The Complexity of Knapsack in Graph Groups

Markus Lohrey[1] **and Georg Zetzsche**[*2]

1 **Universität Siegen, Germany**
`lohrey@eti.uni-siegen.de`
2 **LSV, CNRS & ENS Cachan, Université Paris-Saclay, France**
`zetzsche@lsv.fr`

Abstract

Myasnikov et al. have introduced the knapsack problem for arbitrary finitely generated groups. In [17] the authors proved that for each graph group, the knapsack problem can be solved in NP. Here, we determine the exact complexity of the problem for every graph group. While the problem is TC^0-complete for complete graphs, it is LogCFL-complete for each (non-complete) transitive forest. For every remaining graph, the problem is NP-complete.

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

In their paper [19], Myasnikov, Nikolaev, and Ushakov started the investigation of classical discrete optimization problems, which are classically formulated over the integers, for arbitrary (possibly non-commutative) groups. The general goal of this line of research is to study to what extent results from the classical commutative setting can be transferred to the non-commutative setting. Among other problems, Myasnikov et al. introduced for a finitely generated group G the *knapsack problem* and the *subset sum problem*. The input for the knapsack problem is a sequence of group elements $g_1, \ldots, g_k, g \in G$ (specified by finite words over the generators of G) and it is asked whether there exists a solution $(x_1, \ldots, x_k) \in \mathbb{N}^k$ of the equation $g_1^{x_1} \cdots g_k^{x_k} = g$. For the subset sum problem one restricts the solution to $\{0,1\}^k$. For the particular case $G = \mathbb{Z}$ (where the additive notation $x_1 \cdot g_1 + \cdots + x_k \cdot g_k = g$ is usually preferred) these problems are NP-complete if the numbers $g_1, \ldots, g_k, g$ are encoded in binary representation. For subset sum, this is a classical result from Karp's seminal paper [14] on NP-completeness. Knapsack for integers is usually formulated in a more general form in the literature; NP-completeness of the above form (for binary encoded integers) was shown in [10], where the problem was called MULTISUBSET SUM.[1] Interestingly, if we consider subset sum for the group $G = \mathbb{Z}$, but encode the input numbers $g_1, \ldots, g_k, g$ in unary notation, then the problem is in DLOGTIME-uniform TC^0 (a small subclass of polynomial time and even of logarithmic space that captures the complexity of multiplication of binary encoded numbers; see e.g. the book [23] for more details) [5], and the same holds for knapsack (see Theorem 4.1). Related results can be found in [12].

In [19] the authors encode elements of the finitely generated group G by words over the group generators and their inverses, which corresponds to the unary encoding of integers. Another, more succinct encoding of group elements uses *straight-line programs* (SLP). These are context-free grammars that produce a single word. Over a unary alphabet, one can

* This author is supported by a fellowship within the Postdoc-Program of the German Academic Exchange Service (DAAD).

[1] Note that if we ask for a solution $(x_1, \ldots, x_k)$ in $\mathbb{Z}^k$, then knapsack can be solved in polynomial time (even for binary encoded integers) by checking whether $\gcd(g_1, \ldots, g_k)$ divides g.

achieve for every word exponential compression with SLPs: The word a^n can be produced by an SLP of size $O(\log n)$. This shows that knapsack and subset sum for the group $\mathbb{Z}$ with SLP-compressed group elements correspond to the classical knapsack and subset sum problem with binary encoded numbers. To distinguish between the two variants, we will speak in this introduction of uncompressed knapsack (resp., subset sum) if the input group elements are given explicitly by words over the generators. On the other hand, if these words are represented by SLPs, we will speak of SLP-compressed knapsack (resp., subset sum). Later in this paper, we will only use the uncompressed versions, and denote these simply with knapsack and subset sum.

In our recent paper [17], we started to investigate knapsack and subset sum for graph groups, which are also known as right-angled Artin groups in group theory. A graph group is specified by a finite simple graph Γ and denoted with $\mathbb{G}(\Gamma)$. The vertices are the generators of the group, and two generators a and b are allowed to commute if and only if a and b are adjacent in Γ. Graph groups interpolate between free groups and free abelian groups and can be seen as a group counterpart of trace monoids (free partially commutative monoids), which have been used for the specification of concurrent behavior. In combinatorial group theory, graph groups are currently an active area of research, mainly because of their rich subgroup structure, see e.g. [3, 4, 7].

Contribution. In [17] the authors proved that for every graph group, SLP-compressed knapsack (resp., subset sum) is NP-complete. This result generalizes the classical result for knapsack with binary encoded integers. Moreover, we proved that uncompressed knapsack and subset sum are NP-complete for the group $F_2 \times F_2$ (F_2 is the free group on two generators). The group $F_2 \times F_2$ is the graph group $\mathbb{G}(\Gamma)$, where the graph Γ is a cycle on four nodes. This result leaves open the complexity of uncompressed knapsack (and subset sum) for graph groups, whose underlying graph does not contain an induced cycle on four nodes. In this paper, we completely settle this open problem by showing the following results:

(i) Uncompressed knapsack and subset sum for $\mathbb{G}(\Gamma)$ are complete for TC^0 if Γ is a complete graph (and thus $\mathbb{G}(\Gamma)$ is a free abelian group).[2]
(ii) Uncompressed knapsack and subset sum for $\mathbb{G}(\Gamma)$ are LogCFL-complete if Γ is not a complete graph and neither contains an induced cycle on four nodes (C4) nor an induced path on four nodes (P4).
(iii) Uncompressed knapsack for $\mathbb{G}(\Gamma)$ is NP-complete if Γ contains an induced C4 or an induced P4.

Overview of the proofs. The result (i) is a straightforward extension of the corresponding result for $\mathbb{Z}$ [5]. The statements in (ii) and (iii) are less obvious. Recall that LogCFL is the closure of the context-free languages under logspace reductions; it is contained in NC^2.

To show the upper bound in (ii), we use the fact that the graph groups $\mathbb{G}(\Gamma)$, where Γ neither contains an induced C4 nor an induced P4 (these graphs are the so called transitive forests), are exactly those groups that can be built up from $\mathbb{Z}$ using the operations of free product and direct product with $\mathbb{Z}$. We then construct inductively over these operations a logspace-bounded auxiliary pushdown automaton working in polynomial time (these machines accept exactly the languages in LogCFL) that checks whether an acyclic finite automaton accepts a word that is trivial in the graph group. In order to apply this result to knapsack,

[2] In the following, TC^0 always refers to its DLOGTIME-uniform version.

we finally show that every solvable knapsack instance over a graph group $\mathbb{G}(\Gamma)$ with Γ a transitive forest has a solution with polynomially bounded exponents. This result might be of independent interest.

For the lower bound in (ii), it suffices to consider the group F_2 (the free group on two generators). Our proof is based on the fact that the context-free languages are exactly those languages that can be accepted by valence automata over F_2. This is a reinterpretation of the classical theorem of Chomsky and Schützenberger. To the authors' knowledge, the result (ii) is the first completeness result for LogCFL in the area of combinatorial group theory.

Finally, for the result (iii) it suffices to show NP-hardness of knapsack for the graph group $\mathbb{G}(\mathsf{P4})$ (the NP upper bound and the lower bound for C4 is shown in [17]). We apply a technique that was first used in a paper by Aalbersberg and Hoogeboom [1] to show that the intersection non-emptiness problem for regular trace languages is undecidable for P4.

2 Knapsack and Exponent Equations

We assume that the reader has some basic knowledge concerning (finitely generated) groups (see e.g. [18] for further details). Let G be a finitely generated group, and let A be a finite generating set for G. Then, elements of G can be represented by finite words over the alphabet $A^{\pm 1} = A \cup A^{-1}$. An *exponent equation* over G is an equation of the form

$$h_0 g_1^{\mathsf{x}_1} h_1 g_2^{\mathsf{x}_2} h_2 \cdots g_k^{\mathsf{x}_k} h_k = 1$$

where $g_1, g_2, \ldots, g_k, h_0, h_1, \ldots, h_k \in G$ are group elements that are given by finite words over the alphabet $A^{\pm 1}$ and $\mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_k$ are not necessarily distinct variables. Such an exponent equation is *solvable* if there exists a mapping $\sigma\colon \{\mathsf{x}_1, \ldots, \mathsf{x}_k\} \to \mathbb{N}$ such that $h_0 g_1^{\sigma(\mathsf{x}_1)} h_1 g_1^{\sigma(\mathsf{x}_2)} h_2 \cdots g_k^{\sigma(\mathsf{x}_k)} h_k = 1$ in the group G. The *size* of an equation is $\sum_{i=0}^{k} |h_i| + \sum_{i=1}^{k} |g_i|$, where $|g|$ denotes the length of the shortest word $w \in (A^{\pm 1})^*$ representing g. *Solvability of exponent equations over* G is the following computational problem:

Input: An exponent equation E over G (where elements of G are specified by words over the group generators and their inverses).

Question: Is E solvable?

The *knapsack problem* for the group G is the restriction of solvability of exponent equations over G to exponent equations of the form $g_1^{\mathsf{x}_1} g_2^{\mathsf{x}_2} \cdots g_k^{\mathsf{x}_k} g^{-1} = 1$ or, equivalently, $g_1^{\mathsf{x}_1} g_2^{\mathsf{x}_2} \cdots g_k^{\mathsf{x}_k} = g$ where the exponent variables $\mathsf{x}_1, \ldots, \mathsf{x}_k$ have to be pairwise different. The *subset sum problem* for the group G is defined in the same way as the knapsack problem, but the exponent variables $\mathsf{x}_1, \ldots, \mathsf{x}_k$ have to take values in $\{0, 1\}$.

It is a simple observation that the decidability and complexity of solvability of exponent equations over G as well as the knapsack problem and subset sum problem for G does not depend on the chosen finite generating set for the group G. Therefore, we do not have to mention the generating set explicitly in these problems.

▶ Remark. Since we are dealing with a group, one might also allow solution mappings $\sigma\colon \{\mathsf{x}_1, \ldots, \mathsf{x}_k\} \to \mathbb{Z}$ to the integers. This variant of solvability of (compressed) exponent equations (knapsack, respectively) can be reduced to the above version, where σ maps to $\mathbb{N}$, by simply replacing a power $g_i^{\mathsf{x}_i}$ by $g_i^{\mathsf{x}_i} (g_i^{-1})^{\mathsf{y}_i}$, where y_i is a fresh variable.

3 Traces and Graph Groups

Let (A, I) be a finite simple graph. In other words, the edge relation $I \subseteq A \times A$ is irreflexive and symmetric. It is also called the *independence relation*, and (A, I) is called an

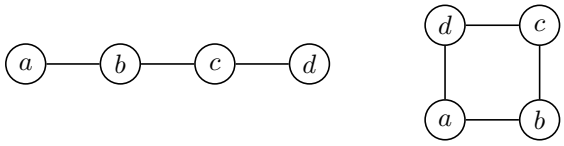

Figure 1 P4 and C4

independence alphabet. Symbols $a, b \in A$ are called dependent if $(a, b) \notin I$. We consider the monoid $\mathbb{M}(A, I) = A^*/\equiv_I$, where $\equiv_I$ is the smallest congruence relation on the free monoid A^* that contains all pairs (ab, ba) with $a, b \in A$ and $(a, b) \in I$. This monoid is called a *trace monoid* or *partially commutative free monoid*. Elements of $\mathbb{M}(A, I)$ are called *Mazurkiewicz traces* or simply *traces*. The trace represented by the word u is denoted by $[u]_i$, or simply $[u]$ if no confusion can arise. The empty trace $[\varepsilon]_I$ is the identity element of the monoid $\mathbb{M}(A, I)$ and is denoted by 1. For a language $L \subseteq A^*$ we denote with $[L]_I = \{[u]_I \in \mathbb{M}(A, I) \mid u \in L\}$ the set of traces represented by L. The length of the trace $[u]_I$ is $|[u]_I| = |u|$

Figure 1 shows two important indepedence alphabets that we denote with P4 (path on four nodes) and C4 (cycle on four nodes). Note that $\mathbb{M}(\mathsf{C4}) = \{a, c\}^* \times \{b, d\}^*$.

