contained in D . A function $f \in G^{(K)}$ is *basic periodic* if there exists a progression D in K and $c \in G$ such that $f(h) = c$ for all $h \in D$ and $f(h) = 1$ otherwise. The *value* of such a function f is the element c ; a *period* of f is a period of its support. We will identify a word $u = c_1 \dots c_n \in G^*$ with the function $u \in G^{(\mathbb{Z})}$ where $u(i) = c_i$ for $i \in [1, n]$ and $u(i) = 1$ otherwise. Recall that for $u \in G^{(\mathbb{Z})}$ and $s \in \mathbb{Z}$, we have ${}^s u(n) = u(n - s)$. We extend this to $s \in \mathbb{Z}_\infty := \mathbb{Z} \cup \{\infty\}$ by setting ${}^\infty u(n) = 1$ for all $n \in \mathbb{Z}$. The *periodic complexity* of $u \in G^{(\mathbb{Z})}$ is the minimal number $\text{pc}(u) = k$ of basic periodic functions u_1, \dots, u_k such that $u = \prod_{i=1}^k u_i$. Given a progression $D = \{p + qn \mid n \in [0, \ell]\}$ in \mathbb{Z} and a function $u \in G^{(\mathbb{Z})}$ we define $\pi_D(u)(n) = u(p + qn)$ for all $n \in \mathbb{Z}$ and say that $\pi_D(u)$ is a *periodic subsequence* of u . Note that periodic subsequences of basic periodic functions are again basic periodic. Furthermore, since $\pi_D: G^{(\mathbb{Z})} \rightarrow G^{(\mathbb{Z})}$ is a homomorphism, taking periodic subsequences does not increase the periodic complexity.

► **Lemma 5.1.** *Given $n, k \in \mathbb{N}$ and $a \in G \setminus \{1\}$, one can compute $u_1, \dots, u_n \in \langle a \rangle^{(\mathbb{N})}$ such that $\prod_{i=1}^n {}^{p_i} u_i {}^{q_i} u_i^{-1}$ has periodic complexity $\geq k$ for all $(p_1, \dots, p_n) \neq (q_1, \dots, q_n) \in \mathbb{Z}_\infty^n$.*

Here is a proof sketch for Lemma 5.1. First we construct a word with large periodic complexity: In the full version [5] we prove that $(a)^{2^{2^k}} (1)^{2^{2^k}} \dots (a)^{2^{2^k}} (1)^{2^{2^k}}$, consisting of $4k$ many blocks, has periodic complexity at least k , where $(b)^n$ is the sequence consisting of n many b 's. The case $n = 1$ can be shown by taking such a sequence $v = a_1 \dots a_m \in \langle a \rangle^{(\mathbb{N})}$ with large periodic complexity and defining $u_1 = a_1 (1)^{m-1} a_2 (1)^{m-1} \dots a_m (1)^{m-1} a_1 \dots a_m$. If $p, q \in \mathbb{Z}_\infty$ are distinct then ${}^p u_1 {}^q u_1^{-1}$ always contains v or v^{-1} as a periodic subsequence and thus has large periodic complexity. For $n > 1$ we define u_i ($i > 1$) to be stretched versions of u_1 such that the supports of any two functions ${}^p u_i, {}^q u_j$ where $i \neq j$ intersect in at most one point. This allows to argue that $\prod_{i=1}^n {}^{p_i} u_i {}^{q_i} u_i^{-1}$ still has large periodic complexity as soon as $p_i \neq q_i$ for some i .

Expressing loop constraints. We now show how to use Lemma 5.1 to encode loop constraints over a product $h_1 \dots h_m$ over H in an instance of $\text{KP}(G \wr H)$.

Recall that a loop constraint (i, j) stipulates that $\sigma(g_{i+1} \dots g_j) = 1$. If we only want to reduce $\text{KP}^+(H)$, it is not hard to see that it would suffice to guarantee $\prod_{i=1}^n {}^{p_i} u_i {}^{q_i} u_i^{-1} \neq 1$ in Lemma 5.1. In that case, we could essentially use the functions u_i as loop words. However, in order to express disjointness constraints in $\text{KP}^\pm(H)$, we will construct expressions over $G \wr H$ that place additional “disjointness patterns” in the Cayley graph of H . We shall make sure that the disjointness patterns are tame: Roughly speaking, this means they are basic periodic and either (i) place elements from a fixed subgroup $\langle a \rangle$ or (ii) can intersect a loop word at most once. Here, the high periodic complexity of $\prod_{i=1}^n {}^{p_i} u_i {}^{q_i} u_i^{-1}$ will allow us to conclude that tame patterns cannot make up for a violated loop constraint.

