Knapsack and the Power Word Problem in Solvable Baumslag-Solitar Groups

Markus Lohrey
Universität Siegen, Germany
lohrey@eti.uni-siegen.de

Georg Zetzsche
Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern, Germany
georg@mpi-sws.org

Abstract

We prove that the power word problem for the solvable Baumslag-Solitar groups $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$ can be solved in TC^0. In the power word problem, the input consists of group elements $g_1, \ldots, g_d$ and binary encoded integers $n_1, \ldots, n_d$ and it is asked whether $g_1^{n_1} \cdots g_d^{n_d} = 1$ holds. Moreover, we prove that the knapsack problem for $\mathrm{BS}(1,q)$ is NP-complete. In the knapsack problem, the input consists of group elements $g_1, \ldots, g_d, h$ and it is asked whether the equation $g_1^{x_1} \cdots g_d^{x_d} = h$ has a solution in $\mathbb{N}^d$.

2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness

Keywords and phrases computational group theory, matrix problems, Baumslag-Solitar groups

Digital Object Identifier 10.4230/LIPIcs.MFCS.2020.67

Related Version A long version of this paper can be found at `https://arxiv.org/abs/2002.03837`.

Funding *Markus Lohrey*: Funded by DFG project LO 748/12-1.

1 Introduction

The power word problem. The study of multiplicative identities and equations has a long tradition in computational algebra, and has recently been extended to the non-abelian case. Here, the multiplicative identities we have in mind have the form $g_1^{n_1} g_2^{n_2} \cdots g_d^{n_d} = 1$, where $g_1, \ldots, g_d$ are elements of a group G and $n_1, n_2, \ldots, n_d \in \mathbb{N}$ are non-negative integers (we may also allow negative n_i, but this makes no difference, since we can replace a g_i by its inverse g_i^{-1}). Typically, the numbers n_i are given in binary representation, whereas the representation of the group elements g_i depends on the underlying group G. Here, we consider the case where G is a finitely generated (f.g. for short) group, and elements of G are represented by finite words over a fixed generating set Σ (the concrete choice of Σ is not relevant). In this setting, the question whether $g_1^{n_1} g_2^{n_2} \cdots g_d^{n_d} = 1$ is a true identity has been recently introduced as the *power word problem* for G [27]. It extends the classical word problem for G (does a given word over the group generators represent the group identity?) in the sense that the word problem trivially reduces to the power word problem (take an identity $w^1 = 1$). Recent results on the power word problem in specific f.g. groups are:

- For every f.g. free group the power word problem belongs to deterministic logspace [27].
- For the following groups the power word problem belongs to the circuit complexity class TC^0:[1] f.g. nilpotent groups [27], iterated wreath products of f.g. free abelian groups and (as a consequence of the latter) free solvable groups [11].

[1] In this paper, TC^0 always refers to the $\mathsf{DLOGTIME}$-uniform version.

- If G is a so-called uniformly efficiently non-solvable group (this is a large class of non-solvable groups that was recently introduced in [3] and that includes all finite non-solvable groups and f.g. free non-abelian groups) then the power word problem for the wreath product $G \wr \mathbb{Z}$ is coNP-hard [11].

Historically, the power word problem appeared earlier in the area of computational (commutative) algebra. Ge [16] proved that one can check in polynomial time whether an identity $\alpha_1^{n_1}\alpha_2^{n_2}\cdots\alpha_d^{n_d} = 1$, where the n_i are binary encoded integers and the α_i are from an algebraic number field (and suitable encoded), holds.

In this paper we investigate the power word problem for the solvable Baumslag-Solitar group $\mathrm{BS}(1,q)$ for $q \geq 2$ an integer. This group is usually defined as the finitely presented group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$. It has a nice matrix representation as the group of all matrices of the form

$$\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \tag{1}$$

with $k \in \mathbb{Z}$ and $u \in \mathbb{Z}[1/q]$ a rational number with a finite q-ary expansion. Our *first main result* is that the power word problem for $\mathrm{BS}(1,q)$ belongs to TC^0. This generalizes a corresponding result for the word problem of $\mathrm{BS}(1,q)$ from [35]; see also [22, 37]. Via the above matrix embedding our result for the power word problem for $\mathrm{BS}(1,q)$ is directly related to recent results on matrix powering problems [1, 14]. These problems can be quite difficult to analyze. For instance, it is not known whether a certain bit of the $(0,0)$-entry of a matrix power A^n can be computed in polynomial time, when n is given in binary notation and A is a (2×2)-matrix over $\mathbb{Z}$. The related problem of checking whether the $(0,0)$-entry (or any other entry) of A^n is positive can be solved in polynomial time by [14].

The knapsack problem. If one replaces in the power word problem the exponents n_i by pairwise different variables x_i and the right-hand side 1 by an arbitrary group element $h \in G$, one obtains a so-called knapsack equation $g_1^{x_1}g_2^{x_2}\cdots g_d^{x_d} = h$. The question, whether such an equation has a solution in $\mathbb{N}^d$ is known as the *knapsack problem* for G. In the general context of finitely generated groups the knapsack problem has been introduced by Myasnikov, Nikolaev, and Ushakov [33]. As for the power word problem, this problem has been studied in the commutative setting before. For the case $G = \mathbb{Z}$ one obtains a variant of the classical NP-complete knapsack problem; a proof of the NP-hardness of our variant of the knapsack problem for the integers can be found in [18]. For this hardness result it is important that integers are represented in binary notation. For unary encoded integers the complexity of the knapsack problem goes down to TC^0. For the case that the g_i are commuting matrices over an algebraic number field, the knapsack problem has been studied in [2, 8].

For the case of (in general) non-commutative groups, the knapsack problem has been studied in [9, 11, 13, 15, 23, 26, 29, 33]. In these papers, group elements are usually represented by finite words over the generators (although in [29] a more succinct representation by so-called straight-line programs is studied as well). Note that for the group $\mathbb{Z}$ this corresponds to a unary representation of integers. Hyperbolic groups (which are of fundamental importance in the area of geometric group theory) are an important class of groups where knapsack can be decided in polynomial time (and even in LogCFL). This result can be extended to the class of all groups that can be built from hyperbolic groups by the operations of (i) direct products with $\mathbb{Z}$ and (ii) free products [29]. On the other hand, for many groups the knapsack problem is NP-complete. Examples are certain right-angled Artin groups (like the direct product of two free groups of rank two [29]), wreath products (e.g. the wreath product $\mathbb{Z} \wr \mathbb{Z}$ [15]) and free solvable groups [11]. For wreath products $G \wr \mathbb{Z}$, where G is finite non-solvable or free of rank at least two, the knapsack problem is Σ_2^p-complete [11]. Finally, for finitely generated nilpotent groups, the knapsack problem is in general undecidable [15, 32].

Our second main result is that for the Baumslag-Solitar groups $\mathrm{BS}(1,q)$ with $q \geq 2$ the knapsack problem is NP-complete. This extends a result from [9], where decidability (without any complexity bound) was shown for a restriction of the knapsack problem for $\mathrm{BS}(1,q)$. In this restriction, all group elements g_i must have the form (1) with $k \neq 0$. Showing NP-hardness of the knapsack problem for $\mathrm{BS}(1,q)$ is easy (based on the result that knapsack for $\mathbb{Z}$ with binary encoded integers is NP-hard). For membership in NP we use a recent result of Guépin, Haase, and Worrell [17] according to which the existential fragment of Büchi arithmetic (an extension of Presburger arithmetic) belongs to NP. The NP-membership of the knapsack problem for $\mathrm{BS}(1,q)$ is a bit of a surprise, since one can show that minimal solutions of knapsack equations over $\mathrm{BS}(1,q)$ can be of size doubly exponential in the length of the equation, see Theorem 4.2. This rules out a simple guess-and-verify strategy.