With an independence alphabet (A, I) we associate the finitely presented group

$$\mathbb{G}(A, I) = \langle A \mid ab = ba \ ((a, b) \in I)\rangle.$$

More explicitly, this group can be defined as follows: Let $A^{-1} = \{a^{-1} \mid a \in A\}$ be a disjoint copy of the alphabet A. We extend the independence relation I to $A^{\pm 1} = A \cup A^{-1}$ by $(a^x, b^y) \in I$ for all $(a, b) \in I$ and $x, y \in \{-1, 1\}$. Then $\mathbb{G}(A, I)$ is the quotient monoid $(A^{\pm 1})^*/\sim_I$, where $\sim_I$ is the smallest congruence relation that contains (i) all pairs (ab, ba) for $a, b \in A^{\pm 1}$ with $(a, b) \in I$ and (ii) all pairs (aa^{-1}, ε) and $(a^{-1}a, \varepsilon)$ for $a \in A$.

A group $\mathbb{G}(A, I)$ is called a *graph group*, or *right-angled Artin group*[3], or *free partially commutative group*. Here, we use the term graph group. Graph groups received a lot of attention in group theory during the last years, mainly due to their rich subgroup structure [3, 4, 7], and their relationship to low dimensional topology (via so-called virtually special groups) [2, 11, 24].

4 TC^0- and LogCFL-completeness

Let us first consider free abelian groups $\mathbb{Z}^m$. Note that $\mathbb{Z}^m$ is isomorphic to the graph group $\mathbb{G}(A, I)$ where (A, I) is the complete graph on m nodes. Our first result is a simple combination of known results [20, 5].

▶ **Theorem 4.1.** *For every fixed $m \geq 1$, knapsack and subset sum for the free abelian group $\mathbb{Z}^m$ are complete for TC^0. Hence, knapsack and subset sum for $\mathbb{G}(A, I)$ are complete for TC^0 if (A, I) is a non-empty complete graph.*

We now characterize those graph groups where knapsack for $\mathbb{G}(A, I)$ is LogCFL-complete. The class LogCFL consists of all problems that are logspace reducible to a context-free language. The *comparability graph* of a tree t is the simple graph with the same vertices as t, but has an edge between two vertices whenever one is a descendent of the other in t. A graph (A, I) is a *transitive forest* if it is a disjoint union of comparability graphs of trees.

[3] This term comes from the fact that right-angled Artin groups are exactly the Artin groups corresponding to right-angled Coxeter groups.

▶ **Theorem 4.2.** *If (A, I) is a transitive forest and not complete, then knapsack and subset sum for $\mathbb{G}(A, I)$ are* LogCFL*-complete.*

If the graph (A, I) is the disjoint union of graphs Γ_0 and Γ_1, then by definition, we have $\mathbb{G}(A, I) \cong \mathbb{G}(\Gamma_0) * \mathbb{G}(\Gamma_1)$. If one vertex v of (A, I) is adjacent to every other vertex and removing v from (A, I) results in the graph Γ_0, then $\mathbb{G}(A, I) \cong \mathbb{G}(\Gamma_0) \times \mathbb{Z}$. Therefore, we have the following *inductive characterization* of the graph groups $\mathbb{G}(A, I)$ for transitive forests (A, I): It is the smallest class of groups containing the trivial group that is closed under taking (i) free products and (ii) direct products with $\mathbb{Z}$.

Acyclic Automata In both the upper and the lower bound of our completeness result, we employ the membership problem for acyclic automata, which has already been studied in connection with the knapsack and subset sum problem [15, 6].

We define a *finite automaton* as a tuple $\mathcal{A} = (Q, \Sigma, \Delta, q_0, q_f)$, where Q is a finite set of states, Σ is the *input alphabet*, $q_0 \in Q$ is the *initial state*, $q_f \in Q$ is the *final state*, and $\Delta \subseteq Q \times \Sigma^* \times Q$ is a finite set of *transitions*. The language accepted by $\mathcal{A}$ is denoted with $L(\mathcal{A})$. An *acyclic automaton* is a finite automaton $\mathcal{A} = (Q, \Sigma, \Delta, q_0, q_f)$ such that the relation $\{(p, q) \mid \exists w \in \Sigma^* : (p, w, q) \in \Delta\}$ is acyclic. For a graph group $\mathbb{G}(A, I)$ the *membership problem for acyclic automata* is the following computational problem:

Input: An acyclic automaton $\mathcal{A}$ over the input alphabet $A \cup A^{-1}$.

Question: Is there a word $w \in L(\mathcal{A})$ such that $w = 1$ in $\mathbb{G}(A, I)$?

In order to show the upper bound in Theorem 4.2, we reduce knapsack for $\mathbb{G}(A, I)$ with (A, I) a transitive forest to the membership problem for acyclic automata for $\mathbb{G}(A, I)$ (note that for subset sum this reduction is obvious). Then, we apply the following proposition. From work of Frenkel, Nikolaev, and Ushakov [6], it follows that the membership problem for acyclic automata is in P. We strengthen this to LogCFL.

▶ **Proposition 4.3.** *If (A, I) is a transitive forest, then the membership problem for acyclic automata over $\mathbb{G}(A, I)$ is in* LogCFL*.*

The class LogCFL is included in the parallel complexity class NC^2 and has several alternative characterizations (see e.g. [22, 23]). Our proof uses the characterization via logspace bounded auxiliary pushdown automata with polynomial running time.

4.1 Bounds on knapsack solutions

As mentioned above, we reduce for graph groups $\mathbb{G}(A, I)$ with (A, I) a transitive forest the knapsack problem to the membership problem for acyclic automata. To this end, we show that every positive knapsack instance has a polynomially bounded solution. The latter is the most involved proof in our paper.

Frenkel, Nikolaev, and Ushakov [6] call groups with this property *polynomially bounded knapsack groups* and show that this class is closed under taking free products. However, it is not clear if direct products with $\mathbb{Z}$ also inherit this property and we leave this question open.

Hence, we are looking for a property that yields polynomial size solutions and is passed on to free products and to direct products with $\mathbb{Z}$. It is known that the solution sets are always semilinear. If (A, I) is a transitive forest, this follows from a more general semilinearity property of rational sets [16] and for arbitrary graph groups, this was shown in [17]. Note that it is not true that the solution sets alwas have polynomial size semilinear representations. This already fails in the case of $\mathbb{Z}$: The equation $\mathsf{x}_1 + \cdots + \mathsf{x}_k = k$ has $\binom{2k-1}{k} \geq 2^k$ solutions.

We will show here that the solution sets have semilinear representations where every occuring number is bounded by a polynomial.

For a vector $x = (x_1, \dots, x_k) \in \mathbb{Z}^k$, we define the norm $\|x\| = \max\{|x_i| \mid i \in [1,k]\}$. For a subset $T \subseteq \mathbb{N}^k$, we write $T^\oplus$ for the smallest subset of $\mathbb{N}^k$ that contains 0 and is closed under addition. A subset $S \subseteq \mathbb{N}^k$ is called *linear* if there is a vector $x \in \mathbb{N}^k$ and a finite set $F \subseteq \mathbb{N}^k$ such that $S = x + F^\oplus$. Note that a set is linear if and only if it can be written as $x + A\mathbb{N}^t$ for some $x \in \mathbb{N}^k$ and some matrix $A \in \mathbb{N}^{k\times t}$. Here, $A\mathbb{N}^t$ denotes the set of all vectors Ay for $y \in \mathbb{N}^t$. A *semilinear set* is a finite union of linear sets. If $S = \bigcup_{i=1}^n x_i + F_i^\oplus$ for $x_1, \dots, x_n \in \mathbb{N}^k$ and finite sets $F_1, \dots, F_n \subseteq \mathbb{N}^k$, then the tuple $(x_1, F_1, \dots, x_n, F_n)$ is a *semilinear representation* of S and the *magnitude* of this representation is defined as the maximum of $\|y\|$, where y ranges over all elements of $\bigcup_{i=1}^n \{x_i\} \cup F_i$. The *magnitude* of a semilinear set S is the smallest magnitude of a semilinear representation for S.

▶ **Definition 4.4.** *A group G is called* knapsack tame *if there is a polynomial p such that for every exponent equation $h_0 g_1^{\mathsf{x}_1} h_1 g_2^{\mathsf{x}_2} h_2 \cdots g_n^{\mathsf{x}_k} h_k = 1$ of size n with pairwise distinct variables $\mathsf{x}_1, \dots, \mathsf{x}_k$, the set $S \subseteq \mathbb{N}^k$ of solutions is semilinear of magnitude at most $p(n)$.*

Observe that although the size of an exponent equation may depend on the chosen generating set of G, changing the generating set increases the size only by a constant factor. Thus, whether or not a group is knapsack tame is independent of the chosen generating set.

▶ **Theorem 4.5.** *If (A, I) is a transitive forest, then $\mathbb{G}(A, I)$ is knapsack tame.*

Note that Theorem 4.5 implies in particular that every solvable exponent equation has a polynomially bounded solution. Theorem 4.5 and Proposition 4.3 easily yield the upper bound in Theorem 4.2, see Appendix C.

We prove Theorem 4.5 by showing that knapsack tameness transfers from groups G to $G \times \mathbb{Z}$ (Proposition 4.6) and from G and H to $G * H$ (Proposition 4.10). Since the trivial group is obviously knapsack tame, the inductive characterization of groups $\mathbb{G}(A, I)$ for transitive forests (A, I) immediately yields Theorem 4.5.

4.2 Tameness of direct products with $\mathbb{Z}$

In this section, we show the following.

▶ **Proposition 4.6.** *If G is knapsack tame, then so is $G \times \mathbb{Z}$.*

Linear Diophantine equations We employ a result of Pottier [21], which bounds the norm of minimal non-negative solutions to a linear Diophantine equation. Let $A \in \mathbb{Z}^{k\times m}$ be an integer matrix where a_{ij} is the entry of A at row i and column j. We will use the norms $\|A\|_{1,\infty} = \max_{i\in[1,k]}(\sum_{j\in[1,m]} |a_{ij}|)$, $\|A\|_{\infty,1} = \max_{j\in[1,m]}(\sum_{i\in[1,k]} |a_{ij}|)$ and $\|A\|_\infty = \max_{i\in[1,k],j\in[1,m]} |a_{ij}|$ for matrices and $\|x\|_1 = \sum_{i=1}^m |x_i|$ for vectors $x \in \mathbb{Z}^m$. Recall that $\|x\| = \max_{i\in[1,m]} |x_i|$. A solution $x \in \mathbb{N}^m \setminus \{0\}$ to the equation $Ax = 0$ is *minimal* if there is no $y \in \mathbb{N}^m \setminus \{0\}$ with $Ay = 0$ and $y \le x$, $y \neq x$. The set of all solutions clearly forms a submonoid of $\mathbb{N}^m$, which is denoted M. The set of minimal solutions is denoted $\mathcal{H}(M)$ and called the *Hilbert basis* of M. Let r be the rank of A.

▶ **Theorem 4.7** (Pottier [21])**.** *For each $x \in \mathcal{H}(M)$, $\|x\|_1 \le (1 + \|A\|_{1,\infty})^r$.*

By applying Theorem 4.7 to the matrix $(A \mid -b)$, it is easy to deduce that for each $x \in \mathbb{N}^m$ with $Ax = b$, there is a $y \in \mathbb{N}^m$ with $Ay = b$, $y \le x$, and $\|y\|_1 \le (1 + \|(A \mid -b)\|_{1,\infty})^{r+1}$. We reformulate Theorem 4.7 as follows.

▶ **Lemma 4.8.** *If $B \in \mathbb{Z}^{\ell\times k}$ has rank r and $b \in \mathbb{Z}^\ell$, then the set $\{x \in \mathbb{N}^k \mid Bx = b\}$ admits a decomposition $\{x \in \mathbb{N}^k \mid Bx = b\} = \bigcup_{i=1}^s c_i + C\mathbb{N}^t$, where $c_i \in \mathbb{N}^k$ and $C \in \mathbb{N}^{k\times t}$ with $\|c_i\|_1$ and $\|C\|_{\infty,1}$ bounded by $(1 + \|B\|_{1,\infty} + \|b\|)^{r+1}$.*

However, we want to apply Lemma 4.8 in a situation where we have no bound on $\|B\|_{1,\infty}$, only one on $\|B\|_\infty$. However, we will know that $\ell = 1$, which allows us to bound magnitudes in terms of $\|B\|_\infty$ in the following lemma. Then, Proposition 4.6 is straightforward.