Let us make this precise. Recall that two elements $g, h \in H$ are called *commensurable* if $g^x = h^y$ for some $x, y \in \mathbb{Z} \setminus \{0\}$. Let $a \in G \setminus \{1\}$. Let $\text{P}_{a,t}(G \wr H)$ be the set of elements $g \in G \wr H$ such that $\tau(g)$ is basic periodic and either, (i) its value belongs to $\langle a \rangle$, or (ii) its period is not commensurable to t . In particular, a power $(ch)^k$ (where $c \in G, h \in H, k \in \mathbb{N}$)

11:12 A Characterization of Wreath Products Where Knapsack Is Decidable

belongs to $P_{a,t}(G \wr H)$ if $c \in \langle a \rangle$ or h is not commensurable to t . Note that since loop words are always placed along the direction t , this guarantees tameness: In case (ii), the period of $\tau(g)$ being non-commensurable to t implies that the support of any $h'g, h' \in H$, can intersect the support of a loop word in $\langle a \rangle^{\langle t \rangle}$ at most once. Using Lemma 5.1, we show the following.

► **Lemma 5.2.** *Given $a \in G \setminus \{1\}$, $m \in \mathbb{N}$ and $L \subseteq [0, m]^2$ we can compute $f_0, \dots, f_m \in \langle a \rangle^{\langle t^* \rangle}$ such that:*

1. *Let $h_1, \dots, h_m \in H$. Then $h_1 \dots h_m = 1$ and $h_{i+1} \dots h_j = 1$ for all $(i, j) \in L$ if and only if $f_0 h_1 f_1 \dots h_m f_m = 1$.*
2. *Let $g_1, \dots, g_m \in P_{a,t}(G \wr H)$ such that $\sigma(g_{i+1} \dots g_j) \neq 1$ for some $(i, j) \in L$. Then $f_0 g_1 f_1 \dots g_m f_m \neq 1$.*

Observe that the first constraint says that if we only use the loop words f_i , then they allow us to express loop constraints. The second constraint tells us that a violated loop constraint cannot be compensated even with perturbations g_1, \dots, g_m , provided that they are tame.

The abelian case. Lemma 5.2 provides a simple reduction from $KP^+(H)$ to $KP(G \wr H)$. Given an instance $(E = e_1 \dots e_n, L)$ of $KP^+(H)$ we compute $f_0, \dots, f_m \in \langle a \rangle^{\langle t^* \rangle}$ using Lemma 5.2. Then $\nu: X \rightarrow \mathbb{N}$ satisfies $\nu(E) = 1$ and $\nu(e_{i+1} \dots e_j)$ for all $(i, j) \in L$ if and only if $\nu(f_0 e_1 f_1 \dots e_n f_n) = 1$. Hence (E, L) has a solution if and only if $\nu(f_0 e_1 f_1 \dots e_n f_n) = 1$ does.

The non-abelian case. Now let G be a non-abelian group. In the following we will reduce $KP^\pm(H)$ to $KP(G \wr H)$. The first step is to construct from an $KP^\pm(H)$ -instance I an equivalent $HKP^+(G \wr H)$ -instance \hat{I} using a nontrivial commutator $[a, b] \neq 1$ in G . In a second step we apply the “loop words”-construction from Lemma 5.2 (point 2) to \hat{I} , going to a (pure) knapsack instance. It guarantees that, if a loop constraint is violated, then the knapsack instance does not evaluate to 1. Furthermore, if a disjointness constraint is violated then there exists a large number of pairwise distant points in the Cayley graph of H which are labeled by a nontrivial element. These points cannot be canceled by the functions f_i from Lemma 5.2. Finally, if all loop and disjointness constraints are satisfied then the induced walk in the Cayley graph provides enough “empty space” such that the loop words can be shifted to be disjoint from the original walk induced by \hat{I} (encoding the disjointness constraints).