2 Preliminaries

For $a, b \in \mathbb{Z}$ we write $a \mid b$ if $b = ka$ for some $k \in \mathbb{Z}$. We denote with $[a,b]$ the interval $\{z \in \mathbb{Z} \mid a \leq z \leq b\}$. With $\mathbb{Z}[1/q]$ we denote the set of all rational numbers that have finite expansion in base q, i.e., the set of all numbers $\sum_{a \leq i \leq b} r_i q^i$ with $r_i \in [0, q-1]$ and $a, b \in \mathbb{Z}$. If $u = \sum_{-k \leq i \leq \ell} r_i q^i \neq 0$ with $k, \ell \geq 0$ and $\ell + k$ minimal, we define $\|u\|_q = \ell + k$. Under the assumption that q is a constant (which will be always the case in this paper), $\|u\|_q$ is the length of a suitable q-ary representation of u.

A *Laurent polynomial* is an ordinary polynomial that may also contain powers x^k with $k < 0$. Formally, a Laurent polynomial over $\mathbb{Z}$ is an expression $P(x) = \sum_{i \in \mathbb{Z}} a_i x^i$ with $a_i \in \mathbb{Z}$ such that only finitely many a_i are non-zero. With $\mathbb{Z}[x, x^{-1}]$ we denote the set of all Laurent polynomials over $\mathbb{Z}$; it is a ring with the natural addition and multiplication operations.

Complexity. We assume basic knowledge in complexity theory. We deal with the circuit complexity class TC^0. It contains all problems that can be solved by a family of threshold circuits of polynomial size and constant depth. In this paper, TC^0 always refers to the $\mathsf{DLOGTIME}$-uniform version of TC^0. In this variant, TC^0 is contained in deterministic logspace. A precise definition of ($\mathsf{DLOGTIME}$-uniform) TC^0 is not needed for our work; see [36] for details. All we need is that the following problems can be solved in TC^0:

1. iterated addition and multiplication of binary encoded numbers and polynomials [10, 19],
2. division with remainder of binary encoded numbers [19],
3. computing the number $|w|_a$ of occurrences of a letter a in a word w,
4. computing an image $h(w)$ where $h : \Sigma^* \to \Gamma^*$ is a homomorphism [24].

The results on binary numbers hold for any basis, since one can transform between binary representation and q-ary representation; this is a consequence of the first two points.

Groups. We assume that the reader is familiar with the basics of group theory. Let G be a group. We always write 1 for the group identity element. We say that G is *finitely generated (f.g.)* if there is a finite subset $\Sigma \subseteq G$ such that every element of G can be written as a product of elements from Σ; such a Σ is called a *(finite) generating set* for G. We always assume that $a \in \Sigma$ implies $a^{-1} \in \Sigma$; such a generating set is also called *symmetric*. We write $G = \langle \Sigma \rangle$ if Σ is a symmetric generating set for G. In this case, we have a canonical morphism $h : \Sigma^* \to G$ that maps a word over Σ to its product in G. If $h(w) = 1$ we also say that $w = 1$ *in* G. On Σ^* we can define a natural involution $\cdot^{-1}$ by $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$ for $a_1, a_2, \ldots, a_n \in \Sigma$.

Baumslag-Solitar groups. For $p, q \in \mathbb{Z} \setminus \{0\}$, the *Baumslag-Solitar group* $\mathrm{BS}(p,q)$ is defined as the finitely presented group $\mathrm{BS}(p,q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$. We can w.l.o.g. assume that $q \geq 1$. Of particular interest are the Baumslag-Solitar groups $\mathrm{BS}(1,q)$ for $q \geq 2$. They are solvable and linear. It is well-known (see e.g. [39, III.15.C]) that $\mathrm{BS}(1,q)$ is isomorphic to the subgroup $T(q)$ of $\mathrm{GL}(2,\mathbb{Q})$ consisting of the upper triangular matrices

$$\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \tag{2}$$

with $k \in \mathbb{Z}$ and $u \in \mathbb{Z}[1/q]$. This means we have the multiplication

$$\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q^\ell & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} q^{\ell+k} & u + v \cdot q^k \\ 0 & 1 \end{pmatrix}. \tag{3}$$

Let us define the morphism $h : \{a, a^{-1}, t, t^{-1}\}^* \to T(q)$ by

$$h(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad h(t) = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \tag{4}$$

and $h(a^{-1}) = h(a)^{-1}$, $h(t^{-1}) = h(t)^{-1}$. Then $h(w)$ is the identity matrix if and only if $w = 1$ in $\mathrm{BS}(1,q)$.

▶ **Lemma 2.1.** *Given a word $w \in \{a, a^{-1}, t, t^{-1}\}^*$ we can compute in TC^0 the matrix $h(w)$ with matrix entries given in q-ary encoding. Vice versa, given a matrix $A \in T(q)$ with q-ary encoded entries, we can compute in TC^0 a word $w \in h^{-1}(A)$.*

Proof. First consider a word $w \in \{a, a^{-1}, t, t^{-1}\}^*$ and let $h(w)$ be the matrix in (2). Then $k = |w|_t - |w|_{t^{-1}}$, which can be computed in TC^0. It remains to compute the q-ary representation of u. Let $w_1 a^{\epsilon_1}, \ldots, w_l a^{\epsilon_l}$ be all prefixes of w that end with a or a^{-1} ($\epsilon_1, \ldots, \epsilon_l \in \{-1, 1\}$). Let $k_i = |w_i|_t - |w_i|_{t^{-1}}$, which can be computed in TC^0 in unary notation. Then, $u = \sum_{i=1}^{l} \epsilon_i q^{k_i}$, which can be easily computed in q-ary notation.

The inverse transformation is straightforward using the q-ary representation of a matrix of the form (2): Note that since q^k is given in q-ary representation, the integer k is implicitly given in unary representation. A matrix of the form $\left(\begin{smallmatrix} 1 & q^z \\ 0 & 1 \end{smallmatrix}\right)$ (for a unary encoded z) can be produced by the word $t^z a t^{-z}$. By concatenating such words (which is possible in TC^0 by point 4 from page 3), one can produce from a given q-ary encoded number $u \in \mathbb{Z}[1/q]$ a word for the matrix $\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)$. Finally, one has to concatenate t^k on the right in order to get (2). ◀

By the previous lemma, we can represent elements of $\mathrm{BS}(1,q)$ either as words over the alphabet $\{a, a^{-1}, t, t^{-1}\}$ or by matrices from $T(q)$ with q-ary encoded entries. For the matrix $A \in T(q)$ in (2) we define $\|A\| = |k| + \|u\|_q$. Hence $\|A\|$ is the length of the encoding of A.

A group that is closely related to $\mathrm{BS}(1,q)$ is the restricted wreath product $\mathbb{Z} \wr \mathbb{Z}$. It is isomorphic to the group of all matrices

$$\begin{pmatrix} x^k & P(x) \\ 0 & 1 \end{pmatrix} \tag{5}$$

where $k \in \mathbb{Z}$ and $P(x) \in \mathbb{Z}[x, x^{-1}]$ (see e.g. [31, Section 2.2]). It can be generated by

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

In contrast to $\mathrm{BS}(1,q)$, the group is $\mathbb{Z} \wr \mathbb{Z}$ not finitely presented [4]. Obviously we have:

▶ **Lemma 2.2.** *The mapping* $\phi_q : \begin{pmatrix} x^c & P(x) \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} q^c & P(q) \\ 0 & 1 \end{pmatrix}$ *is a surjective homomorphism* $\phi_q : \mathbb{Z} \wr \mathbb{Z} \to T(q) \cong \mathrm{BS}(1,q)$.