▶ **Lemma 4.9.** *If $B \in \mathbb{Z}^{1\times k}$ and $b \in \mathbb{Z}$ with $\|B\|_\infty, |b| \leq M$, then we have a decomposition $\{x \in \mathbb{N}^k \mid Bx = b\} = \bigcup_{i=1}^s c_i + C\mathbb{N}^t$ where $\|c_i\|_1$ and $\|C\|_{\infty,1}$ are at most $(M+1)^4$.*

4.3 Tameness of free products

This section is devoted to the proof of the following proposition.

▶ **Proposition 4.10.** *If G_0 and G_1 are knapsack tame, then so is $G_0 * G_1$.*

Suppose that for $i = 0, 1$, the group G_i is a generated by A_i, where $A_i^{-1} = A_i$ and let $A = A_0 \uplus A_1$. Recall that every $g \in G$ can be written uniquely as $g = g_1 \cdots g_n$ where $g_i \in G_0$ or $g_i \in G_1$ for each $i \in [1, n]$ and where $g_j \in G_t$ iff $g_{j+1} \in G_{1-t}$ for $j \in [1, n-1]$. We call g *cyclically reduced* if for some $t \in \{0, 1\}$, either $g_1 \in G_t$ and $g_n \in G_{1-t}$ or $g_1, g_n \in G_t$ and $g_n g_1 \neq 1$. Consider an exponent equation

$$h_0 g_1^{x_1} h_1 \cdots g_k^{x_k} h_k = 1, \tag{1}$$

of size n, where g_i is represented by $u_i \in A^*$ for $i \in [1, k]$ and h_i is represented by $v_i \in A^*$ for $i \in [0, k]$. Then clearly $\sum_{i=0}^k |v_i| + \sum_{i=1}^k |u_i| \leq n$. Let $S \subseteq \mathbb{N}^k$ be the set of all solutions to (1). Every word $w \in A^*$ has a (possibly empty) unique factorization into maximal factors from $A_0^+ \cup A_1^+$, which we call *syllables*. By $\|w\|$, we denote the number of syllables of w. The word w is *reduced* if none of its syllables represents 1 (in G_0 resp. G_1). We define the maps $\lambda, \rho\colon A^+ \to A^+$ ("rotate left/right"), where for each word $w \in A^+$ with its factorization $w = w_1 \cdots w_m$ into syllables, we set $\lambda(w) = w_2 \cdots w_m w_1$ and $\rho(w) = w_m w_1 w_2 \cdots w_{m-1}$.

Consider a word $w \in A^*$ and suppose $w = w_1 \cdots w_m$, where for each $i \in [1, m]$, we have $w_i \in A_j^*$ for some $j \in \{0, 1\}$. A *cancellation* is a subset $C \subseteq 2^{[1,m]}$ that is

- *a partition*: $\bigcup_{I\in C} I = [1, m]$ and $I \cap J = \emptyset$ for any $I, J \in C$ with $I \neq J$.
- *consistent*: for each $I \in C$, there is an $i \in \{0, 1\}$ such that $w_j \in A_i^*$ for all $j \in I$.
- *cancelling*: if $\{i_1, \ldots, i_\ell\} \in C$ with $i_1 < \cdots < i_\ell$, then $w_{i_1} \cdots w_{i_\ell}$ represents 1 in G.
- *well-nested*: there are no $I, J \in C$ with $i_1, i_2 \in I$ and $j_1, j_2 \in J$ such that $i_1 < j_1 < i_2 < j_2$.

Since C can be regarded as a hypergraph on $[1, m]$, the elements of C will be called *edges*. By the definition of $G_0 * G_1$, a word w admits a cancellation if and only if it represents 1 in G.

Of course, when showing that the solution sets have a polynomial magnitude, we may assume that $g_i \neq 1$ for any $i \in [1, k]$. Moreover, we lose no generality by assuming that all words u_i, $i \in [1, k]$ and v_i, $i \in [0, k]$ are reduced. Furthermore, we may assume that each g_i is cyclically reduced. Indeed, if some g_i is not cyclically reduced, we can write $g_i = f^{-1} g f$ for some cyclically reduced g and replace h_{i-1}, g_i, and h_i by $h_{i-1} f^{-1}$, $g = f g_i f^{-1}$, and $f h_i$, respectively. This does not change the solution set because $h_{i-1} f^{-1} (f g_i f^{-1})^{x_i} f h_i = h_{i-1} g_i^{x_i} h_i$. Moreover, if we do this replacement for each g_i that is not cyclically reduced, we increase the size of the instance by at most $2|g_1| + \cdots + 2|g_k| \leq 2n$ (note that $|g| = |g_i|$). Applying this argument again, we may even assume that

$$u_i \in A_0^+ \cup A_1^+ \cup A_0^+ A^* A_1^+ \cup A_1^+ A^* A_0^+ \tag{2}$$

for every $i \in [1,k]$. Note that λ and ρ are bijections on words of this form.

Consider a solution $(x_1, \dots, x_k)$ to (1). Then the word

$$w = v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k \tag{3}$$

represents 1 in $G = G_0 * G_1$. We factorize each v_i, $i \in [0,k]$, and each u_i, $i \in [1,k]$, into its syllables. These factorizations define a factorization $w = w_1 \cdots w_m$ and we call this the *block factorization* of w. The participating factors $w_1, \dots, w_m$ are the *blocks* of w. (In other words, this is the coarsest refinement of the factorization $w = v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k$ and of w's factorization into syllables.)

Certified solutions. In the representation $v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1$ of (1), the words $u_1, \dots, u_k$ are called the *cycles*. If $u_i \in A_0^+ \cup A_1^+$, the cycle u_i is said to be *simple* and otherwise *mixed* (note that $u_i = \varepsilon$ cannot happen because $g_i \neq 1$). If u_i is a cycle, then the blocks inside the factor $u_i^{x_i}$ are u_i-*blocks* or *blocks from* u_i. A block inside a factor v_i is a v_i-*block* or a *block from* v_i. A cancellation $C \subseteq 2^{[1,m]}$ is called *normal* if for each simple cycle u_i, all u_i-blocks are contained in the same edge. By Lemma 4.11, every solution of (1) admits a normal cancellation. This motivates the following definition. A *certified solution* is a pair (x, C), where x is a solution to (1) and C is a normal cancellation of the word w as in (3). Observe that the non-trivial part of this lemma is to show that merging all edges incident to blocks of simple cycles does not violate well-nestedness.

▶ **Lemma 4.11.** *If a word $w \in A^*$ represents 1 in G, then it admits a normal cancellation.*

An edge $I \in C$ is called *standard* if $|I| = 2$ and the two blocks in I are from mixed cycles. Intuitively, the following tells us that in a normal cancellation, most edges are standard.

▶ **Lemma 4.12.** *Let C be a normal cancellation and u_i be a mixed cycle. Then there are at most $n + 3k + 1$ non-standard edges $I \in C$ containing a u_i-block.*

Mixed periods From now on, for each $i \in [1,k]$, we use e_i to denote the i-th unit vector in $\mathbb{N}^k$, i.e. the vector with 1 in the i-th coordinate and 0 otherwise. A *mixed period* is a vector $\pi \in \mathbb{N}^k$ of the form $\|u_j\| \cdot e_i + \|u_i\| \cdot e_j$, where u_i and u_j are mixed cycles. Let $\mathbb{P} \subseteq \mathbb{N}^k$ be the set of mixed periods. Note that $|\mathbb{P}| \leq k^2$.

We will need a condition that guarantees that a given period $\pi \in \mathbb{P}$ can be added to a solution x to obtain another solution. Suppose we have two blocks w_p and w_q for which we know that if we insert a string f_1 to the left of w_p and a string f_2 to the right of w_q and $f_1 f_2$ cancels to 1 in G, then the whole word cancels to 1. Which string would we insert to the left of w_p and to the right of w_q if we build the solution $x + \pi$?

Suppose w_p is a u_i-block and w_q is a u_j-block. Moreover, let w_r be the first (left-most) u_i-block and let w_s be the last (right-most) u_j-block. If we add $\|u_j\| \cdot e_i$ to x, this inserts $\lambda^{p-r}(u_i^{\|u_j\|})$ to the left of w_p: Indeed, in the case $p = r$, we insert $u_i^{\|u_j\|}$; and when p moves one position to the right, the inserted string is rotated once to the left. Similarly, if we add $\|u_i\| \cdot e_j$, we insert $\rho^{s-q}(u_j^{\|u_i\|})$ to the right of w_q: This is clear for $q = s$ and decrementing q means rotating the inserted string to the right. This motivates the following definition.

Let (x, C) be a certified solution and let u_i and u_j be mixed cycles with $i < j$. Moreover, let $[r, r'] \subseteq [1,m]$ and $[s', s] \subseteq [1,m]$ be the interval of u_i-blocks and of u_j-blocks, respectively. Then the mixed period $\pi = \|u_j\| \cdot e_i + \|u_i\| \cdot e_j$ is *compatible with* (x, C) if there are $p \in [r, r']$ and $q \in [s', s]$ such that

$$\lambda^{p-r}(u_i^{\|u_j\|}) \rho^{s-q}(u_j^{\|u_i\|}) \text{ represents 1 in } G, \qquad \{p, q\} \in C. \tag{4}$$

With $\mathbb{P}(x, C)$, we denote the set of mixed periods that are compatible with (x, C). One might wonder why we require an edge $\{p, q\} \in C$. In order to guarantee that $\lambda^{p-r}(u_i^{\|u_j\|})$ and $\rho^{s-q}(u_j^{\|u_i\|})$ can cancel, it would be sufficient to merely forbid edges $I \in C$ that intersect $[p, q]$ and contain a block outside of $[p-1, q+1]$. However, this weaker condition can become false when we insert other mixed periods. Our stronger condition is preserved, which implies:

▶ **Lemma 4.13.** *Let (x, C) be a certified solution. Then every $x' \in x + \mathbb{P}(x, C)^{\oplus}$ is a solution.*

Let $M \subseteq [1, k]$ be the set of $i \in [1, k]$ such that u_i is a mixed cycle and $\|x\|_{\mathsf{m}} = \max_{i \in M} x_i$.

▶ **Lemma 4.14.** *There is a polynomial q such that the following holds. For every certified solution (x, C) with $\|x\|_{\mathsf{m}} > q(n)$, there exists a mixed period $\pi \in \mathbb{P}$ and a certified solution (x', C') such that $x = x' + \pi$, $\pi \in \mathbb{P}(x', C')$, and $\mathbb{P}(x, C) \subseteq \mathbb{P}(x', C')$.*

Proof. We show that the lemma holds if $q(n) \geq (n + 3k + 1) + k(k^2 + 1)n^2$. (Recall that $k \leq n$.) Let (x, C) be a certified solution with $\|x\|_{\mathsf{m}} > q(n)$. Then there is a mixed cycle u_i such that $x_i > q(n)$ and hence $u_i^{x_i}$ consists of more than $q(n)$ blocks. Let $D \subseteq C$ be the set of all standard edges $I \in C$ that contain a block from u_i. Since an edge can contain at most one block per mixed cycle (see Lemma H.1), we have $|D| > q(n)$. Hence, Lemma 4.12 tells us that D contains more than $k(k^2 + 1)n^2$ standard edges. Hence, we find a mixed cycle u_j such that the set $E \subseteq D$ of edges $I \in D$ that contain a block both from u_i and one from u_j has $|E| > (k^2 + 1)n^2$. If B_i (B_j) denotes the set of blocks from u_i (u_j) contained in some edge $I \in E$, then each of the sets B_i and B_j has to be consecutive (see Lemma J.1).

For each $\pi \in \mathbb{P}(x, C)$, we choose an edge $I_\pi \in C$ that witnesses the compatibility of π. Let $W \subseteq C$ be the set of those chosen edges I_π. Since $|\mathbb{P}(x, C)| \leq |\mathbb{P}| \leq k^2$, we also have $|W| \leq k^2$. Since $|B_i| > (k^2 + 1)n^2 \geq (|W| + 1) \cdot n^2$, there is a sequence of more than n^2 consecutive blocks in B_i that do not belong to any $I \in W$.

We show the case $i < j$, the case $i > j$ can be done similarly. Our consecutive sequence in B_i consists of at least $n^2 + 1 \geq \|u_i\| \cdot \|u_j\| + 1$ blocks, and thus contains a segment of precisely $\|u_i\| \cdot \|u_j\| + 1$ blocks, say $w_{p'}, w_{p'+1}, \ldots, w_p$. By well-nestedness and since the blocks in B_j are consecutive, the neighbors of $w_{p'}, \ldots, w_p$ are consecutive as well, say $w_q, w_{q+1}, \ldots, w_{q'}$. Then $p - p' = q' - q = \|u_i\| \cdot \|u_j\| + 1$. Moreover, we have an edge $\{p + \ell, q - \ell\}$ in C for each $\ell \in [0, p' - p]$. In particular, $w_{p'} w_{p'+1} \cdots w_p w_q w_{q+1} \cdots w_{q'}$ represents 1 in G.