Normalization. Let $I = (E = e_1 \dots e_n, L, D)$ be a $KP^\pm(H)$ -instance where e_i is either a constant $e_i = h_i$ or a power $e_i = h_i^{x_i}$. We will start by establishing the following useful properties. We call I *torsion-free* if h_i has infinite order for all $i \in P_E$. Call I *orthogonalized* for all $(i, j) \in D \cap P_E^2$ such that we have $\langle h_i \rangle \cap \langle h_j \rangle = \{1\}$. If I is torsion-free and orthogonalized then it is called *normalized*. The orthogonality will be crucial for the tameness of the disjointness patterns since at most one of the elements h_i, h_j for $(i, j) \in D \cap P_E^2$ is commensurable to t . Furthermore, it guarantees that there is at most one intersection point for any pair $(i, j) \in D$.

► **Lemma 5.3.** *One can compute a finite set \mathcal{I} of normalized instances of $KP^\pm(H)$ such that I has a solution if and only if there exists $I' \in \mathcal{I}$ which has a solution.*

Here, torsion-freeness is easily achieved: If h_i has finite order, then $h_i^{x_i}$ can only assume finitely many values, so we replace $h_i^{x_i}$ by one of finitely many constants. Orthogonality requires an observation: If $\langle h_i \rangle \cap \langle h_j \rangle \neq \{1\}$, then any two intersecting progressions π_i, π_j

with periods h_i and h_j , respectively, must intersect periodically, meaning there exists an intersection point that is close to an endpoint of π_i or π_j . This means, in lieu of $(i, j) \in D$, we can require disjointness of one power with a constant.

Expressing disjointness constraints. Hence we can assume that I is normalized. To express disjointness constraints, we must assume that G is non-abelian. Let $a, b \in G$ with $aba^{-1}b^{-1} = [a, b] \neq 1$. Our starting point is the following idea. To express that two progressions π_i and π_j , induced by a valuation of E , are disjoint, we construct an expression over $G \wr H$ that first places a at each point in π_i , then b at each point in π_j , then again a^{-1} at each point in π_i , and finally b^{-1} at each point in π_j , see (2). Here we need loop constraints that express that the start and endpoints of the two traversals of π_i (and π_j) coincide. Then, if π_i and π_j are disjoint, the effect will be neutral; otherwise any intersection point will carry $aba^{-1}b^{-1} \neq 1$.

However, this leads to two problems. First, there might be more than one disjointness constraint: If k disjointness constraints are violated by the same point $h'' \in H$, then h'' would carry $[a, b]^k$, which can be the identity (for example, G may be finite). Second, when we also place loop words (which multiply elements from $\langle a \rangle$), those could also interfere with the commutator (for example, instead of $aba^{-1}b^{-1}$, we might get $aba^{-1}(a)b^{-1}(a^{-1}) = 1$).

Instead, we do the following. Let $t \in H$ be the element of infinite order used for the loop words. Moreover, let $D = \{(i_1, j_1), \dots, (i_d, j_d)\}$. For each $(i_k, j_k) \in D$, instead of performing the above “commutator construction” once, we perform it $n + d$ times, each time shifted by $t^{N_k} \in H$ for some large N_k . The numbers $N_0 < N_1 < \dots$ are chosen so large that for at least one commutator, there will be no interference from other commutators or from loop words.

Let us make this precise. Since I is orthogonalized, we may assume that for each $(i, j) \in D \cap P_E^2$, the elements h_j and t are not commensurable; otherwise we swap i and j . The resulting HKP $^+(G \wr H)$ -instance \hat{I} will have length $m = n + 4d(n + d)(n + 2)$. In preparation, we can compute a number N such that the functions f_0, \dots, f_m from Lemma 5.2 for any $L \subseteq [0, m]^2$ satisfy $\text{supp}(f_i) \subseteq \{t^j \mid j \in [0, N - 1]\}$. For each $i \in [1, n]$, $c \in G$, $s \in \mathbb{N}$, we define the knapsack expression $E_{i,c,s}$ over $G \wr H$ as

$$E_{i,c,s} = \begin{cases} e_1 \dots e_{i-1} (t^s) (ct^{-s} h_i t^s)^{x_i} (ct^{-s}) e_{i+1} \dots e_n, & \text{if } e_i = h_i^{x_i}, \\ e_1 \dots e_{i-1} (t^s) (ct^{-s} h_i t^s) (ct^{-s}) e_{i+1} \dots e_n, & \text{if } e_i = h_i. \end{cases} \quad (1)$$