With our choice of generators a, t for $\mathbb{Z} \wr \mathbb{Z}$ and $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$, the above homomorphism ϕ_q satisfies $\phi_q(a) = a$ and $\phi_q(t) = t$.

Knapsack and the power word problem. Let $G = \langle \Sigma \rangle$ be a f.g. group. Moreover, let $x_1, x_2, \ldots, x_d$ be pairwise distinct variables. A *knapsack expression* over G is an expression of the form $E = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_d^{x_d} v_d$ with $d \geq 1$, words $v_0, \ldots, v_d \in \Sigma^*$ and non-empty words $u_1, \ldots, u_d \in \Sigma^*$. A tuple $(n_1, \ldots, n_d) \in \mathbb{N}^d$ is a *G-solution* of E if $v_0 u_1^{n_1} v_1 u_2^{n_2} v_2 \cdots u_d^{n_d} v_d = 1$ in G. With $\mathrm{sol}_G(E)$ we denote the set of all G-solutions of E. The *size* of E is defined as $|E| = \sum_{i=1}^{d} |u_i| + |v_i|$. The *knapsack problem for G*, $\textsc{Knapsack}(G)$ for short, is the following decision problem:

Input A knapsack expression E over G.

Question Is $\mathrm{sol}_G(E)$ non-empty?

It is easy to observe that the concrete choice of the generating set Σ has no influence on the decidability/complexity status of $\textsc{Knapsack}(G)$. W.l.o.g. we can restrict to knapsack expressions of the form $u_1^{x_1} u_2^{x_2} \cdots u_d^{x_d} v$: for $E = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_d^{x_d} v_d$ and

$$E' = (v_0 u_1 v_0^{-1})^{x_1} (v_0 v_1 u_2 v_1^{-1} v_0^{-1})^{x_2} \cdots (v_0 \cdots v_{d-1} u_d v_{d-1}^{-1} \cdots v_0^{-1})^{x_d} v_0 \cdots v_{d-1} v_d$$

we have $\mathrm{sol}_G(E) = \mathrm{sol}_G(E')$.

A *power word* (over Σ) is a tuple $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$ where $u_1, \ldots, u_d \in \Sigma^*$ are words over the group generators and $k_1, \ldots, k_d \in \mathbb{Z}$ are integers that are given in binary notation. Such a power word represents the word $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d}$. Quite often, we will identify the power word $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$ with the word $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d}$. The *power word problem* for the f.g. group G, $\textsc{PowerWP}(G)$ for short, is defined as follows:

Input A power word $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$.

Question Does $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d} = 1$ hold in G?

Due to the binary encoded exponents, a power word can be seen as a succinct description of an ordinary word. The size of the above power word w is $\sum_{i=1}^{d} |u_i| + \lceil \log_2 k_i \rceil$ which is the length of the binary encoding of w.

3 Power word problem for BS(1,q)

In this section we prove our first main result:

▶ **Theorem 3.1.** *For every $q \in \mathbb{N}$ with $q \geq 2$, $\textsc{PowerWP}(\mathrm{BS}(1,q))$ belongs to* TC^0.

For the proof we will first work in the wreath product $\mathbb{Z} \wr \mathbb{Z}$. Recall the homomorphism ϕ_q from Lemma 2.2. The evaluation of a given power word over the group $\mathbb{Z} \wr \mathbb{Z}$ leads to periodic Laurent polynomials, which we consider first.

Periodic Laurent polynomials. Consider a Laurent polynomial $P(x) = \sum_{i \in \mathbb{Z}} a_i x^i \in \mathbb{Z}[x, x^{-1}]$. We define its support $\mathrm{supp}(P) = \{i \in \mathbb{Z} \mid a_i \neq 0\}$. For $f \geq 1$ we say that $P(x)$ is *f-periodic* on the interval $[k, \ell] \subseteq \mathbb{Z}$ if $\mathrm{supp}(P) \subseteq [k, \ell]$ and $a_i = a_{i-f}$ for all $k + f \leq i \leq \ell$. Then we have

$$(1 - x^f) \cdot P(x) = \sum_{i=k}^{\ell} (a_i x^i - a_i x^{i+f}) = \sum_{i=k}^{k+f-1} a_i x^i - \sum_{i=\ell+1}^{\ell+f} a_{i-f} x^i. \tag{6}$$

We have to work with periodic Laurent polynomials that consist of exponentially (with respect to the size of the input power word) many monomials but where the period f is polynomially bounded in the input size. Such a Laurent polynomial can be represented by the first f coefficients together with the period f (in unary representation). We will always use this representation when dealing with periodic Laurent polynomials.

▶ **Lemma 3.2.** *Let $k, \ell \in \mathbb{Z}$ and $P_1(x), \ldots, P_m(x) \in \mathbb{Z}[x, x^{-1}]$ be Laurent polynomials such that P_i is f_i-periodic on $[k, \ell]$ and let $f := \sum_{1 \le i \le m} f_i$. Then we can compute in TC^0 Laurent polyomials $S(x)$, $L(x)$ and $R(x)$ with the following properties:*
- $S(x) \cdot \sum_{i=1}^m P_i(x) = L(x) + R(x)$,
- $\mathrm{supp}(S) \subseteq [0, f]$ *(hence, S is an ordinary polynomial of degree at most f),*
- $\mathrm{supp}(L) \subseteq [k, k+f-1]$,
- $\mathrm{supp}(R) \subseteq [\ell+1, \ell+f]$, *and*
- $S(q) \neq 0$ *for every $q \in \mathbb{N} \setminus \{1\}$.*

Proof. By (6) there exist polynomials $L_i(x)$ and $R_i(x)$ such that for all $i \in [1, m]$:
- $(1 - x^{f_i}) \cdot P_i(x) = L_i(x) + R_i(x)$,
- $\mathrm{supp}(L_i) \subseteq [k, k + f_i - 1]$, and
- $\mathrm{supp}(R_i) \subseteq [\ell + 1, \ell + f_i]$.

Moreover, the $L_i(x)$ and $R_i(x)$ are clearly computable in TC^0 from the $P_i(x)$. With $S(x) := \prod_{1 \le i \le m}(1 - x^{f_i})$ and $\tilde{S}_i(x) := \prod_{j \neq i}(1 - x^{f_j})$ we get

$$S(x) \cdot \sum_{i=1}^{m} P_i(x) \quad = \quad \sum_{i=1}^{m} S(x) \cdot P_i(x) = \sum_{i=1}^{m} \tilde{S}_i(x) L_i(x) + \sum_{i=1}^{m} \tilde{S}_i(x) R_i(x).$$

Let us set $L(x) = \sum_{i=1}^m \tilde{S}_i(x) L_i(x)$ and $R(x) = \sum_{i=1}^m \tilde{S}_i(x) R_i(x)$. We then get $\mathrm{supp}(S) \subseteq [0, f]$, $\mathrm{supp}(L) \subseteq [k, k+f-1]$, and $\mathrm{supp}(R) \subseteq [\ell+1, \ell+f]$. Since iterated addition and multiplication of polynomials is in TC^0, we can compute the polynomials $L(x)$ and $R(x)$ in TC^0. The fact that we are dealing with Laurent polynomials does not cause any problems here. Formally, one can multiply all polynomials by suitable powers of x in order to get ordinary polynomials, then add/multiply all polynomials and finally multiply by the appropriate negative power of x. ◀

Proof sketch of Theorem 3.1. Let us now consider a Baumslag-Solitar group $\mathrm{BS}(1, q)$ with $q \ge 2$ and the surjective homomorphism $\phi_q : \mathbb{Z} \wr \mathbb{Z} \to \mathrm{BS}(1, q)$. Let us write $\chi : \{a, a^{-1}, t, t^{-1}\}^* \to \mathbb{Z} \wr \mathbb{Z}$ for the canonical monoid morphism that maps a word $w \in \{a, a^{-1}, t, t^{-1}\}^*$ to the group element of $\mathbb{Z} \wr \mathbb{Z}$ represented by w.