Let w_r be the left-most u_i-block and let w_s be the right-most u_j-block. Then, as shown before the definition of compatibility (p. 8), we have $\lambda^{p-r}(u_i^{\|u_j\|}) = w_{p'} w_{p'+1} \cdots w_p$ and $\rho^{s-q}(u_j^{\|u_i\|}) = w_q w_{q+1} \cdots w_{q'}$. Therefore, $\lambda^{p-r}(u_i^{\|u_j\|}) \rho^{s-q}(u_j^{\|u_i\|})$ represents 1 in G and $\{p, q\}$ witnesses compatibility of $\pi = \|u_j\| \cdot e_i + \|u_i\| \cdot e_j$ with (x, C). Hence, $\pi \in \mathbb{P}(x, C)$.

Let $x' = x - \pi$. We remove the blocks $w_{p'}, \ldots, w_p$ and $w_q, \ldots, w_{q'}$. Then, the remaining blocks spell $w' = v_0 u_1^{x_1'} v_1 \cdots u_k^{x_k'} v_k$. Indeed, recall that removing from a word y^t any factor of length $\ell \cdot |y|$ will result in the word $y^{t-\ell}$. Moreover, let C' be the set of edges that agrees with C on the remaining blocks. By the choice of the removed blocks, it is clear that C' is a normal cancellation. Hence, (x', C') is a certified solution.

It remains to verify $\mathbb{P}(x, C) \subseteq \mathbb{P}(x', C')$. This follows from the fact that for every mixed cycle u_ℓ, all remaining u_ℓ-blocks change their position relative to the left-most and the right-most u_ℓ-block by a difference that is divisible by $\|u_\ell\|$. Note that the expressions $\lambda^{p-r}(u_i^{\|u_j\|})$ is not altered when $p - r$ changes by a difference divisible by $\|u_i\|$, and an analogous fact holds for $\rho^{q-s}(u_j^{\|u_i\|})$. This means those block pairs that witnessed the compatibility of mixed periods before are still available and can serve as witnesses for (x', C'). ◀

Repeated application of Lemma 4.13 now yields:

▶ **Lemma 4.15.** *There exists a polynomial q such that the following holds. For every solution $x \in \mathbb{N}^k$, there exists a certified solution (x', C') with at most $q(n)$ mixed cycles such that $x \in x' + \mathbb{P}(x', C')^{\oplus}$.*

We are now ready to prove Proposition 4.10 and thus Theorem 4.5.

Proof of Proposition 4.10. Suppose that p_0 and p_1 are the polynomials guaranteed by the knapsack tameness of G_0 and G_1, respectively. Recall that $S \subseteq \mathbb{N}^k$ is the set of solutions to (1). We prove that there exists a polynomial p such that there is a semilinear set $S' \subseteq \mathbb{N}^k$ of magnitude at most $p(n)$ such that $x \in S' \subseteq S$. This clearly implies that S has magnitude at most $p(n)$. First, we apply Lemma 4.15. It yields a polynomial q and a certified solution (x', C') with $\|x\|_{\mathsf{m}} \leq q(n)$ such that $x \in x' + \mathbb{P}(x', C')$. Let $w' = v_0 u_1^{x'_1} v_1 \cdots u_k^{x'_k} v_k$ and consider w' decomposed into blocks as we did above with w.

Let $T \subseteq [1, k]$ be the set of all $i \in [1, k]$ for which the cycle u_i is simple. Since C' is normal, for each $i \in T$, all u_i-blocks are contained in one edge $I_i \in C'$. Note that it is allowed that one edge contains the blocks of multiple simple cycles. We partition T into sets $T = T_1 \uplus \cdots \uplus T_t$ so that $i \in T$ and $j \in T$ belong to the same part if and only if the u_i-blocks and the u_j-blocks belong to the same edge of C, i.e. $I_i = I_j$.

For a moment, let us fix an $\ell \in [1, t]$ and let $I \in C'$ be the edge containing all u_i-blocks for all the $i \in T_\ell$. Moreover, let $T_\ell = \{i_1, \ldots, i_r\}$. The words $\bar{v}_j$ for $j \in [0, r]$ will collect those blocks that belong to I but are not u_{i_s}-blocks for any $s \in [1, r]$. Formally, $\bar{v}_0$ consists of all blocks that belong to I that are to the left of all u_{i_1}-blocks. Similarly, $\bar{v}_r$ is the concatenation of all blocks belonging to I that are to the right of all u_{i_r}-blocks. Finally, for $j \in [1, r-1]$, $\bar{v}_j$ consists of all blocks that belong to I and are to the right of all u_{i_j}-blocks and to the left of all $u_{i_{j+1}}$-blocks. By consistency of C', for some $s \in \{0, 1\}$, all the words $\bar{v}_j$ for $j \in [0, r]$ and the words u_{i_j} for $j \in [1, r]$ belong to A_s^* and thus represent elements of G_s. Since G_s is knapsack tame, we know that the set

$$S_\ell = \{z \in \mathbb{N}^k \mid \bar{v}_0 u_{i_1}^{z_{i_1}} \bar{v}_1 u_{i_2}^{z_{i_2}} \bar{v}_2 \cdots u_{i_r}^{z_{i_r}} \bar{v}_r \text{ represents } 1 \text{ in } G_s, \quad z_j = 0 \text{ for } j \notin T_\ell\}$$

has magnitude at most $p_s(n)$. Consider the vector $y \in \mathbb{N}^k$ with $y_i = 0$ for $i \in T$ and $y_i = x'_i$ for $i \in [1, k] \setminus T$ (i.e. when u_i is a mixed cycle). We claim that $S' = y + S_1 + \cdots S_t + \mathbb{P}(x', C')^{\oplus}$ has magnitude at most $q(n) + p_0(n) + p_1(n) + n$ and satisfies $x \in S' \subseteq S$.

First, since y and the members of $S_1, \ldots, S_t$ are non-zero on pairwise disjoint coordinates, the magnitude of $y + S_1 + \cdots + S_t$ is the maximum of $\|y\|$ and the maximal magnitude of $S_1, \ldots, S_\ell$. Hence, it is bounded by $q(n) + p_0(n) + p_1(n)$. The summand $\mathbb{P}(x', C')^{\oplus}$ contributes only periods, and their magnitude is bounded by n (recall that they are mixed periods). Thus, the magnitude of S' is at most $p(n) = q(n) + p_0(n) + p_1(n) + n$.

The cancelling property of (x', C') tells us that $x' - y$ is contained in $S_1 + \cdots + S_t$. By the choice of (x', C'), we have $x \in x' + \mathbb{P}(x', C')^{\oplus}$. Together, this means $x \in S'$. Hence, it remains to show $S' \subseteq S$. To this end, consider a vector $x'' \in y + S_1 + \cdots + S_t$. It differs from x' only in the exponents at simple cycles. Therefore, we can apply essentially the same cancellation to x'' as to x': we just need to adjust the edges containing the blocks of simple cycles. It is therefore clear that the resulting cancellation C'' has the same compatible mixed periods as C': $\mathbb{P}(x'', C'') = \mathbb{P}(x', C')$. Thus, by Lemma 4.13, we have $x'' + \mathbb{P}(x', C')^{\oplus} \subseteq S$. This proves $y + S_1 + \cdots + S_t + \mathbb{P}(x', C')^{\oplus} \subseteq S$ and hence the proposition. ◀

4.4 LogCFL-hardness

It remains to show the lower bound in Theorem 4.2. If (A, I) is not complete, then (A, I) contains two non-adjacent vertices and thus $\mathbb{G}(A, I)$ contains an isomorphic copy of F_2, the

free group of rank two. Hence, we will show that knapsack and subset sum for F_2 are LogCFL-hard. Let $\{a, b\}$ be a generating set for F_2. Let $\theta\colon \{a, b, a^{-1}, b^{-1}\}^* \to F_2$ be the morphism that maps a word w to the group element represented by w. A *valence automaton* over a group G is a tuple $\mathcal{A} = (Q, \Sigma, \Delta, q_0, q_f)$ where Q, Σ, q_0, q_f are as in a finite automaton and Δ is a finite subset of $Q \times \Sigma^* \times G \times Q$. The *language accepted by* $\mathcal{A}$ is denoted $L(\mathcal{A})$ and consists of all words $w_1 \cdots w_n$ such that there is a computation $p_0 \xrightarrow{w_1,g_1} p_1 \to \cdots \to p_{n-1} \xrightarrow{w_n,g_n} p_n$ such that $(p_{i-1}, w_i, g_i, p_i) \in \Delta$ for $i \in [1, n]$ and $p_0 = q_0$, $p_n = q_f$, and $g_1 \cdots g_n = 1$.

An analysis of a proof (in this case [13]) of the Chomsky-Schützenberger theorem yields:

▶ **Lemma 4.16.** *For every context-free language $L \subseteq \Sigma^*$ there exists a valence automaton $\mathcal{A}$ over F_2 and a constant c such that the following statements are equivalent for every $w \in \Sigma^*$: (i) $w \in L$. (ii) $w \in L(\mathcal{A})$. (iii) There exists an accepting run of $\mathcal{A}$ for w of length $\leq c \cdot |w|$.*

Given w, it is easy to convert the valence automaton $\mathcal{A}$ from Lemma 4.16 into an acyclic automaton that exhausts all computations of $\mathcal{A}$ of length $c \cdot |w|$. This yields the following.

▶ **Proposition 4.17.** *For F_2, the membership problem for acyclic automata is* LogCFL*-hard.*

▶ **Proposition 4.18.** *For F_2, knapsack and subset sum are* LogCFL*-hard.*

Proof. Let $\mathcal{A} = (Q, \{a, b, a^{-1}, b^{-1}\}, \Delta, q_0, q_f)$ be an acyclic automaton. We construct words $w, w_1, \ldots, w_m \in \{a, b, a^{-1}, b^{-1}\}$ such that the following three statements are equivalent: (i) $1 \in \theta(L(\mathcal{A}))$. (ii) $\theta(w) \in \theta(w_1^* w_2^* \cdots w_m^*)$. (iii) $\theta(w) \in \theta(w_1^{e_1} w_2^{e_2} \cdots w_m^{e_m})$ for some $e_1, e_2, \ldots, e_m \in \{0, 1\}$. W.l.o.g. assume that $Q = \{1, \ldots, n\}$, where 1 is the initial state and n is the unique final state of $\mathcal{A}$.

Let $\alpha_i = a^i b a^{-i}$ for $i \in [1, n+2]$. It is well known that the α_i generate a free subgroup of rank $n+2$ in F_2 [18, Proposition 3.1]. Define the embedding $\varphi\colon F_2 \to F_2$ by $\varphi(a) = \alpha_{n+1}$ and $\varphi(b) = \alpha_{n+2}$. For a transition $t = (p, w, q) \in \Delta$ let $\tilde{t} = \alpha_p \varphi(w) \alpha_q^{-1}$. Let $\Delta = \{t_1, \ldots, t_m\}$ such that $t_i = (p, a, q)$ and $t_j = (q, b, r)$ implies $i < j$. Since $\mathcal{A}$ is acyclic, such an enumeration must exist. Together with the fact that the α_i generate a free group, it follows that the following three statements are equivalent: (i) $1 \in \theta(L(\mathcal{A}))$. (ii) $\theta(\alpha_1 \alpha_n^{-1}) \in \theta(\tilde{t}_1^* \tilde{t}_2^* \cdots \tilde{t}_m^*)$. (iii) $\theta(\alpha_1 \alpha_n^{-1}) \in \theta(\tilde{t}_1^{e_1} \tilde{t}_2^{e_2} \cdots \tilde{t}_m^{e_m})$ for some $e_1, e_2, \ldots, e_m \in \{0, 1\}$. ◀

5 NP-completeness

In [17], the authors proved that knapsack for the graph group $\mathbb{G}(\mathsf{C4}) \cong F_2 \times F_2$ is NP-complete. Here we extend this result to all graph groups $\mathbb{G}(A, I)$ where (A, I) is not a transitive forest. An *acyclic loop automaton* is a finite automaton $\mathcal{A} = (Q, \Sigma, \Delta, q_0, q_f)$ such that there exists a linear order $\preceq$ on Δ having the property that for all $(p, u, q), (q, v, r) \in \Delta$ it holds $(p, a, q) \preceq (q, b, r)$. Thus, an acyclic loop automaton is obtained from an acyclic automaton by attaching to some of the states a unique loop. For a trace monoid $\mathbb{M}(A, I)$, the *intersection nonemptiness problem for acyclic loop automata* is the following computational problem:

Input: Two acyclic loop automata $\mathcal{A}_1$, $\mathcal{A}_2$ over the input alphabet A.