The parentheses indicate the atoms. We define

$$\hat{E} = E \cdot \prod_{k=1}^d \prod_{s \in S_k} \left(E_{i_k, a, s} \cdot E_{j_k, b, s} \cdot E_{i_k, a^{-1}, s} \cdot E_{j_k, b^{-1}, s} \right) \quad (2)$$

where $S_k = \{j(n + d)^{2k} N \mid j \in [1, n + d]\}$ for all $k \in [1, d]$, and all occurrences of expressions of the form $E_{i,c,s}$ use fresh variables. Note that $E_{i_k, a, s} \cdot E_{j_k, b, s} \cdot E_{i_k, a^{-1}, s} \cdot E_{j_k, b^{-1}, s}$ performs the commutator construction for (i_k, j_k) , shifted by t^s . Let $\hat{E} = \hat{e}_1 \dots \hat{e}_m$ be the resulting expression. Notice that its length is indeed $m = n + 4d(n + d)(n + 2)$ as claimed above.

Finally, in our HKP $^+(G \wr H)$ instance, we also add a set $J \subseteq [0, m]^2$ of loop constraints stating that for each $k \in [1, d]$ and $s \in S_k$, the i_k -th atom in $E_{i_k, a, s}$ arrives at the same place in H as the i_k -th atom in E (and analogously for $E_{j_k, b, s}$, $E_{i_k, a^{-1}, s}$, $E_{j_k, b^{-1}, s}$). See [5] for details.

Let $f_0, \dots, f_m \in \langle a \rangle^{(t^*)}$ be the loop words from Lemma 5.2 for the set $J \subseteq [0, m]^2$. It is now straightforward to verify that the elements \hat{e}_i are all tame as explained above. In other words, for every valuation ν and $i \in [1, m]$, we have $\nu(\hat{e}_i) \in P_{a,t}$ (see [5] for a proof).

Shifting loop words. By construction, we now know that if the instance $f_0 \hat{e}_1 f_1 \cdots \hat{e}_m f_m$ of $\text{KP}(G \wr H)$ has a solution, then so does our normalized instance I of $\text{KP}^\pm(H)$. However, there is one last obstacle: Even if all loop and disjointness constraints can be met for I , we cannot guarantee that $f_0 \hat{e}_1 f_1 \cdots \hat{e}_m f_m$ has a solution: It is possible that some loop words interfere with some commutator constructions so as to yield an element $\neq 1$.

The idea is to *shift* all the loop words f_0, \dots, f_m in direction t by replacing f_i by $t^r f_i t^{-r} = {}^t r f_i$ for some $r \in \mathbb{N}$. We shall argue that for some r in some bounded interval, this must result in an interference free expression; even though the elements \hat{e}_i may modify an unbounded number of points in H . To this end, we use again that the \hat{e}_i are tame: Each of them either (i) places elements from $\langle a \rangle$, or (ii) has a period non-commensurable to t . In the case (i), there can be no interference because the f_i also place elements in $\langle a \rangle$, which is an abelian subgroup. In the case (ii), \hat{e}_i can intersect the support of each f_j at most once. Hence, there are at most m points each f_j has to avoid after shifting. The following simple lemma states that one can always shift finite sets F_i in parallel to avoid finite sets A_i , by a bounded shift. Notice that the bound does not depend on the size of the elements in the sets F_i and A_i .

► **Lemma 5.4.** *Let $F_1, \dots, F_m \subseteq \mathbb{Z}$ with $|F_i| \leq N$ and $A_1, \dots, A_m \subseteq \mathbb{Z}$ with $|A_i| \leq \ell$. There exists a shift $r \in [0, Nm\ell]$ such that $(r + F_i) \cap A_i = \emptyset$ for each $i \in [1, m]$.*

Proof. For every $a \in \mathbb{Z}$ there exist at most $|F_i| \leq N$ many shifts $r \in \mathbb{N}$ where $a \in r + F_i$. Therefore there must be a shift $r \in [0, Nm\ell]$ such that $(r + F_i) \cap A_i = \emptyset$ for each $i \in [1, m]$. ◀

We can thus prove the following lemma, which clearly completes the reduction from $\text{KP}^\pm(H)$ to $\text{KP}(G \wr H)$.