Consider a power word $w = u_1^{z_1} u_2^{z_2} \cdots u_d^{z_d}$ with $u_i \in \{a, a^{-1}, t, t^{-1}\}^*$ and let n be the size of w. In the first step we compute a suitable representation of the group element $\chi(w) \in \mathbb{Z} \wr \mathbb{Z}$. Based on this representation we check in the second step whether $\phi_q(\chi(w)) = 1$ in $\mathrm{BS}(1, q)$.

Step 1. The first step follows [27, 28], where it was shown that $\mathrm{P{\small OWER}WP}(\mathbb{Z} \wr \mathbb{Z})$ is in TC^0. Let

$$\chi(w) = \begin{pmatrix} x^c & P(x) \\ 0 & 1 \end{pmatrix}.$$

The integer c can be computed in TC^0; this is just iterated addition. If $c \neq 0$, then $\phi_q(\chi(w)) \neq 1$ and we can reject. Hence, let us assume that $c = 0$. Clearly, we cannot compute the Laurent polynomial $P(x)$ in polynomial time; it could be a sum of exponentially many monomials. Nevertheless we can compute a certain implicit representation of $P(x)$. In more detail, we compute from the power word w in TC^0 polynomially many binary-encoded integers $c_0 < c_1 < \cdots < c_m$ with m odd such that $\mathrm{supp}(P) \subseteq [c_0, c_m - 1]$. Hence, the Laurent polynomial $P(x)$ can be written as

$$P(x) = \sum_{c_0 \le i < c_m} a_i x^i.$$

By conjugating the power word w with a large enough power of t, we can assume that $c_0 = 0$. Hence $P(x) \in \mathbb{Z}[x]$. Moreover, if we define the polynomials

$$P_j(x) = \sum_{c_j \le i < c_{j+1}} a_i x^i$$

(so that $P(x) = P_0(x) + P_1(x) + \cdots + P_{m-1}(x)$) then we get the following from [28]:

- For every even j, the polynomial P_j can be computed explicitly in TC^0. In particular, this means that $c_{j+1} - c_j$ must be bounded by $\mathrm{poly}(n)$. The coefficients of P_j are of magnitude $\exp(n)$, hence they will be computed in binary notation.
- For every odd j, the polynomial P_j is a sum of at most d polynomials $P_{j,1}, \ldots, P_{j,d_j}$, where for all $1 \le \ell \le d_j$, $P_{j,\ell}$ is $f_{j,\ell}$-periodic on the interval $[c_j, c_{j+1} - 1]$ for some $f_{j,\ell} \le n$. All coefficients of $P_{j,\ell}$ are bounded by n too. We can then compute in TC^0 for all $1 \le \ell \le d_j$ the period $f_{j,\ell}$ (in unary notation) and the $f_{j,\ell}$ first coefficients of $P_{j,\ell}$. These data uniquely represent P_j.

We refer to the full version [30] for a brief summary of the arguments from [28].

Step 2. Using the data that was computed in the first step, it remains to verify in TC^0 that $P(q) = \sum_{i=0}^{m-1} P_i(q) = 0$. From the polynomials $P_{j,\ell}$ and their periods $f_{j,\ell}$ we can by Lemma 3.2 compute in TC^0 for every odd j polyomials $S_j(x)$, $L_j(x)$ and $R_j(x)$ with the following properties, where $f_j = \sum_{\ell=1}^{d_j} f_{j,\ell}$:

- $S_j(x) \cdot P_j(x) = L_j(x) + R_j(x)$,
- $\mathrm{supp}(S_j) \subseteq [0, f_j]$
- $\mathrm{supp}(L_j) \subseteq [c_j, c_j + f_j - 1]$,
- $\mathrm{supp}(R_j) \subseteq [c_{j+1}, c_{j+1} + f_j - 1]$, and
- $S_j(q) \neq 0$.

Let $p_j = q^{-c_j} P_j(q)$ (an integer) for $j \in [0, m-1]$ and $s_j = S_j(q)$ (a non-zero integer) for every odd $j \in [1, m-2]$. We can compute in TC^0 for every odd $j \in [1, m-2]$ the integer s_j as well as the integers $\ell_j = q^{-c_j} L_j(q)$ and $r_j = q^{-c_{j+1}} R_j(q)$ in binary representation. For every even $j \in [0, m-1]$ we can compute in TC^0 the binary representation of the integer p_j. For all odd j we have

$$q^{c_j} s_j p_j = q^{c_j} \ell_j + q^{c_{j+1}} r_j. \tag{7}$$

To streamline the presentation, we define $r_{-1} = \ell_m = 0$ and $s_{-1} = s_m = 1$. We can also compute an upper bound $e \in \mathbb{N}$ for the absolute value of the coefficients a_i in the polynomial $P(x)$. This number e is of size $\exp(n)$ and we can compute in TC^0 its binary representation.

For a position $i \in [0, c_m]$ let $\mathrm{carry}(i)$ be the carry that arrives in position i when we compute the q-ary expansion of $P(q)$. Formally, it can be defined by

$$\mathrm{carry}(i) = \left\lfloor \sum_{0 \le j < i} a_j q^{j-i} \right\rfloor \cdot q^i.$$

Clearly, $\mathrm{carry}(0) = 0$. Moreover, we can bound the absolute value $|\mathrm{carry}(i)|$ by

$$|\mathrm{carry}(i)| = \left| \left\lfloor \sum_{0 \le j < i} a_j q^{j-i} \right\rfloor \cdot q^i \right| \le e \cdot \sum_{0 \le j < i} q^j < e \cdot q^i.$$

Let us write $\mathrm{carry}(c_j) = q^{c_j} \gamma_j$ for an integer γ_j satisfying $|\gamma_j| < e$. Then for every odd $j \in [1, m-2]$ we get from (7)

$$(q^{c_j} p_j + \mathrm{carry}(c_j)) \cdot s_j = q^{c_j} \ell_j + \mathrm{carry}(c_j) s_j + q^{c_{j+1}} r_j = q^{c_j} (\ell_j + \gamma_j \cdot s_j) + q^{c_{j+1}} r_j. \quad (8)$$

The following claim follows directly from the definition of the carries:

Claim 1. $P(q) = 0$ if and only if the following two properties hold:
(A) $q^{c_{j+1}} \mid (q^{c_j} p_j + \mathrm{carry}(c_j))$ for all $0 \le j \le m-1$, and
(B) $\mathrm{carry}(c_m) = 0$.
Hence, for every $0 \le j \le m-1$ we have to compute $p_j + q^{-c_j} \mathrm{carry}(c_j) = p_j + \gamma_j$, whose absolute value is bounded by $|p_j| + e$. There are two problems: If j is odd then we cannot compute p_j explicitly (it may have exponentially many bits). Moreover, we do not know $\mathrm{carry}(c_j)$. In order to solve these problems, we start with some preprocessing.