Question: Does $[L(\mathcal{A}_1)]_I \cap [L(\mathcal{A}_2)]_I \neq \emptyset$ hold?

Aalbersberg and Hoogeboom [1] proved that for the trace monoid $\mathbb{M}(\mathsf{P4})$ the intersection nonemptiness problem for arbitrary finite automata is undecidable. We use their technique to show:

▶ **Lemma 5.1.** *For $\mathbb{M}(\mathsf{P4})$, intersection nonemptiness for acyclic loop automata is* NP*-hard.*

Proof. We give a reduction from 3SAT. Let $\varphi = \bigwedge_{i=1}^{m} C_i$ where for every $i \in [1,m]$, $C_i = (L_{i,1} \vee L_{i,2} \vee L_{i,3})$ is a clause consisting of three literals. Let $x_1, \ldots, x_n$ be the boolean variables that occur in φ. Every literal $L_{i,j}$ belongs to $\{x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n\}$.

Let $p_1, p_2, \ldots, p_n$ be a list of the first n prime numbers. So, for each boolean variable x_i we have the corresponding prime number p_i. We encode a valuation $\beta\colon \{x_1, \ldots, x_n\} \to \{0,1\}$ by any natural number N such that $N \equiv 0 \bmod p_i$ if and only if $\beta(x_i) = 1$. For a positive literal x_i let $S(x_i) = \{p_i \cdot n \mid n \in \mathbb{N}\}$ and for a negative literal $\neg x_i$ let $S(\neg x_i) = \{p_i \cdot n + r \mid n \in \mathbb{N}, r \in [1, p_i - 1]\}$. Moreover, for every $i \in [1,m]$ let $S_i = S(L_{i,1}) \cup S(L_{i,2}) \cup S(L_{i,3})$. Thus, S_i is the set of all numbers that encode a valuation, which makes the clause C_i true. Hence, the set $S = \bigcap_{i=1}^{n} S_i$ encodes the set of all valuations that make φ true.

We first construct an acyclic loop automaton $\mathcal{A}_1$ with $L(\mathcal{A}_1) = \prod_{i=1}^{m} \{a(bc)^{N_i} d \mid N_i \in S_i\}$. Note that φ is satisfiable iff $[L(\mathcal{A}_1)]_I$ contains a trace from $[\{(a(bc)^N d)^m \mid N \in \mathbb{N}\}]_I$. We will ensure this property with a second acyclic loop automaton $\mathcal{A}_2$ that satisfies the equality $L(\mathcal{A}_2) = b^*(ad(bc)^*)^{m-1}adc^*$. We claim that $[L(\mathcal{A}_1)]_I \cap [L(\mathcal{A}_2)]_I = [\{(a(bc)^N d)^m \mid N \in S\}]_I$.

First assume that $w \equiv_I (a(bc)^N d)^m$ for some $N \in S$. We have

$$w \equiv_I (a(bc)^N d)^m \equiv_I b^N (ad(bc)^N)^{m-1} adc^N$$

and thus $[w]_I \in [L(\mathcal{A}_2)]_I$. Moreover, since $N \in S$ we get $[w]_I \in [L(\mathcal{A}_1)]_I$. For the other direction, let $[w]_I \in [L(\mathcal{A}_1)]_I \cap [L(\mathcal{A}_2)]_I$. Thus

$$w \equiv_I \prod_{i=1}^{m} (a(bc)^{N_i} d) \equiv b^{N_1} \left(\prod_{i=1}^{m-1} (adc^{N_i} b^{N_{i+1}}) \right) adc^{N_m}$$

where $N_i \in S_i$ for $i \in [1,m]$. Moreover, $[w]_I \in [L(\mathcal{A}_2)]_I$ yields $k_0, k_1, \ldots, k_{m-1}, k_m \geq 0$ with

$$b^{N_1} \left(\prod_{i=1}^{m-1} (adc^{N_i} b^{N_{i+1}}) \right) adc^{N_m} \equiv_I b^{k_0} \left(\prod_{i=1}^{m-1} (ad(bc)^{k_i}) \right) adc^{k_m} \equiv_I b^{k_0} \left(\prod_{i=1}^{m-1} (adb^{k_i} c^{k_i}) \right) adc^{k_m}$$

Since every symbol is dependent from a or d, this identity implies $N_i = N_{i+1}$ for $i \in [1, m-1]$. Thus, $[w]_I \in [\{(a(bc)^N d)^m \mid N \in S\}]_I$. ◀

For a graph group $\mathbb{G}(A,I)$ the *membership problem for acyclic loop automata* is the following computational problem:

Input: An acyclic loop automaton $\mathcal{A}$ over the input alphabet $A \cup A^{-1}$.

Question: Is there a word $w \in L(\mathcal{A})$ such that $w = 1$ in $\mathbb{G}(A,I)$?

It is straightforward to reduce the intersection emptiness problem for acyclic loop automata over $\mathbb{M}(A,I)$ to the membership problem for acyclic loop automata over $\mathbb{G}(A,I)$.

▶ **Lemma 5.2.** *For $\mathbb{G}(\mathsf{P4})$, the membership problem for acyclic loop automata is* NP*-hard.*

We can now use a construction from [16] to reduce knapsack to membership for acyclic loop automata.

▶ **Lemma 5.3.** *Knapsack for the graph group $\mathbb{G}(\mathsf{P4})$ is* NP*-hard.*

▶ **Theorem 5.4.** *Let (A,I) be an independence alphabet, which is not a transitive forest. Then, knapsack for the graph group $\mathbb{G}(A,I)$ is* NP*-complete.*

Proof. If (A,I) is not a transitive forest, then P4 or C4 is an induced subgraph of (A,I) [25]. Thus, $\mathbb{G}(\mathsf{P4})$ or $\mathbb{G}(\mathsf{C4}) \cong F_2 \times F_2$ is a subgroup of $\mathbb{G}(A,I)$. Hence, NP-hardness of knapsack for $\mathbb{G}(A,I)$ follows from [17] or Lemma 5.3. ◀

References

1 I. J. Aalbersberg and H. J. Hoogeboom. Characterizations of the decidability of some problems for regular trace languages. *Mathematical Systems Theory*, 22:1–19, 1989.

2 I. Agol. The virtual Haken conjecture. Technical report, arXiv.org, 2012. `http://arxiv.org/abs/1204.2810`.

3 M. Bestvina and N. Brady. Morse theory and finiteness properties of groups. *Inventiones Mathematicae*, 129(3):445–470, 1997.

4 J. Crisp and B. Wiest. Embeddings of graph braid and surface groups in right-angled Artin groups and braid groups. *Algebraic & Geometric Topology*, 4:439–472, 2004.

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

6 E. Frenkel, A. Nikolaev, and A. Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016.

7 R. Ghrist and V. Peterson. The geometry and topology of reconfiguration. *Advances in Applied Mathematics*, 38(3):302–323, 2007.

8 S. Greibach. The hardest context-free language. *SIAM Journal on Computing*, 2(4):304–310, 1973.

9 S. A. Greibach. A new normal-form theorem for context-free phrase structure grammars. *Journal of the ACM*, 12(1):42–52, 1965.

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

11 F. Haglund and D. T. Wise. Coxeter groups are virtually special. *Advances in Mathematics*, 224(5):1890–1903, 2010.

12 B. Jenner. Knapsack problems for NL. *Information Processing Letters*, 54(3):169–174, 1995.

13 M. Kambites. Formal languages and groups as memory. *Communications in Algebra*, 37:193–208, 2009.

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

15 D. König, M. Lohrey, and G. Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. Technical report, arXiv.org, 2015. `http://arxiv.org/abs/1507.05145`.

16 M. Lohrey and B. Steinberg. The submonoid and rational subset membership problems for graph groups. *Journal of Algebra*, 320(2):728–755, 2008.

17 M. Lohrey and G. Zetzsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In *Proceedings of STACS 2016*, volume 47 of *LIPIcs*, pages 50:1–50:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

18 R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer, 1977.

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

20 C. H. Papadimitriou. On the complexity of integer programming. *Journal of the Association for Computing Machinery*, 28(4):765–768, 1981.

21 L. Pottier. Minimal solutions of linear diophantine systems : bounds and algorithms. In *Proc. of 4th International Conference on Rewriting Techniques and Applications (RTA 1991)*, pages 162–173, Berlin, Heidelberg, 1991. Springer.

22 I. H. Sudborough. On the tape complexity of deterministic context–free languages. *Journal of the ACM*, 25(3):405–414, 1978.

23 H. Vollmer. *Introduction to Circuit Complexity*. Springer, 1999.

24 D. T. Wise. Research announcement: the structure of groups with a quasiconvex hierarchy. *Electronic Research Announcements in Mathematical Sciences*, 16:44–55, 2009.

25 E. S. Wolk. A note on "The comparability graph of a tree". *Proceedings of the American Mathematical Society*, 16:17–20, 1965.

A Proof of Theorem 4.1

Hardness for TC^0 follows from the fact that the word problem for $\mathbb{Z}$ is TC^0-complete: this is exactly the problem of checking whether for a given word $w \in \{a, b\}^*$, $|w|_a = |w|_b$ holds.

Let us now show that knapsack for $\mathbb{Z}^m$ belongs to TC^0. Let $A = \{a_1, \ldots, a_m\}$ be the generating set for $\mathbb{Z}^m$. Given a word $w \in (A \cup A^{-1})^*$ we can compute the vector $(b_1, \ldots, b_m) \in \mathbb{Z}^m$ with $b_i := |w|_{a_i} - |w|_{a_i^{-1}}$ represented in unary notation in TC^0 (counting the number of occurrences of a symbol in a string and subtraction can be done in TC^0). Hence, we can transform in TC^0 an instance of knapsack for $\mathbb{Z}^m$ into a system of equations $Ax = b$, where $A \in \mathbb{Z}^{m \times n}$ is an integer matrix with unary encoded entries, $b \in \mathbb{Z}^m$ is an integer vector with unary encoded entries, and x is a vector of n variables ranging over $\mathbb{N}$. Let $t = n(ma)^{2m+1}$, where a is the maximal absolute value of an entry in $(A \mid b)$. By [20] the system $Ax = b$ has a solution if and only if it has a solution with all entries of x from the interval $[0, t]$. Since m is a constant, the unary encoding of the number t can be computed in TC^0 (iterated multiplication can be done in TC^0). However, the question whether the system $Ax = b$ has a solution from $[0, t]^n$ is an instance of the m-integer-linear-programming problem from [5], which was shown to be in TC^0 in [5]. For subset sum for $\mathbb{Z}^m$ one can use the same argument with $t = 1$.

B Proof of Proposition 4.3

The class LogCFL is included in the parallel complexity class NC^2 and has several alternative characterizations (see e.g. the book [23] for more details):

- logspace bounded alternating Turing-machines with polynomial proof tree size,
- semi-unbounded Boolean circuits of polynomial size and logarithmic depth, and
- logspace bounded auxiliary pushdown automata with polynomial running time.

For our purposes, the last characterization is most suitable. An AuxPDA (for auxiliary pushdown automaton) is a nondeterministic pushdown automaton with a two-way input tape and an additional work tape. Here we only consider AuxPDA with the following two restrictions:

- The length of the work tape is restricted to $O(\log n)$ for an input of length n (logspace bounded).
- There is a polynomial $p(n)$, such that every computation path of the AuxPDA on an input of length n has length at most $p(n)$ (polynomially time bounded).