► **Lemma 5.5.** *$I = (E, L, D)$ has a solution if and only if ${}^t r f_0 \hat{e}_1 {}^t r f_1 \dots \hat{e}_m {}^t r f_m$ has a solution for some $r \in [0, Nm^2]$.*

6 Applications

The discrete Heisenberg group. Here, we prove that $\text{SAT}^+(H_3(\mathbb{Z}))$ is undecidable. Together with Theorem 3.1 and Theorem 3.2, this directly implies Theorem 3.3. Define the matrices $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, and $C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The group $H_3(\mathbb{Z})$ is generated by A and B and we have $AC = CA$ and $BC = CB$. It is well-known that (I) $A^i C^j = A^{i'} C^{j'}$ iff $i = i'$ and $j = j'$; and (II) $B^i C^j = B^{i'} C^{j'}$ iff $i = i'$ and $j = j'$; and (III) $A^i B^j A^{-i'} B^{-j'} = C^k$ if and only if $i = i'$, $j = j'$, and $k = ij$. For proofs, see the full version [5].

We show undecidability of $\text{SAT}^+(H_3(\mathbb{Z}))$ by reducing from solvability of Diophantine equations over natural numbers. Hence, we are given a finite system $\bigwedge_{j=1}^m E_j$ of equations of the form $x = a$, $z = x + y$, and $z = xy$. It is well-known that solvability of such equation systems is undecidable [23]. Given such an equation system over a set of variables X we define a $\mathcal{C}^+(H_3(\mathbb{Z}))$ -formula containing the variables $\{g_x \mid x \in X\} \cup \{g_0\}$ with the interpretation that $g_x = g_0 C^x$. First we state that $g_0 \xrightarrow{C}^* g_x$ for all $x \in X$. Expressing $x = a$ is done simply with $g_0 \xrightarrow{C^a} g_x$. For $z = x + y$, we use

$$C^x A^* \cap A^{x'} C^* \cap (AC)^* \neq \emptyset \quad \wedge \quad A^{x'} C^* \cap C^z A^* \cap C^y (AC)^* \neq \emptyset.$$

This can be expressed in $\mathcal{C}^+(H_3(\mathbb{Z}))$ with a fresh variable $f_{x'}$ for $g_0 A^{x'}$: For example, the first conjunct holds iff there exists $h \in H_3(\mathbb{Z})$ such that $g_0 \xrightarrow{A}^* f_{x'}$, $g_x \xrightarrow{A}^* h$, $f_{x'} \xrightarrow{C}^* h$, $g_0 \xrightarrow{AC}^* h$. By (I) and $AC = CA$, the first conjunct holds iff $x = x'$. Similarly, the second conjunct holds iff $z = x' + y$, hence $z = x + y$. For $z = xy$, we use:

$$C^x A^* \cap A^{x'} C^* \cap (AC)^* \neq \emptyset \wedge B^{y'} C^* \cap C^{y'} B^* \cap (BC)^* \neq \emptyset \wedge A^{x'} B^* (A^{-1})^* \cap B^{y'} C^* \cap C^z B^* \neq \emptyset.$$

Like above, the first and second conjunct express $x' = x$ and $y' = y$. The third says that $A^{x'} B^r (A^{-1})^s = B^{y'} C^z$ for some $r, s \geq 0$, so by (III), it states $z = x'y'$, hence $z = xy$.

Solvable Baumslag-Solitar groups. We show that $\text{SAT}^\pm(\text{BS}(1, q))$ is decidable for every $q \geq 1$. By Theorem 3.1 and Theorem 3.2, this proves Theorem 3.5. Our proof is based on the following observation, which is shown in the full version [5].

► **Proposition 6.1.** *The first-order theory of $C^+(\text{BS}(1, q))$ is decidable.*

For Proposition 6.1, we show that given any finite subset $F \subseteq \text{BS}(1, q)$, the structure $(\text{BS}(1, q), (\xrightarrow{g})_{g \in F}, (\xrightarrow{g^*})_{g \in F})$ is effectively an automatic structure, which implies that its first-order theory is decidable [15, Corollary 4.2]. This uses a straightforward extension of the methods in [21]. In [21, proof of Theorem 4.1], it is shown that $\text{KP}(\text{BS}(1, q))$ can be reduced to the existential fragment of the structure $(\mathbb{Z}, +, V_q)$, where $V_q(n)$ is the largest power of q that divides n . The structure $(\mathbb{Z}, +, V_q)$ is called *Büchi arithmetic* and is well-known to be automatic. Here, we show that $(\text{BS}(1, q), (\xrightarrow{g})_{g \in F}, (\xrightarrow{g^*})_{g \in F})$ can be interpreted in a slight extension of Büchi arithmetic that is still automatic. From Proposition 6.1, we can derive a stronger statement, which clearly implies decidability of $\text{SAT}^\pm(\text{BS}(1, q))$:

► **Theorem 6.2.** *The first-order theory of $C^\pm(\text{BS}(1, q))$ is decidable.*

Indeed, since $\text{BS}(1, q)$ is torsion-free, we can express the predicate $\perp_{g,h}$ using universal quantification: We have $(g_1, g_2) \perp_{g,h} (h_1, h_2)$ if and only if $g_1 \xrightarrow{g^*} g_2$ and $h_1 \xrightarrow{h^*} h_2$ and

$$\forall f, f' \in \text{BS}(1, q): \left(g_1 \xrightarrow{g^*} f \wedge f \xrightarrow{g^*} g_2 \wedge h_1 \xrightarrow{h^*} f' \wedge f' \xrightarrow{h^*} h_2 \right) \rightarrow f \neq f'.$$

7 Conclusion

We have shown that for non-trivial groups G and infinite groups H , the problem $\text{KP}(G \wr H)$ is decidable if and only if $\text{ExpEq}(G)$ is decidable and either (i) G is abelian and $\text{KP}^+(H)$ is decidable or (ii) G is non-abelian and $\text{KP}^\pm(H)$ is decidable. This reduces the study of decidability of $\text{KP}(G \wr H)$ to decidability questions about the factors G and H .

Intersection knapsack (KP^\pm) vs positive intersection knapsack (KP^+). However, we leave open whether there is a group H where $\text{KP}^+(H)$ is decidable, but $\text{KP}^\pm(H)$ is undecidable. It is clear that both are decidable for all groups in the class of knapsack-semilinear groups. This class contains a large part of the groups for which knapsack has been studied. For example, it contains graph groups [20, Theorem 3.11] and hyperbolic groups [17, Theorem 8.1]. Moreover, knapsack-semilinearity is preserved by a variety of constructions: This includes wreath products [10, Theorem 5.4], graph products [8], free products with amalgamation and HNN-extensions over finite identified subgroups [8], and taking finite-index overgroups [8]. Moreover, the groups $H_3(\mathbb{Z})$ and $\text{BS}(1, q)$ for $q \geq 2$ are also unable to distinguish KP^+ and KP^\pm : We have shown here that KP^+ is undecidable in $H_3(\mathbb{Z})$ and KP^\pm is decidable in $\text{BS}(1, q)$. To the best of the authors' knowledge, among the groups for which knapsack is currently known to be decidable, this only leaves $\text{BS}(p, q)$ for p, q coprime, and $G \wr \text{BS}(1, q)$ (with decidable $\text{ExpEq}(G)$) as candidates to distinguish KP^+ and KP^\pm .

Complexity. Another aspect that our work does not settle is the complexity of $\text{KP}(G \wr H)$ for each G and H . We refer to [7] for a current overview on this.

The reductions presented here have high complexity. For example, our reduction from $\text{KP}(G \wr H)$ involves several transformations of instances of $\text{KP}(G \wr H)$, $\text{HKP}(G \wr H)$, $\text{KP}^\pm(H)$, $\text{KP}(H)$, or $\text{ExpEq}(G)$. In multiple of these transformations, as an auxiliary step, we take an instance I , extract from it a set of knapsack equations $a^x b^y = c$ with $a, b, c \in H$, find minimal solutions, and use them to compute a new instance I' . Thus, the complexity of our reduction depends on the size of minimal solutions to (two-variable) knapsack equations in H . Moreover, even if one assumes a polynomial bound on such solution sizes (which is known to hold, for example, in graph groups defined by transitive forests [20, Theorem 4.10] and in hyperbolic groups [27] (see also [17, Theorem 8.1])), our reduction still involves multiple steps that incur an exponential blow-up.

Furthermore, our reduction from $\text{KP}^\pm(H)$ (or $\text{KP}^+(H)$) to $\text{KP}(G \wr H)$ produces double-exponentially many instances of $\text{KP}(G \wr H)$, each of which is doubly exponential in size.