Preprocessing. We merge an interval $[c_j, c_{j+1} - 1]$ with j odd with the neighboring (polynomially long) intervals $[c_{j-1}, c_j - 1]$ and $[c_{j+1}, c_{j+2} - 1]$ (if they exist) in case the interval length $c_{j+1} - c_j$ satisfies $q^{c_{j+1} - c_j} \le |\ell_j| + e \cdot |s_j|$. Note that this implies $c_{j+1} - c_j \le \log_q(|\ell_j| + e \cdot |s_j|)$ which is of size $\mathrm{poly}(n)$. Hence, we can compute in TC^0 the polynomial $P_j(x)$ explicitly, which allows us to add to $P_j(x)$ the neighboring polynomials $P_{j-1}(x)$ and $P_{j+1}(x)$ (that have been computed explicitly before). In fact this merging might happen for a block of more than three consecutive polynomials $P_j(x)$.

After this preprocessing, we can assume that for every odd $j \in [1, m-2]$ we have $q^{c_{j+1} - c_j} > |\ell_j| + e \cdot |s_j|$. For the absolute value of the term $q^{c_j} \cdot (\ell_j + \gamma_j \cdot s_j)$ in (8) we then obtain

$$q^{c_j} \cdot |\ell_j + \gamma_j \cdot s_j| \le q^{c_j} \cdot (|\ell_j| + |\gamma_j| \cdot |s_j|) < q^{c_j} \cdot (|\ell_j| + e \cdot |s_j|) < q^{c_{j+1}}. \quad (9)$$

With (8), this implies that if $\ell_j + \gamma_j \cdot s_j \ne 0$ then $(q^{c_j} p_j + \mathrm{carry}(c_j)) \cdot s_j$ is not a multiple of $q^{c_{j+1}}$. Hence, also $q^{c_j} p_j + \mathrm{carry}(c_j)$ is not a multiple of $q^{c_{j+1}}$, which implies $P(q) \ne 0$ by (A). In summary, the preprocessing makes the term $\ell_j + \gamma_j \cdot s_j$ in (8) vanish for odd $j \ge 1$ in case $P(q) = 0$. In particular, this lets us express $q^{c_j} p_j + \mathrm{carry}(c_j)$ in terms of $q^{c_{j+1}}$, r_j, and s_j.

We now state the following main claim, which directly implies that $P(q) = 0$ can be checked in TC^0 (for this, we use the seminal result of Hesse et al. [19] according to which integer division is in TC^0).

Claim 2. $P(q) = 0$ if and only if the following conditions hold.
(a) $s_j \mid r_j$ for every odd $1 \le j \le m-2$ (for $j = -1$ this holds by definition of r_{-1} and s_{-1}),
(b) $q^{c_{j+2} - c_{j+1}} \mid (p_{j+1} + r_j / s_j)$ for every odd $-1 \le j \le m-2$,
(c) $\ell_{j+2} + q^{c_{j+1} - c_{j+2}} (p_{j+1} + r_j / s_j) s_{j+2} = 0$ for every odd $-1 \le j \le m-2$,

The proof is based on equations (8) and (9). For the only-if-direction (where we start with $P(q) = 0$) we must have $\ell_j + \gamma_j \cdot s_j = 0$ for all odd $j \ge 1$ by the remark after (9). From this and Claim 1 one can easily deduce properties (a)–(c). Vice versa, from (a)–(c) one can show Claim 1(A) by induction over $j \ge 0$. For this one proves simultaneously over j the following auxiliary statements:

(C) $\text{carry}(c_j) = q^{c_j} r_{j-1}/s_{j-1}$ for even $j \in [0, m-1]$,
(D) $\text{carry}(c_j) = q^{c_{j-1}}(p_{j-1} + r_{j-2}/s_{j-2})$ for odd $j \in [1, m]$.
Claim 1(B) then follows directly from (c) (for $j = m-2$) and (D) (for $j = m$). Full details can be found in the long version [30]. ◀

4 Knapsack for BS(1,q)

Whether the knapsack problem is decidable for $\mathrm{BS}(1,q)$ was left open in [9]. Our second main result gives a positive answer and also settles the computational complexity:

▶ **Theorem 4.1.** *For every $q \geq 2$, $\textsc{Knapsack}(\mathrm{BS}(1,q))$ is* NP*-complete.*

Let us first remark that $\mathrm{BS}(1,q)$ is unusual in terms of its knapsack solution sets. In almost all groups where knapsack is known to be decidable, knapsack equations have semilinear solution sets [11, 12, 15, 23, 26, 29]. After the discrete Heisenberg group [23], the groups $\mathrm{BS}(1,q)$ are only the second known example where this is not the case: The knapsack equation $t^{-x_1}a^{x_2}t^{x_3} = a$ has the non-semilinear solution set $\{(k, q^k, k) \mid k \in \mathbb{N}\}$.

Another unusual aspect is that knapsack is in NP although there are knapsack equations over $\mathrm{BS}(1,2)$ whose solutions are all at least doubly exponential in the size of the equation:

▶ **Theorem 4.2.** *There is a family $E_k = E_k(x,y,z)$, $k \geq 1$, of solvable knapsack expressions over $\mathrm{BS}(1,2)$ such that $|E_k| = \Theta(k)$ and $z \geq (2^{2\cdot 3^{k-1}} - 1)/3^k - 1$ for every solution of $E_k = 1$.*

Proof. It is a well-known fact in elementary number theory that 2 is a primitive root modulo 3^k for every $k \geq 1$. See, for example, Theorem 3.6 and the remarks before Theorem 3.8 in [34]. Consider the knapsack equation

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^x \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^{-1} & 0 \\ 0 & 1 \end{pmatrix}^y \begin{pmatrix} 1 & -3^k \\ 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & 3^k+1 \\ 0 & 1 \end{pmatrix} \tag{10}$$

in $\mathrm{BS}(1,2)$. In the top-left entry, it implies $2^x 2^{-y} = 2^0$. Therefore, we must have $x = y$ in every solution. In this case, the left-hand side of Equation (10) is

$$\begin{pmatrix} 2^x & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^{-x} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -z3^k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2^x - z\cdot 3^k \\ 0 & 1 \end{pmatrix}.$$

Therefore, Equation (10) is equivalent to $x = y$ and $2^x - z\cdot 3^k = 3^k + 1$. Since some non-zero power of 2 is congruent to 1 modulo 3^k, Equation (10) has a solution. Moreover, any solution must satisfy $2^x \equiv 1 \pmod{3^k}$. Since 2 is a primitive root modulo 3^k, i.e., 2 generates the group $(\mathbb{Z}/3^k\mathbb{Z})^*$ (the group of units of $\mathbb{Z}/3^k\mathbb{Z}$), x must be a multiple of $|(\mathbb{Z}/3^k\mathbb{Z})^*| = \varphi(3^k) = 2\cdot 3^{k-1}$ (here, φ is Euler's phi-function). Moreover, x must be non-zero, because $1 - z\cdot 3^k = 3^k + 1$ is not possible for $z \in \mathbb{N}$. We obtain $x \geq 2\cdot 3^{k-1}$. Since $2^x - z\cdot 3^k = 3^k + 1$, this yields $z = (2^x - 3^k - 1))/3^k \geq (2^{2\cdot 3^{k-1}} - 1)/3^k - 1$. ◀

▶ Remark 4.3. Subject to Artin's conjecture on primitive roots [20], a similar doubly-exponential lower bound results for every $\mathrm{BS}(1,q)$ where $q \geq 2$ is not a perfect square. Moreover, Theorem 4.2 holds even if the variables x, y, z range over $\mathbb{Z}$. For this, one replaces $3^k + 1$ with the inverse of 2 in $(\mathbb{Z}/3^k\mathbb{Z})^*$.