Whenever we speak of an AuxPDA in the following, we implicitly assume that the AuxPDA is logspace bounded and polynomially time bounded. Deterministic AuxPDA are defined in the obvious way. The class of languages that are accepted by AuxPDA (resp., deterministic AuxPDA) is denoted by LogCFL (resp., $\mathsf{LogDCFL}$). The proof of Proposition 4.3 uses the following lemma:

▶ **Lemma B.1.** *For every transitive forest (A, I) with the associated graph group $G = \mathbb{G}(A, I)$ there is a deterministic AuxPDA $\mathcal{P}(G)$ with input alphabet $A^{\pm 1}$ and the following properties:*

- *In each step, the input head for $\mathcal{P}(G)$ either does not move, or moves one step to the right.*
- *If the input word is equal to 1 in G, then $\mathcal{P}(G)$ terminates in the distinguished state q_1 with empty stack. Let us call this state the 1-state of $\mathcal{P}(G)$.*
- *If the input word is not equal to 1 in G, then $\mathcal{P}(G)$ terminates in a state different from q_1 (and the stack is not necessarily empty).*

Proof. We construct the AuxPDA $\mathcal{P}(G)$ by induction over the structure of the group G. For this, we consider the three cases that $G = 1$, $G = G_1 * G_2$, and $G = \mathbb{Z} \times G'$. The case that $G = 1$ is of course trivial.

- Case $G = \mathbb{Z} \times G'$. We have already constructed the AuxPDA $\mathcal{P}(G')$. The AuxPDA $\mathcal{P}(G)$ simulates the AuxPDA $\mathcal{P}(G')$ on the generators of G'. Moreover, it stores the current value of the $\mathbb{Z}$-component in binary notation on the work tape. If the input word has length n, then $O(\log n)$ bits are sufficient for this. At the end, $\mathcal{P}(G)$ goes into its 1-state if and only if $\mathcal{P}(G')$ is in its 1-state (which implies that the stack will be empty) and the $\mathbb{Z}$-component is zero.
- Case $G = G_1 * G_2$. For $i \in \{1, 2\}$, we have already constructed the AuxPDA $\mathcal{P}_i = \mathcal{P}(G_i)$. Let $A_i^{\pm 1}$ be its input alphabet, which is a monoid generating set for G_i. Consider now an input word $w \in (A_1^{\pm 1} \cup A_2^{\pm 1})^*$. Let us assume that $w = u_1 v_1 u_2 v_2 \cdots u_k v_k$ with $u_i \in (A_1^{\pm 1})^+$ and $v_i \in (A_2^{\pm 1})^+$ (other cases can be treated analogously). The AuxPDA $\mathcal{P}(G)$ starts with empty stack and simulates the AuxPDA $\mathcal{P}_1$ on the prefix u_1. If it turns out that $u_1 = 1$ in G_1 (which means that $\mathcal{P}_1$ is in its 1-state) then the stack will be empty and the AuxPDA $\mathcal{P}(G)$ continues with simulating $\mathcal{P}_2$ on v_1. On the other hand, if $u_1 \neq 1$ in G_1, then $\mathcal{P}(G)$ pushes the state together with the work tape content of $\mathcal{P}_1$ reached after reading u_1 on the stack (on top of the final stack content of $\mathcal{P}_1$). This allows $\mathcal{P}(G)$ to resume the computation of $\mathcal{P}_1$ later. Then $\mathcal{P}(G)$ continues with simulating $\mathcal{P}_2$ on v_1. The computation of $\mathcal{P}(G)$ will continue in the above way. More precisely, if after reading u_i (resp. v_i with $i < k$) the AuxPDA $\mathcal{P}_1$ (resp. $\mathcal{P}_2$) is in its 1-state then either

  (i) the stack is empty or
  (ii) the top part of the stack is of the form sqt (t is the top), where s is a stack content of $\mathcal{P}_2$ (resp. $\mathcal{P}_1$), q is a state of $\mathcal{P}_2$ (resp. $\mathcal{P}_1$) and t is a work tape content of $\mathcal{P}_2$ (resp. $\mathcal{P}_1$).

  In case (i), $\mathcal{P}(G)$ continues with the simulation of $\mathcal{P}_2$ (resp. $\mathcal{P}_1$) on the word v_i (resp. u_{i+1}) in the initial configuration. In case (ii), $\mathcal{P}(G)$ continues with the simulation of $\mathcal{P}_2$ (resp. $\mathcal{P}_1$) on the word v_i (resp. u_{i+1}), where the simulation is started with stack content s, state q, and work tape content t. On the other hand, if after reading u_i (resp. v_i with $i < k$) the AuxPDA $\mathcal{P}_1$ (resp. $\mathcal{P}_2$) is not in its 1-state then $\mathcal{P}(G)$ pushes on the stack the state and work tape content of $\mathcal{P}_1$ reached after its simulation on u_i.

This concludes the description of the AuxPDA $\mathcal{P}(G)$. ◀

We can now prove Proposition 4.3:

Proof of Proposition 4.3. Fix the graph group $G = \mathbb{G}(A, I)$, where (A, I) is a transitive forest. An AuxPDA for the membership problem for acyclic automata guesses a path in the input automaton $\mathcal{A}$ and thereby simulates the AuxPDA $\mathcal{P}(G)$ from Lemma B.1. If the final state of the input automaton $\mathcal{A}$ is reached while the AuxPDA $\mathcal{P}(G)$ is in the accepting state q_1, then the overall AuxPDA accepts. It is important that the AuxPDA $\mathcal{P}(G)$ works one-way since the guessed path in $\mathcal{A}$ cannot be stored in logspace. This implies that the AuxPDA

cannot reaccess the input symbols that already have been processed. Also note that the AuxPDA is logspace bounded and polynomially time bounded since $\mathcal{A}$ is acyclic. ◀

C Proof of the upper bound in Theorem 4.2

According to Proposition 4.3, it suffices to provide a logspace reduction to the knapsack problem over G to the membership problem for acyclic automata over G. Suppose we have an instance $h_0 g_1^{x_1} h_1 \cdots g_k^{x_k} h_k = 1$ of the knapsack problem over G of size n. Moreover, let h_i be represented by $v_i \in A^*$ for each $i \in [0,k]$ and let g_i be represented by $u_i \in A^*$ for $i \in [1,k]$.

By Theorem 4.5, there is a polynomial p such that the equation has a solution if and only if it has a solution $x \in \mathbb{N}^k$ with $\|x\| \leq p(n)$. We construct an acyclic automaton $\mathcal{A} = (Q, A, \Delta, q_0, q_f)$ as follows. It has the state set $Q = [0,k+1] \times [0,p(n)]$ and the following transitions. From $(0,0)$, there is one transition labeled v_0 to $(1,0)$. For each $i \in [1,k]$ and $j \in [0,p(n)-1]$, there are two transitions from (i,j) to $(i,j+1)$; one labeled by u_i and one labeled by ε. Furthermore, there is a transition from $(i,p(n))$ to $(i+1,0)$ labeled v_i for each $i \in [1,k]$. The initial state is $q_0 = (0,0)$ and the final state is $q_f = (k+1,0)$.

It is clear that $\mathcal{A}$ accepts a word that represents 1 if and only if the exponent equation has a solution. Finally, the reduction can clearly be carried out in logarithmic space.

For subset sum the same reduction as above works but the polynomial bound on solutions is for free.

D Proof of Lemma 4.8

Let $\{c_1, \ldots, c_s\}$ be the set of minimal solutions of $Bx = b$. Then, Theorem 4.7 yields

$$\|c_i\|_1 \leq (1 + \|(B \mid -b)\|_{1,\infty})^{r+1} \leq (1 + \|B\|_{1,\infty} + \|b\|)^{r+1}.$$

Moreover, let C be the matrix whose columns are the t elements of the Hilbert basis of $Bx = 0$. Then we have

$$\|C\|_{\infty,1} \leq (1 + \|B\|_{1,\infty})^r.$$

This clearly yields the desired decomposition.

E Proof of Lemma 4.9

Write $B = (b_1, \ldots, b_k)$ and consider the row vector $B' \in \mathbb{Z}^{1 \times (2M+1)}$ with entries

$$(b'_1, \ldots, b'_{2M+1}) = (-M, -M+1, \ldots, -1, 0, 1, \ldots, M)$$

and the matrix $S \in \mathbb{N}^{(2M+1) \times k}$, $S = (s_{ij})$, with

$$s_{ij} = \begin{cases} 1 & \text{if } b_j = i, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have $B = B'S$, $\|B'\|_{1,\infty} = (M+1)M$. Furthermore, observe that $\|Sx\|_1 = \|x\|_1$ for every $x \in \mathbb{N}^k$ and that for each $y \in \mathbb{N}^t$, the set

$$T_y = \{x \in \mathbb{N}^k \mid Sx = y\}$$

is finite. According to Lemma 4.8, we can write

$$\{x \in \mathbb{Z}^{2M+1} \mid B'x = b\} = \bigcup_{i=1}^{s'} c'_i + C'\mathbb{N}^{t'} \tag{5}$$

where $\|c'_i\|_1$ and $\|C'\|_{\infty,1}$ are bounded by $(1+(M+1)M+M)^2 = (M+1)^4$. Let $\{c_1, \ldots, c_s\}$ be the union of all sets $T_{c'_i}$ for $i \in [1, s']$ and let $C \in \mathbb{N}^{k \times t}$ be the matrix whose columns comprise all T_v where $v \in \mathbb{N}^{2M+1}$ is a column of C'. Since $\|Sx\|_1 = \|x\|_1$ for $x \in \mathbb{N}^k$, the vectors c_i obey the same bound as the vectors c'_i, meaning $\|c_i\|_1 \leq (M+1)^4$. By the same argument, we have $\|C\|_{\infty,1} \leq \|C'\|_{\infty,1} \leq (M+1)^4$. It remains to be shown that the equality from the lemma holds.

Suppose $Bx = b$. Then $B'Sx = b$ and hence $Sx = c'_i + C'y$ for some $y \in \mathbb{N}^{t'}$. Observe that if $Sz = p + q$, then z decomposes as $z = p' + q'$ so that $Sp' = p$ and $Sq' = q$. Therefore, we can write $x = x_0 + \cdots + x_n$ with $Sx_0 = c'_i$ and Sx_j is some column of C' for each $j \in [1, n]$. Hence, $x_0 = c_r$ for some $r \in [1, s]$ and for each $j \in [1, n]$, x_j is a column of C. This proves $x \in c_r + C\mathbb{N}^t$.

On the other hand, the definition of $c_1, \ldots, c_s$ and C implies that for each column v of C, Sv is a column of C'. Moreover, for each $i \in [1, s]$, there is a $j \in [1, s']$ with $Sc_i = c'_j$ and thus $Sc_i + SC\mathbb{N}^t \subseteq c'_i + C'\mathbb{N}^{t'}$. Therefore

$$B(c_i + C\mathbb{N}^t) = B'S(c_i + C\mathbb{N}^t) \subseteq B'(c'_i + C'\mathbb{N}^{t'})$$

and the latter set contains only b because of (5).

F Proof of Proposition 4.6

We need one more lemma.

▶ **Lemma F.1.** *Let $S \subseteq \mathbb{N}^k$ be a semilinear set of magnitude M and $B \in \mathbb{Z}^{1\times k}$, $b \in \mathbb{Z}$ with $\|B\|_\infty \leq m$ and $|b| \leq m$. Then $\{x \in S \mid Bx = b\}$ is a semilinear set of magnitude at most $(kmM)^d$ for some constant d.*

Proof. Let $T = \{x \in \mathbb{N}^k \mid Bx = b\}$. We may assume that S is linear of magnitude M, because if $S = L_1 \cup \cdots \cup L_n$, then $S \cap T = (L_1 \cap T) \cup \cdots \cup (L_n \cap T)$.

Write $S = a + A\mathbb{N}^n$ with $a \in \mathbb{N}^k$ and $A \in \mathbb{N}^{k\times n}$. Then we have $\|a\| \leq M$ and $\|A\|_\infty \leq M$. Consider the set $U = \{x \in \mathbb{N}^n \mid BAx = b - Ba\}$. Note that $BA \in \mathbb{Z}^{1\times n}$ and

$$\|BA\|_\infty \leq k \cdot \|B\|_\infty \cdot \|A\|_\infty \leq kmM.$$

$$|b - Ba| \leq m + k \cdot \|B\|_\infty \cdot \|a\| \leq m + kmM.$$

According to Lemma 4.9, we can write $U = \bigcup_{i=1}^{s} c_i + C\mathbb{N}^t$ where $\|c_i\|_1$ and $\|C\|_{\infty,1}$ are at most $(m + kmM + 1)^4$. Observe that

$$a + AU = \bigcup_{i=1}^{s} a + Ac_i + AC\mathbb{N}^t$$

and

$$\|a + Ac_i\| \leq \|a\| + \|A\|_\infty \cdot \|c_i\|_1 \leq M + M(m + kmM + 1)^4$$

$$\|AC\|_\infty \leq \|A\|_\infty \cdot \|C\|_{\infty,1} \leq M(m + kmM + 1)^4.$$

Finally, note that $S \cap T = a + AU$. ◀

We are now ready to prove Proposition 4.6.