References

- 1 L. Babai, R. Beals, J. Cai, G. Ivanyos, and E. M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of SODA 1996*, pages 498–507. ACM/SIAM, 1996.
- 2 G. Baumslag and D. Solitar. Some two-generator one-relator non-Hopfian groups. *Bulletin of the American Mathematical Society*, 68(3):199–201, 1962. doi:10.1090/S0002-9904-1962-10745-9.
- 3 P. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. Matrix equations and hilbert’s tenth problem. *International Journal of Algebra and Computation*, 18(8):1231–1241, 2008. doi:10.1142/S0218196708004925.
- 4 P. Bell, I. Potapov, and P. Semukhin. On the mortality problem: From multiplicative matrix equations to linear recurrence sequences and beyond. In *Proceedings of MFCS 2019*, pages 83:1–83:15, 2019. doi:10.4230/LIPIcs.MFCS.2019.83.
- 5 P. Bergsträßer, M. Ganardi, and G. Zetsche. A characterization of wreath products where knapsack is decidable, 2021. arXiv:2101.06132.
- 6 F. A. Dudkin and A. V. Treyer. Knapsack problem for baumslag–solitar groups. *Siberian Journal of Pure and Applied Mathematics*, 18(4):43–55, 2018.
- 7 M. Figelius, M. Ganardi, M. Lohrey, and G. Zetsche. The complexity of knapsack problems in wreath products. In *Proceedings of ICALP 2020*, pages 126:1–126:18, 2020. doi:10.4230/LIPIcs.ICALP.2020.126.
- 8 M. Figelius, M. Lohrey, and G. Zetsche. Closure properties of knapsack semilinear groups, 2019. arXiv:1911.12857.
- 9 E. Frenkel, A. Nikolaev, and A. Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016. doi:10.1016/j.jsc.2015.05.006.
- 10 M. Ganardi, D. König, M. Lohrey, and G. Zetsche. Knapsack problems for wreath products. In *Proceedings of STACS 2018*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018. doi:10.4230/LIPIcs.STACS.2018.32.
- 11 M. Ganardi and M. Lohrey, 2020. Personal communication.
- 12 M. Gromov. Groups of polynomial growth and expanding maps. *Publications Mathématiques de l’Institut des Hautes Études Scientifiques*, 53(1):53–78, 1981.
- 13 F. Gul, M. Sohrabi, and A. Ushakov. Magnus embedding and algorithmic properties of groups $f/n^{(d)}$. *Transactions of the American Mathematical Society*, 369(9):6189–6206, 2017.
- 14 M. I. Kargapolov and J. I. Merzljakov. *Fundamentals of the Theory of Groups*. Springer-Verlag, New York, 1979. Translated from the second Russian edition.
- 15 B. Khossainov and A. Nerode. Automatic presentations of structures. In *International Workshop on Logic and Computational Complexity*, pages 367–392. Springer, 1994.

- 16 D. König, M. Lohrey, and G. 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. doi:10.1090/comm/677.
- 17 M. Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020. doi:10.1016/j.jalgebra.2019.04.008.
- 18 M. Lohrey, B. Steinberg, and G. Zetsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015. doi:10.1016/j.ic.2014.12.014.
- 19 M. Lohrey and G. Zetsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In *Proceedings of 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. doi:10.4230/LIPIcs.STACS.2016.50.
- 20 M. Lohrey and G. Zetsche. Knapsack in graph groups. *Theory of Computing Systems*, 62(1):192–246, 2018. doi:10.1007/s00224-017-9808-3.
- 21 M. Lohrey and G. Zetsche. Knapsack and the power word problem in solvable baumslag-solitar groups. In *Proceedings of MFCS 2020*, pages 67:1–67:15, 2020. doi:10.4230/LIPIcs.MFCS.2020.67.
- 22 W. Magnus. On a theorem of Marshall Hall. *Annals of Mathematics. Second Series*, 40:764–768, 1939.
- 23 Y. V. Matiyasevich. *Hilbert’s Tenth Problem*. MIT Press, Cambridge, Massachusetts, 1993.
- 24 J. Matthews. The conjugacy problem in wreath products and free metabelian groups. *Transactions of the American Mathematical Society*, 121(2):329–339, 1966.
- 25 A. Miasnikov, S. Vassileva, and A. Weiß. The conjugacy problem in free solvable groups and wreath products of abelian groups is in TC^0 . *Theory of Computing Systems*, 63(4):809–832, 2019.
- 26 A. Mishchenko and A. Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017.
- 27 A. Myasnikov, A. Nikolaev, and A. Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015. doi:10.1090/S0025-5718-2014-02880-9.
- 28 V. Remeslennikov and V. Sokolov. Some properties of a magnus embedding. *Algebra and Logic*, 9(5):342–349, 1970.