Theorem 4.2 rules out a simple guess-and-verify strategy to show Theorem 4.1. If one has an exponential upper bound (in terms of input length) on the size of a smallest solution of a knapsack equation, then one can guess the binary representation of a solution and verify, using the power word problem, whether the guess is indeed a solution. The second step (verification of a solution using the power word problem) would work for $\mathrm{BS}(1,q)$ in polynomial time due to Theorem 3.1, but the first step (guessing a binary encoded candidate for a solution) does not work for $\mathrm{BS}(1,2)$ due to Theorem 4.2.

Our main tool for the proof of Theorem 4.1 is a recent result from [17] concerning the existential fragment of Büchi arithmetic.

Büchi arithmetic. *Büchi arithmetic* [7] is the first-order theory of $(\mathbb{Z},+,\geq,0,V_q)$. Here, V_q is the function that maps $n \in \mathbb{Z}$ to the largest power of q that divides n. It is well-known that Büchi arithmetic is decidable (this was first claimed in [7]; a correct proof was given in [5]). We will rely on the following recent result of Guépin, Haase, and Worrell [17]:

▶ **Theorem 4.4** (c.f. [17]). *The existential fragment of Büchi arithmetic belongs to* NP. [2]

We will also make use of the following simple lemma:

▶ **Lemma 4.5.** *Given the q-ary representation of a number $r \in \mathbb{Z}[1/q]$ we can construct in polynomial time an existential Presburger formula over $(\mathbb{Z},+)$ of size $\mathcal{O}(\|r\|_q)$ which expresses $y = r \cdot x$ for $x, y \in \mathbb{Z}$.*

Proof. Let $r = \sum_{-k \leq i \leq \ell} a_i q^i$ with $k, \ell \geq 0$ and $0 \leq a_i < q$ for $-k \leq i \leq \ell$. We have $y = rx$ if and only if $q^k y = r' x$ for $r' = \sum_{i=0}^{k+\ell} a_{i-k} q^i \in \mathbb{Z}$. Using iterated multiplication with the constant q (which can be replaced by addition) we can easily define from x and y the integers $q^k y$ and $r'x$ by Presburger formulas of size $\mathcal{O}(k+\ell) = \mathcal{O}(\|r\|_q)$. ◀

Proof of Theorem 4.1. We start with the lower bound. The *multisubset sum problem* asks for integers $a_1, \ldots, a_d, b \in \mathbb{Z}$ given in binary, whether there exist natural numbers $x_1, \ldots, x_d \geq 0$ with $x_1 a_1 + \cdots + x_d a_d = b$. It is known to be NP-complete [18]. Since the knapsack equation

$$\begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix}^{x_1} \cdots \begin{pmatrix} 1 & a_d \\ 0 & 1 \end{pmatrix}^{x_d} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

is equivalent to $x_1 a_1 + \cdots + x_d a_d = b$, we obtain NP-hardness of knapsack over $\mathrm{BS}(1,q)$. Note that computing the q-ary representation of a_i from the binary representation is possible in logspace (even in TC^0).

For the upper bound we reduce $\textsc{Knapsack}(\mathrm{BS}(1,q))$ to the existential fragment of Büchi arithmetic, which belongs to NP by Theorem 4.4. We proceed in three steps.

Step 1: Expressing M_g and M_g^* using S_ℓ. We first express a particular set of binary relations using existential first-order formulas over $(\mathbb{Z},+,\geq,0,V_q,(S_\ell)_{\ell\in\mathbb{Z}})$. Here, for $\ell \in \mathbb{Z}$, S_ℓ is the binary predicate with

$$xS_\ell y \iff \exists r \in \mathbb{N}\ \exists s \in \mathbb{N} \colon x = q^r \wedge y = q^{r+\ell\cdot s}.$$

Let $T_{\mathbb{Z}}(q)$ denote the subset of matrices in $T(q)$ that have entries in $\mathbb{Z}$. We represent the matrix $\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right) \in T_{\mathbb{Z}}(q)$ by the pair $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ (note that we must have $m \in \mathbb{N}$). Observe that we can define the set of pairs $(m,n) \in \mathbb{Z}$ such that $\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right) \in T_{\mathbb{Z}}(q)$, because this is equivalent to m being a power of q, which is expressed by $1S_1m$.

[2] The paper [17] shows an NP upper bound for the structure $(\mathbb{N},+,0,V_q)$, but an existential sentence over the structure $(\mathbb{Z},+,\geq,0,V_q)$ easily translates into one over $(\mathbb{N},+,0,V_q)$.

A key trick is to express solvability of a knapsack equation $g_1^{x_1} \cdots g_d^{x_d} = g$ without introducing variables in the logic for $x_1, \ldots, x_d$. Instead, we employ the binary relations M_g and M_g^* on $T_{\mathbb{Z}}(q)$, which allow us to express existence of powers implicitly. For $g \in T(q)$ and $x, y \in T_{\mathbb{Z}}(q)$, we have:

- $x M_g y \iff y = xg$,
- $x M_g^* y \iff \exists s \in \mathbb{N}\colon y = xg^s$.

We construct existential formulas of size polynomial in $\|g\|$ over $(\mathbb{Z}, +, \geq, 0, V_q, (S_\ell)_{\ell \in \mathbb{Z}})$, which define the relations M_g and M_g^*. Let $g = \begin{pmatrix} q^\ell & v \\ 0 & 1 \end{pmatrix}$.

Note that the relation M_g is easily expressible because we can express multiplication with q^ℓ and v by Presburger formulas of length $\|g\|$, see Lemma 4.5. We now focus on the relations M_g^*. Observe that for $\ell \neq 0$, we have

$$\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q^\ell & v \\ 0 & 1 \end{pmatrix}^s = \begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q^{\ell s} & v + q^\ell v + \cdots + q^{(s-1)\ell} v \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} q^{\ell s} & v\frac{q^{\ell s}-1}{q^\ell - 1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} q^{k+\ell s} & u + v\frac{q^{k+\ell s}-q^k}{q^\ell - 1} \\ 0 & 1 \end{pmatrix}.$$

Therefore, $\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} M_g^* \begin{pmatrix} q^m & w \\ 0 & 1 \end{pmatrix}$ is equivalent to

$$\exists x \in \mathbb{Z}\ \exists s \in \mathbb{N}\colon q^m = q^{k+\ell s} \wedge w = u + vx \wedge (q^\ell - 1)x = q^m - q^k.$$

Here, we can quantify x over $\mathbb{Z}$, because $\frac{q^{k+\ell s}-q^k}{q^\ell - 1}$ is always an integer. Note that since we can express multiplication with v and q^ℓ by Presburger formulas of size $\mathcal{O}(\|g\|)$ (Lemma 4.5), we can also express $w = u + vx$ and $(q^\ell - 1)x = q^m - q^k$ by formulas of size $\mathcal{O}(\|g\|)$. Finally, we can express $\exists s \in \mathbb{N}\colon q^m = q^{k+\ell s}$ using $q^k S_\ell q^m$.