Proof of Proposition 4.6. Suppose G is knapsack tame with polynomial $\bar{p}$. Let

$$h_0 g_1^{\mathsf{x}_1} h_1 g_2^{\mathsf{x}_2} h_2 \cdots g_k^{\mathsf{x}_k} h_k = 1 \tag{6}$$

be an exponent equation of size n with pairwise distinct variables $\mathsf{x}_1, \ldots, \mathsf{x}_k$ and with $h_0, g_1, h_1, \ldots, g_k, h_k \in G \times \mathbb{Z}$. Let $h_i = (\bar{h}_i, y_i)$ for $i \in [0, k]$ and $g_i = (\bar{g}_i, z_i)$ for $i \in [1, k]$.

The exponent equation $\bar{h}_0 \bar{g}_1^{\mathsf{x}_1} \bar{h}_1 \bar{g}_2^{\mathsf{x}_2} \bar{h}_2 \cdots \bar{g}_k^{\mathsf{x}_k} \bar{h}_k = 1$ has a semilinear solution set $\bar{S} \subseteq \mathbb{N}^k$ of magnitude at most $\bar{p}(n)$. The solution set of (6) is $S = \{(x_1, \ldots, x_k) \in \bar{S} \mid z_1 x_1 + \cdots + z_k x_k = y\}$, where $y = -(y_0 + \cdots + y_k)$. Note that $|z_i| \leq n$ and $|y| \leq n$. By Lemma F.1, S is semilinear of magnitude $(n^2 \bar{p}(n))^d$ for some constant d (recall that $k \leq n$). ◀

G Proof of Lemma 4.11

We have convinced ourselves that every word that represents 1 in G admits some cancellation C. The *normalization of* C is obtained as follows. For each simple cycle u_i, let $I_1, \ldots, I_\ell$ be those edges of C that contain a block from u_i. Remove $I_1, \ldots, I_\ell$ from C and instead include $I_1 \cup \cdots \cup I_\ell$. We claim that the normalization of C is again a cancellation.

To this end, it suffices to show that if C is a cancellation and $I_1, I_2 \in C$ such that there are neighboring blocks u and u' with $uu' \in A_0^* \cup A_1^*$ such that $u \in I_1$ and $u' \in I_2$, then the set $C' = (C \setminus \{I_1, I_2\}) \cup \{I_1 \cup I_2\}$ is a cancellation: Then, our claim (and hence the lemma) follows by repeated application of this fact.

Clearly, C' is a partition, consistent, and cancelling. Let us verify that it is well-nested. We begin with a small observation. Let $J \in C$, $J \neq I_1, I_2$, and $j, j' \in J$ with $j < j'$. Since I_1 contains a block neighboring a block in I_2, if $[j, j']$ includes at least one of the sets I_1, I_2, it includes both.

Now suppose C' is not well-nested. Then there is a $J \in C$, $i_1, i_2 \in I_1 \cup I_2$, and $j, j' \in J$ such that $i_1 < j < i_2$ and $j' \notin [i_1, i_2]$. By well-nestedness of C, each of the edges I_1, I_2 contains at most one of the elements i_1, i_2. Without loss of generality, let $i_1 \in I_1$ and $i_2 \in I_2$. We distinguish two cases.

- If $i_1 < j < i_2 < j'$, then $i_2 \in [j, j']$ and hence by well-nestedness of C, we have $I_2 \subseteq [j, j']$. By our observation above, this also means $I_1 \subseteq [j, j']$, contradicting $I_1 \ni i_1 < j$.
- If $j' < i_1 < j < i_2$, then $i_1 \in [j', j]$ and by well-nestedness of C, we have $I_1 \subseteq [j', j]$. By our observation, this implies $I_2 \subseteq [j', j]$, in contradiction to $j < i_2$.

H Proof of Lemma 4.12

Before we prove Lemma 4.12, we need an auxiliary lemma.

▶ **Lemma H.1.** *Let C be a cancellation. If w_i, w_j are two distinct blocks from the same mixed cycle, then there is no edge $I \in C$ with $w_i, w_j \in I$.*

Proof. Suppose there is such an $I \in C$. Furthermore, assume that i and j are chosen so that $|i - j|$ is minimal and $i < j$. Since w_i and w_j are both contained in I, we have $w_i w_j \in A_0^+ \cup A_1^+$ by consistency of C. Hence, by (2), w_i and w_j cannot be neighboring blocks. Hence, there is an $\ell \in [1, m]$ with $i < \ell < j$. This means there is a $J \in C$ with $\ell \in J$. By well-nestedness, $J \subseteq [i, j]$. Since every edge in C must contain at least two elements, we have $|J| \geq 2$ and thus a contradiction to the minimality of $|i - j|$. ◀

Proof of Lemma 4.12. Let $N \subseteq C$ be the set of all non-standard edges $I \in C$ that contain a u_i-block. Then, each edge $I \in N$ satisfies one of the following.

(i) I contains a block from some simple cycle. Since C is normal, there are at most k such I.
(ii) I contains a block from some v_j, $j \in [0,k]$. Since $\|v_0\| + \cdots + \|v_k\| \leq n$, there are at most n such I.
(iii) I contains only blocks from mixed cycles and $|I| > 2$.

Let $M \subseteq C$ be the set of edges of type (iii). If we can show that $|M| \leq 2k+1$, then the lemma is proven. Consider the sets

$$M_- = \{I \in M \mid I \text{ contains a block from a mixed cycle } u_j,\ j < i\},$$
$$M_+ = \{I \in M \mid I \text{ contains a block from a mixed cycle } u_j,\ j > i\}.$$

We shall prove that $|M_- \cap M_+| \leq 1$ and that $|M_+ \setminus M_-| \leq k$. By symmetry, this also means $|M_- \setminus M_+| \leq k$ and thus $|M| = |M_- \cup M_+| \leq 2k+1$.

Suppose $I_1, I_2 \in M_- \cap M_+$, $I_1 \neq I_2$. Let $r \in I_1$ and $s \in I_2$ such that w_r and w_s are blocks from u_i, say with $r < s$. Since $I_1 \in M_+$, I_1 contains a block $w_{r'}$ from a mixed cycle u_j, $j > i$. This means in particular $s < r'$. By well-nestedness, this implies $I_2 \subseteq [r, r']$, so that I_2 cannot contain a block from a mixed cycle u_ℓ with $\ell < i$, contradicting $I_2 \in M_-$. Thus, $|M_- \cap M_+| \leq 1$.

In order to prove $|M_+ \setminus M_-| \leq k$, we need another concept. For each $I \in M_+$, there is a maximal $j \in [1,k]$ such that u_j is a mixed cycle and I contains a block from u_j. Let $\mu(I) = j$. We will show $\mu(I_1) \neq \mu(I_2)$ for all $I_1, I_2 \in M_+ \setminus M_-$, $I_1 \neq I_2$. This clearly implies $|M_+ \setminus M_-| \leq k$.

Suppose $I_1, I_2 \in M_+ \setminus M_-$, $I_1 \neq I_2$, with $\mu(I_1) = \mu(I_2)$. Let $j = \mu(I_1) = \mu(I_2)$. Let w_r be a block from u_i contained in I_1 and let $w_{r'}$ be a block from u_i contained in I_2. (Recall that those exist because $I_1, I_2 \in M$.) Without loss of generality, assume $r < r'$. Moreover, let w_s be a block from u_j contained in I_1 and let $w_{s'}$ be a block from u_j contained in I_2. By well-nestedness and since $r' \in [r,s]$, we have $I_2 \subseteq [r,s] \subseteq I_1$. Thus, $r < r' < s' < s$.

However, we have $|I_1| > 2$, meaning I_1 contains a block w_p other than w_r and w_s. Since an edge cannot contain two blocks of one mixed cycle (see Lemma H.1), w_p has to belong to a mixed cycle u_t other than u_i and u_j. By the maximality of j, we have $i < t < j$. This implies, however, $r' < p < s'$. By well-nestedness, this means $I_1 \subseteq [r', s'] \subseteq I_2$ and thus $I_1 = I_2$, a contradiction. ◀

I Proof of Lemma 4.13

It suffices to show that if (x, C) is a certified solution and $\pi \in \mathbb{P}(x, C)$, then there is a certified solution (x', C') such that $x' = x + \pi$ and $\mathbb{P}(x, C) \subseteq \mathbb{P}(x', C')$. Suppose $\pi = \|u_j\| \cdot e_i + \|u_i\| \cdot e_j \in \mathbb{P}(x, C)$. Without loss of generality, assume $i < j$. Let $r \in [1,m]$ and $s \in [1,m]$ be the left-most u_i-block and the right-most u_j-block, respectively.

Since $\pi \in \mathbb{P}(x, C)$, there is a u_i-block w_p and a u_j-block w_q such that (4) holds. As explained above, we can insert $\lambda^{p-r}(u_i^{\|u_j\|})$ on the left of w_p and $\rho^{s-q}(u_j^{\|u_i\|})$ on the right of w_q and thus obtain a word that corresponds to the vector $x' = x + \pi$.

Both inserted block sequences consist of the same number of $\|u_j\| \cdot \|u_i\|$ blocks and they cancel to 1, which means we can construct a cancelling C' from C as follows. Between the two sequences of inserted blocks, we add two-element edges so that the left-most inserted u_i-block is connected to the right-most inserted u_j-block, and so forth. The blocks that existed before are connected by edges as in C. It is clear that then, C' is a partition that is

consistent and cancelling. Moreover, since there is an edge $\{p, q\}$, the new edges between the inserted blocks do not violate well-nestedness: If there were a crossing edge, then there would have been one that crosses $\{p, q\}$. Finally, C' is clearly normal.

It remains to verify $\mathbb{P}(x, C) \subseteq \mathbb{P}(x', C')$. This, however, follows from the fact that instead of the edges that witnessed compatibility in C, we can use their counterparts in C': When going from (x, C) to (x', C'), the distance (measured in blocks) between two blocks changes by a difference that is divisible by $\|u_i\|$ and by $\|u_j\|$. Therefore, the expressions on the left-hand side of (4) evaluate to the same words. This completes the proof of the lemma.

J Lemma J.1

▶ **Lemma J.1.** *Let C be a normal cancellation. Let u_i and u_j be distinct cycles. Let $D \subseteq C$ be the set of standard edges $I \in C$ that contain one block from u_i and one block from u_j. Then the set B of blocks from u_i that are contained in some edge $I \in D$ are consecutive.*

Proof. We prove the case $i < j$, the other follows by symmetry. Suppose there are $r_1, r_2 \in B$ such that $r_1 < r_2$ and there is no $t \in B$ with $r_1 < t < r_2$.

Towards a contradiction, suppose $|r_1 - r_2| > 1$. Since $r_1, r_2 \in B$, there are $I_1, I_2 \in D$ with $r_1 \in I_1$ and $r_2 \in I_2$. Let $I_1 = \{r_1, s_1\}$ and $I_2 = \{r_2, s_2\}$. Then w_{s_1} and w_{s_2} are from u_j and by well-nestedness, we have $r_1 < r_2 < s_2 < s_1$. Since $|r_1 - r_2| > 1$, there is a t with $r_1 < t < r_2$ and therefore some $J \in C$ with $t \in J$. Since $|J| \geq 2$, there has to be a $t' \in J$, $t' \neq t$. However, well-nestedness dictates that $t' \in [r_1, s_1] \setminus [r_2, s_2]$. Since J cannot contain another block from u_i (Lemma H.1), we cannot have $t' \in [r_1, r_2]$, which only leaves $t' \in [s_2, s_1]$ and hence that $w_{t'}$ is from u_j. By the same argument, any $w_{t''}$ with $t'' \in J \setminus \{t, t'\}$ must be from u_i or u_j, contradicting Lemma H.1. This means $|J| = 2$ and thus $t \in B$, in contradiction to the choice of r_1, r_2. ◀

K Proof of Lemma 4.15

Let q be the polynomial provided by Lemma 4.14. Since x is a solution, there is a certified solution (x, C). Repeated application of Lemma 4.14 yields certified solutions $(x_0, C_0), \ldots, (x_m, C_m)$ and periods $\pi_1, \ldots, \pi_m$ such that $(x_0, C_0) = (x, C)$, $\pi_i \in \mathbb{P}(x_{i-1}, C_{i-1})$, $\mathbb{P}(x_{i-1}, C_{i-1}) \subseteq \mathbb{P}(x_i, C_i)$, $x_{i-1} = x_i + \pi_i$, and (x_m, C_m) contains at most $q(n)$ mixed cycles. In particular, $\mathbb{P}(x_m, C_m)$ contains each π_i and hence

$$x = x_m + \pi_1 + \cdots + \pi_m \in x_m + \mathbb{P}(x_m, C_m)^{\oplus}.$$

Thus, $(x', C') = (x_m, C_m)$ is the desired certified solution.