It remains to express $\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} M_g^* \begin{pmatrix} q^m & w \\ 0 & 1 \end{pmatrix}$ in the case $\ell = 0$. Note that $g^s = \begin{pmatrix} 1 & sv \\ 0 & 1 \end{pmatrix}$ in this case. Therefore, we have $\begin{pmatrix} q^k & u \\ 0 & 1 \end{pmatrix} M_g^* \begin{pmatrix} q^m & w \\ 0 & 1 \end{pmatrix}$ if and only if (i) there exists $s \in \mathbb{N}$ with $w = u + q^k \cdot s \cdot v$ and (ii) $q^m = q^k$. Note that condition (i) is equivalent to $\exists t \in \mathbb{N}\colon V_q(t) \geq q^k \wedge w = u + v \cdot t$. This is because choosing $t = q^k \cdot s$ yields (i). By Lemma 4.5, $w = u + v \cdot t$ can be expressed by a formula of size $\mathcal{O}(\|g\|)$.

Step 2: Expressing S_ℓ using V_q. In our second step, we show that the binary relations M_g and M_g^* can be expressed using existential formulas over $(\mathbb{Z}, +, \geq, 0, V_q)$ of size $\mathrm{poly}(\|g\|)$. As shown above, for this it suffices to define S_ℓ by an existential formula over $(\mathbb{Z}, +, \geq, 0, V_q)$ of size $\mathrm{poly}(\ell)$ (note that the relations S_ℓ occur only positively in the formulas from Step 1). For $m \in \mathbb{N}$, let P_m be the predicate where $P_m(x)$ states that x is a power of m. We first claim that for each $\ell \geq 0$, we can express P_{q^ℓ} using an existential formula of size polynomial in ℓ over $(\mathbb{Z}, +, \geq, 0, V_q)$. The case $\ell = 0$ is clear and $P_q(x)$ is just $V_q(x) = x$. The following observation is from the proof of Proposition 7.1 in [6].

▶ **Fact 4.6.** *For all $\ell \geq 1$, $P_{q^\ell}(x)$ if and only if $P_q(x)$ and $q^\ell - 1$ divides $x - 1$.*

Proof. If x is a power of q^ℓ, then $x = q^{\ell \cdot s}$ for some $s \geq 0$. So, x is a power of q. Moreover, $(x-1)/(q^\ell - 1) = (q^{\ell \cdot s} - 1)/(q^\ell - 1) = \sum_{i=0}^{s-1} q^{i\ell}$ is an integer.

Conversely, suppose x is a power of q and $q^\ell - 1$ divides $x - 1$. Write $x = q^{\ell \cdot s + r}$ with $0 \leq r < \ell$. Observe that $x - 1 = q^{s\ell + r} - 1 = q^r(q^{s\ell} - 1) + (q^r - 1)$. Since $q^\ell - 1$ divides $x - 1$ as well as $q^{s\ell} - 1$, we conclude that $q^\ell - 1$ divides $q^r - 1$. As $0 \leq r < \ell$, this is only possible with $r = 0$. This shows the above fact. ◀

Using the predicates P_{q^ℓ}, we can now express S_ℓ. Note that for $\ell \geq 0$, we have $xS_\ell y$ if and only if $y \geq x \wedge \bigvee_{i=0}^{\ell-1} P_{q^\ell}(q^i x) \wedge P_{q^\ell}(q^i y)$. Furthermore, for $\ell < 0$, we have $xS_\ell y$ if and only if $yS_{|\ell|}x$. Therefore, we can express each S_ℓ using an existential formula of size polynomial in ℓ over $(\mathbb{Z}, +, \geq, 0, V_q)$. Hence, we can express M_g and M_g^* using existential formulas of size poly($\|g\|$) over $(\mathbb{Z}, +, \geq, 0, V_q)$.

Step 3: Expressing solvability of knapsack. In the last step, we express solvability of a knapsack equation by an existential first-order sentence over $(\mathbb{Z}, +, \geq, 0, V_q)$, using the predicates M_g and M_g^*. We claim that $g_1^{x_1} \cdots g_d^{x_d} = g$ has a solution $(x_1, \dots, x_d) \in \mathbb{N}^d$ if and only if there exist $h_0, \dots, h_d \in T_\mathbb{Z}(q)$ with

$$h_0 M_{g_1}^* h_1 \;\wedge\; h_1 M_{g_2}^* h_2 \;\wedge \cdots \wedge\; h_{d-1} M_{g_d}^* h_d \;\wedge\; h_0 M_g h_d. \tag{11}$$

Clearly, the claim implies that solvability of knapsack equations can be expressed in existential first-order logic over $(\mathbb{Z}, +, \geq, 0, V_q)$.

If such $h_0, \dots, h_d$ exist, then for some $x_1, \dots, x_d \in \mathbb{N}$, we have $h_i = h_{i-1} g_i^{x_i}$ and $h_d = h_0 g$, which implies $g_1^{x_1} \cdots g_d^{x_d} = g$. For the converse, we observe that for each matrix $A \in T(q)$, there is some large enough $k \in \mathbb{N}$ such that $\begin{pmatrix} q^k & 0 \\ 0 & 1 \end{pmatrix} A$ has integer entries. Therefore, if $g_1^{x_1} \cdots g_d^{x_d} = g$, then there is some large enough $k \in \mathbb{N}$ so that for every $i = 1, \dots, d$, the matrix $\begin{pmatrix} q^k & 0 \\ 0 & 1 \end{pmatrix} g_1^{x_1} \cdots g_i^{x_i}$ has integer entries. With this, we set $h_0 = \begin{pmatrix} q^k & 0 \\ 0 & 1 \end{pmatrix}$ and $h_i = h_{i-1} g_i^{x_i}$ for $i = 1, \dots, d$. Then we have $h_0, \dots, h_d \in T_\mathbb{Z}(q)$ and Equation (11) is satisfied. ◀

5 Open problems

Several open problems arise from our work:

- What is the complexity/decidability status of the power word/knapsack problem for Baumslag-Solitar groups $\mathrm{BS}(p,q) = \langle a, t \mid ta^pt^{-1} = a^q \rangle$ for $p > 1$? Decidability of knapsack in case $\gcd(p,q) = 1$ was shown in [9], but the complexity as well as the decidability in case $\gcd(p,q) > 1$ are open. Since the word problem for $\mathrm{BS}(p,q)$ can be solved in logspace [38], one can easily show that the power word problem for $\mathrm{BS}(p,q)$ belongs to PSPACE. By using techniques from [27] one might try to find a logspace reduction from the power word problem for $\mathrm{BS}(p,q)$ to the word problem for $\mathrm{BS}(p,q)$ (the same was done for a free group in [27]); this would show that the power word problem for $\mathrm{BS}(p,q)$ can be solved in logspace.
- Baumslag-Solitar groups $\mathrm{BS}(1,q)$ are examples of f.g. solvable linear groups. In [22] it was shown that for every f.g. solvable linear group the word problem can be solved in TC^0. This leads to the question whether for every f.g. solvable linear group the power word problem belongs to TC^0.
- The power word problem is a restriction of the compressed word problem, where it is asked whether the word produced by a so-called straight-line program (a context-free grammar that produces a single word) represents the group identity; see [25]. The compressed word problem for $\mathrm{BS}(1,q)$ belongs to coRP (the complement of randomized polynomial time); this holds in fact for every f.g. linear group [25]. No better complexity bound is known for the compressed word problem for $\mathrm{BS}(1,q)$.
- Let us define an exponent expression over a f.g. group $G = \langle \Sigma \rangle$ as a formal expression $E = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_d^{x_d} v_d$ with $d \geq 1$, words $v_0, \dots, v_d \in \Sigma^*$, non-empty words $u_1, \dots, u_d \in \Sigma^*$, and variables $x_1, \dots, x_d$. In contrast to knapsack expressions, we allow $x_i = x_j$ for $i \neq j$ in an exponent expression. The set of solutions $\mathrm{sol}_G(E)$ for the exponent expression

E can be defined analogously to knapsack expressions. We define *solvability of exponent equations over* G, $\textsc{ExpEq}(G)$ for short, as the following decision problem:

Input A finite list of exponent expressions $E_1, \ldots, E_n$ over G.