L Proof of Lemma 4.16

We shall use the concept of rational transductions. If Σ and Γ are alphabets, subsets $T \subseteq \Gamma^* \times \Sigma^*$ are called *transductions*. Given a language $L \subseteq \Sigma^*$ and a transduction $T \subseteq \Gamma^* \times \Sigma^*$, we define

$$TL = \{u \in \Gamma^* \mid (u, v) \in T \text{ for some } v \in L\}.$$

A *finite-state transducer* is a tuple $\mathcal{A} = (Q, \Sigma, \Gamma, \Delta, q_0, q_f)$, where Q is a finite set of *states*, Σ is its *input alphabet*, Γ is its *output alphabet*, Δ is a finite subset of $Q \times \Gamma^* \times \Sigma^* \times Q$, $q_0 \in Q$ is its *initial state*, and $q_f \in Q$ is its *final state*. The elements of Δ are called

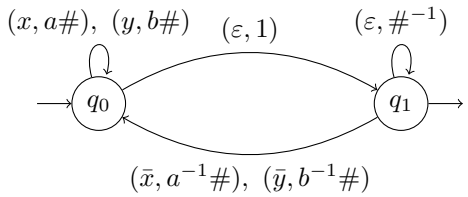

Figure 2 Transducer used in proof of Lemma 4.16

transitions. We say that a pair $(u, v) \in \Gamma^* \times \Sigma^*$ is *accepted by* $\mathcal{A}$ if there is a sequence $(p_0, u_1, v_1, p_1), (p_1, u_2, v_2, p_2), \ldots, (p_{n-1}, u_n, v_n, p_n)$ of transitions where $n \geq 1$, $p_0 = q_0$, $p_n = q_f$, $u = u_1 \cdots u_n$, and $v = v_1 \cdots v_n$. The set of all pairs $(u, v) \in \Gamma^* \times \Sigma^*$ that are accepted by $\mathcal{A}$ is denoted by $T(\mathcal{A})$. A transduction $T \subseteq \Gamma^* \times \Sigma^*$ is called *rational* if there is a finite-state transducer $\mathcal{A}$ with $T(\mathcal{A}) = T$.

Let $W_2 \subseteq \{a, b, a^{-1}, b^{-1}\}^*$ be the word problem of F_2, i.e.

$$W_2 = \{w \in \{a, b, a^{-1}, b^{-1}\}^* \mid \theta(w) = 1\}.$$

For languages $K \subseteq \Sigma^*$ and $L \subseteq \Gamma^*$, we write $K \rightsquigarrow L$ if there is a rational transduction T and a constant c such that $K = TL$ and for each $u \in K$, there is a $v \in L$ with $|v| \leq c|u|$ and $(u, v) \in T$. Observe that the relation $\rightsquigarrow$ is transitive, meaning that it suffices to show $L \rightsquigarrow W_2$ for every context-free language L.

Let D_2 be the one-sided Dyck language over two pairs of parentheses, in other words: D_2 is the smallest language $D_2 \subseteq \{x, \bar{x}, y, \bar{y}\}^*$ such that $\varepsilon \in D_2$ and whenever $uv \in D_2$, we also have $uwv \in D_2$ for $w \in \{x\bar{x}, y\bar{y}\}$.

It is easy to see that $L \rightsquigarrow D_2$ for every context-free language L. Indeed, an ε-free pushdown automaton (which exists for every context-free language [9]) for L can be converted into a transducer witnessing $L \rightsquigarrow D_2$. Therefore, it remains to show that $D_2 \rightsquigarrow W_2$.

Let F_3 be the free group of rank 3 and let $\{a, b, \#\}$ be a free generating set for F_3. As above, let

$$W_3 = \{w \in \{a, b, \#, a^{-1}, b^{-1}, \#^{-1}\}^* \mid w \text{ represents } 1 \text{ in } F_3\}$$

be the word problem of F_2. Since F_3 can be embedded into F_2 [18, Proposition 3.1], we clearly have $W_3 \rightsquigarrow W_2$. It therefore suffices to show $D_2 \rightsquigarrow W_3$.

For this, we use a construction of Kambites [13]. He proves that if $\mathcal{A}$ is the transducer in Fig. 2 and $T = T(\mathcal{A})$, then $D_2 = TW_3$. Thus, for every $u \in D_2$, we have $(u, v) \in T$ for some $v \in W_3$. An inspection of $\mathcal{A}$ yields that $|v| = 2|u| + |v|_{\#^{-1}}$ and $|v|_{\#} = |u|$. Since $v \in W_3$, we have $|v|_{\#^{-1}} = |v|_{\#}$ and thus $|v| = 3|u|$. Hence, the transduction T witnesses $D_2 \rightsquigarrow W_3$. We have thus shown $L \rightsquigarrow D_2 \rightsquigarrow W_3 \rightsquigarrow W_2$ and hence the lemma.

M Proof of Proposition 4.17

Fix a context-free language $L \subseteq \Sigma^*$ with a LogCFL-complete membership problem; such languages exist [8]. Fix a valence automaton $\mathcal{A}$ over F_2 and a constant $c \in \mathbb{N}$ such that the statement of Lemma 4.16 holds for L, $\mathcal{A}$, and c. Consider a word $w \in \Sigma^*$. From w we construct an acyclic automaton $\mathcal{B}$ over the input alphabet $\{a, b, a^{-1}, b^{-1}\}$ such that $1 \in \theta(L(\mathcal{B}))$ if and only if $w \in L$. Let $m = |w|$, $w = a_1 a_2 \cdots a_m$ and $n = c \cdot m$. The set of states of $\mathcal{B}$ is $[0, m] \times [0, n] \times Q$, where Q is the state set of $\mathcal{A}$. The transitions of $\mathcal{B}$ are defined as follows:

- $(i-1, j-1, p) \xrightarrow{x} (i, j, q)$ if $p \xrightarrow{(a_i, x)} q$ for all $i \in [1, m]$, $j \in [1, n]$, and $x \in \{a, b, a^{-1}, b^{-1}\}^*$
- $(i, j-1, p) \xrightarrow{x} (i, j, q)$ if $p \xrightarrow{(\varepsilon, x)} q$ for all $i \in [0, m]$, $j \in [1, n]$, and $x \in \{a, b, a^{-1}, b^{-1}\}^*$

The initial state of $\mathcal{B}$ is $(0, 0, q_0)$, where q_0 is the initial state of $\mathcal{A}$ and all states (m, j, q) with $j \in [0, n]$ and q final in $\mathcal{A}$ are final in $\mathcal{B}$. It is then straightforward to show that $1 \in h(L(\mathcal{B}))$ if and only if $w \in L$. The intuitive idea is that in state of $\mathcal{B}$ we store in the first component the current position in the word w. In this way we enforce to the simulation of a run of $\mathcal{A}$ on input w. In the second component of the state we store the total number of simulated $\mathcal{A}$-transitions. In this way we make $\mathcal{B}$ acyclic. Finally, the third state component of $\mathcal{B}$ stores the current $\mathcal{A}$-state.

N Proof of Lemma 5.2

For the rest of this section let $\Sigma = \{a, b, c, d, a^{-1}, b^{-1}, c^{-1}, d^{-1}\}$ and let $\theta\colon \Sigma^* \to \mathbb{G}(P_4)$ be the canonical homomorphism that maps a word over Σ to the corresponding group element.

The lemma follows easily from Lemma 5.1. Note that $[L(\mathcal{A}_1)]_I \cap [L(\mathcal{A}_2)]_I \neq \emptyset$ if and only if $1 \in \theta(L(\mathcal{A}_1)L(\mathcal{A}_2)^{-1})$ in the graph group $\mathbb{G}(\mathsf{P4})$. Moreover, it is straightforward to construct from acyclic loop automata $\mathcal{A}_1$ and $\mathcal{A}_2$ an acyclic loop automaton for $L(\mathcal{A}_1)L(\mathcal{A}_2)^{-1}$. We only have to replace every transition label w in $\mathcal{A}_2$ by w^{-1}, then reverse all transitions in $\mathcal{A}_2$ and concatenate the resulting automaton with $\mathcal{A}_1$ on the left.

O Proof of Lemma 5.3

Let Σ and θ be defined as in Appendix N.

By Lemma 5.2 it suffices to reduce for $\mathbb{G}(\mathsf{P4})$ the membership problem for acyclic loop automata to knapsack. Let $\mathcal{A} = (Q, \Sigma, \Delta, q_0, q_f)$ be an acyclic loop automaton with transitions $\Delta \subseteq Q \times \Sigma^* \times Q$. W.l.o.g. assume that $Q = \{1, \ldots, n\}$.

We reuse a construction from [16], where the rational subset membership problem for $\mathbb{G}(\mathsf{P4})$ was reduced to the submonoid membership problem for $\mathbb{G}(\mathsf{P4})$. For a state $q \in Q$ let $\widetilde{q} = (ada)^q d (ada)^{-q} \in \Sigma^*$. Let us fix the morphism $\varphi\colon \Sigma^* \to \Sigma^*$ with $\varphi(x) = xx$ for $x \in \Sigma$. For a transition $t = (p, w, q) \in \Delta$ let $\tilde{t} = \widetilde{p}\,\varphi(w)\,\widetilde{q}^{-1}$ and define $S = \{\tilde{t} \mid t \in \Delta\}^*$. In [16] it was shown that $1 \in \theta(L(A))$ if and only if $\theta(\widetilde{q_0}\,\widetilde{q_f}^{-1}) \in \theta(S)$.

We construct in polynomial time a knapsack instance over $\mathbb{G}(P_4)$ from the automaton $\mathcal{A}$ as follows: Let us choose an enumeration $t_1, t_2, \ldots, t_m$ of the transitions of $\mathcal{A}$ such that the following holds, where $t_i = (p_i, w_i, q_i)$: If $q_j = p_k$ then $j \leq k$. Since $\mathcal{A}$ is an acyclic loop automaton such an enumeration exists. The following claim proves the theorem.

Claim: $1 \in \theta(L(\mathcal{A}))$ if and only if $\theta(\widetilde{q_0}\,\widetilde{q_f}^{-1}) \in \theta(\tilde{t}_1^*\,\tilde{t}_2^* \cdots \tilde{t}_m^*)$.

One direction is clear: If $\theta(\widetilde{q_0}\,\widetilde{q_f}^{-1}) \in \theta(\tilde{t}_1^*\,\tilde{t}_2^* \cdots \tilde{t}_m^*)$, then $h(\widetilde{q_0}\,\widetilde{q_f}^{-1}) \in h(S)$. Hence, by [16] we have $1 \in \theta(L(\mathcal{A}))$. On the other hand, if $1 \in \theta(L(\mathcal{A}))$, then there exists a path in A of the form

$$q_0 = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} s_2 \cdots s_{k-1} \xrightarrow{a_k} s_k = q_f$$

such that $\theta(a_1 a_2 \cdots a_k) = 1$. Let $(s_{j-1}, a_j, s_j) = t_{i_j}$, where we refer to the above enumeration of all transitions. Then, we must have $i_1 \leq i_2 \leq \cdots \leq i_k$. Moreover, we have

$$\theta(\widetilde{q_0}\,\widetilde{q_f}^{-1}) = \theta(\widetilde{q_0}\,a_1 a_2 \cdots a_k\,\widetilde{q_f}^{-1}) = \theta(\tilde{t}_{i_1}\tilde{t}_{i_2}\cdots\tilde{t}_{i_k}) \in \theta(\tilde{t}_1^*\,\tilde{t}_2^* \cdots \tilde{t}_m^*).$$

This proves the claim and hence the theorem.