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

This problem has been studied for various groups [11, 15, 26, 29]. Our algorithm for the knapsack problem in $\mathrm{BS}(1, q)$ cannot be extended to solvability of exponent equations (not even to solvability of a single exponent equation). Recently, it has been shown that the Diophantine theory (or, equivalently, solvability of systems of word equations) is decidable for $\mathrm{BS}(1, q)$ [21]. Since every element of $\mathrm{BS}(1, q)$ can be written in the form $t^x a^y t^z$ for $x, y, z \in \mathbb{Z}$, one can easily reduce the Diophantine theory of $\mathrm{BS}(1, q)$ to solvability of exponent equations for $\mathrm{BS}(1, q)$. But it is not clear at all, whether a reduction in the opposite direction exists as well.

References

1 Eric Allender, Nikhil Balaji, and Samir Datta. Low-depth uniform threshold circuits and the bit-complexity of straight line programs. In *Proceedings of the 39th International Symposium on Mathematical Foundations of Computer Science 2014, MFCS 2014*, volume 8635 of *Lecture Notes in Computer Science*, pages 13–24. Springer, 2014.

2 Lázló Babai, Robert Beals, Jin yi Cai, Gábor Ivanyos, and Eugene M.Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 1996*, pages 498–507. ACM/SIAM, 1996.

3 Laurent Bartholdi, Michael Figelius, Markus Lohrey, and Armin Weiß. Groups with ALOGTIME-hard word problems and PSPACE-complete compressed word problems. *CoRR*, abs/1909.13781, 2019. URL: `https://arxiv.org/abs/1909.13781`.

4 Gilbert Baumslag. Wreath products and finitely presented groups. *Mathematische Zeitschrift*, 75(1):22–28, 1961.

5 Véronique Bruyère. Entiers et automates finis. Mémoire de fin d'études, Université de Mons, 1985.

6 Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and p-recognizable sets of integers. *Bulletin of the Belgian Mathematical Society*, 1:191–238, 1994.

7 J Richard Büchi. Weak second-order arithmetic and finite automata. *Mathematical Logic Quarterly*, 6(1-6):66–92, 1960.

8 Jin-Yi Cai, Richard J. Lipton, and Yechezkel Zalcstein. The complexity of the A B C problem. *SIAM Journal on Computing*, 29(6):1878–1888, 2000.

9 Fedor Dudkin and Alexander Treyer. Knapsack problem for Baumslag–Solitar groups. *Siberian Journal of Pure and Applied Mathematics*, 18:43–55, 2018.

10 Wayne Eberly. Very fast parallel polynomial arithmetic. *SIAM Journal on Computing*, 18(5):955–976, 1989.

11 Michael Figelius, Moses Ganardi, Markus Lohrey, and Georg Zetzsche. The complexity of knapsack problems in wreath products. In *Proceedings of the 47th International Colloquium on Automata, Languages, and Programming, ICALP 2020*, volume 168 of *LIPIcs*, pages 126:1–126:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

12 Michael Figelius, Markus Lohrey, and Georg Zetzsche. Closure properties of knapsack semilinear groups. *CoRR*, abs/1911.12857, 2019. URL: `https://arxiv.org/abs/1911.12857`.

13 Elizaveta Frenkel, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016.

14 Esther Galby, Joël Ouaknine, and James Worrell. On matrix powering in low dimensions. In *Proceedings of the 32nd International Symposium on Theoretical Aspects of Computer Science, STACS 2015*, volume 30 of *LIPIcs*, pages 329–340. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.

15 Moses Ganardi, Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack problems for wreath products. In *Proceedings of the 35th Symposium on Theoretical Aspects of Computer Science, STACS 2018*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

16 Guoqiang Ge. Testing equalities of multiplicative representations in polynomial time (extended abstract). In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science, FOCS 1993*, pages 422–426. IEEE Computer Society, 1993.

17 Florent Guépin, Christoph Haase, and James Worrell. On the existential theories of Büchi arithmetic and linear p-adic fields. In *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019*, pages 1–10. IEEE Computer Society, 2019.

18 Christoph Haase. *On the complexity of model checking counter automata*. PhD thesis, University of Oxford, St Catherine's College, 2011.

19 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(4):695–716, 2002.

20 Christopher Hooley. On Artin's conjecture. *Journal für die reine und angewandte Mathematik*, 1967(225):209–220, 1967.

21 Olga Kharlampovich, Laura López, and Alexei Myasnikov. The diophantine problem in some metabelian groups. *Mathematics of Computation*, 89:2507–2519, 2020.

22 Daniel König and Markus Lohrey. Evaluation of circuits over nilpotent and polycyclic groups. *Algorithmica*, 80(5):1459–1492, 2018.

23 Daniel König, Markus Lohrey, and Georg Zetzsche. 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.

24 Klaus-Jörn Lange and Pierre McKenzie. On the complexity of free monoid morphisms. In *Proceedings of the 9th International Symposium on Algorithms and Computation, ISAAC 1998*, number 1533 in Lecture Notes in Computer Science, pages 247–256. Springer, 1998.

25 Markus Lohrey. *The Compressed Word Problem for Groups*. SpringerBriefs in Mathematics. Springer, 2014.

26 Markus Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020.

27 Markus Lohrey and Armin Weiß. The power word problem. In *Proceedings of the 44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019*, volume 138 of *LIPIcs*, pages 43:1–43:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

28 Markus Lohrey and Armin Weiß. The power word problem. *CoRR*, abs/1904.08343, 2019. URL: `http://arxiv.org/abs/1904.08343`.

29 Markus Lohrey and Georg Zetzsche. Knapsack in graph groups. *Theory of Computing Systems*, 62(1):192–246, 2018.

30 Markus Lohrey and Georg Zetzsche. Knapsack and the power word problem in solvable Baumslag-Solitar groups. *CoRR*, abs/2002.03837, 2020. URL: `https://arxiv.org/abs/2002.03837`.

31 Alexei Miasnikov, Vitaly Roman'kov, Alexander Ushakov, and Anatoly Vershik. The word and geodesic problems in free solvable groups. *Transactions of the American Mathematical Society*, 362(9):4655–4682, 2010.

32 Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87, 2017.

33 Alexei Myasnikov, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015.

34 Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Springer, 2000.

35 David Robinson. *Parallel Algorithms for Group Word Problems*. PhD thesis, University of California, San Diego, 1993.

36 Heribert Vollmer. *Introduction to Circuit Complexity*. Springer, 1999.

37 Armin Weiß. *On the complexity of conjugacy in amalgamated products and HNN extensions*. PhD thesis, University of Stuttgart, 2015. URL: http://elib.uni-stuttgart.de/opus/volltexte/2015/10018/.

38 Armin Weiß. A logspace solution to the word and conjugacy problem of generalized Baumslag-Solitar groups. *CoRR*, abs/1602.02445, 2016. URL: https://arxiv.org/abs/1602.02445.

39 Wolfgang Woess. *Random Walks on Infinite Graphs and Groups*. Cambridge University Press, 2000.