journal of Groups, Complexity, Cryptology
Volume 14, Issue 2, 2022, pp. 1:1–1:25
https://gcc.episciences.org/

Submitted Sept. 26, 2022
Published Dec. 27, 2022

EXPONENT EQUATIONS IN HNN-EXTENSIONS

MICHAEL FIGELIUS AND MARKUS LOHREY

Department of Electrical Engineering and Computer Science, University of Siegen, Germany
e-mail address: figelius@eti.uni-siegen.de

Department of Electrical Engineering and Computer Science, University of Siegen, Germany
e-mail address: lohrey@eti.uni-siegen.de

Abstract. We consider exponent equations in finitely generated groups. These are equations, where the variables appear as exponents of group elements and take values from the natural numbers. Solvability of such (systems of) equations has been intensively studied for various classes of groups in recent years. In many cases, it turns out that the set of all solutions on an exponent equation is a semilinear set that can be constructed effectively. Such groups are called knapsack semilinear. Examples of knapsack semilinear groups are hyperbolic groups, virtually special groups, co-context-free groups and free solvable groups. Moreover, knapsack semilinearity is preserved by many group theoretic constructions, e.g., finite extensions, graph products, wreath products, amalgamated free products with finite amalgamated subgroups, and HNN-extensions with finite associated subgroups. On the other hand, arbitrary HNN-extensions do not preserve knapsack semilinearity. In this paper, we consider the knapsack semilinearity of HNN-extensions, where the stable letter t acts trivially by conjugation on the associated subgroup A of the base group G. We show that under some additional technical conditions, knapsack semilinearity transfers from base group G to the HNN-extension H. These additional technical conditions are satisfied in many cases, e.g., when A is a centralizer in G or A is a quasiconvex subgroup of the hyperbolic group G.

1. Introduction

For an infinite finitely generated group G we consider equations of the form

$$h_0 g_0^{x_1} h_1 g_1^{x_2} \cdots h_n g_n^{x_n} h_{n+1} = 1 \tag{1.1}$$

where the g_i and h_i are given elements of G and the x_i are variables that range over $\mathbb{N}$ (in this paper, the natural numbers always include 0). In general, it is allowed that $x_i = x_j$ for $i \neq j$. Equations of this form are known as exponent equations and have received a lot of attention in recent years, see e.g. [2, 4, 6, 7, 8, 11, 13, 14, 15, 25, 26, 27, 28, 30, 31]. Several variants and problems have been studied in this context. The most general decision problem is to decide whether a given system of exponential equations has a solution where natural numbers are assigned to the variables x_i. This problem is known to be decidable in hyperbolic groups [26], free solvable groups [11], co-context-free groups (groups where the complement of the word problem is context-free), and virtually special groups (finite extensions of subgroups of

Key words and phrases: HNN-extensions, hyperbolic groups, knapsack problems, exponent equations.

DOI:10.46298/jgcc.2022.14.2.10521

right-angled Artin groups).[1] Many groups are known to be virtually special, e.g., Coxeter groups, fully residually free groups, one-relator groups with torsion, and fundamental groups of hyperbolic 3-manifolds.

A simpler problem is the so-called knapsack problem: In this problem the input is a single equation of the form (1.1), where all x_i are pairwise different variables, and it is asked whether a solution exists. There are groups with a decidable knapsack problem but an undecidable solvability problem for systems of exponent equations. Examples are the discrete Heisenberg group [25] and the Baumslag-Solitar group $\mathsf{BS}(1,2)$ [5, Theorem E.1]. Let us also remark that the variants of these problems, where the variables x_i range over $\mathbb{Z}$ are not harder, since one can replace a power $g_i^{x_i}$ with x_i ranging over $\mathbb{Z}$ by $g_i^{x_i}(g_i^{-1})^{y_i}$ with x_i, y_i ranging over $\mathbb{N}$.

Another problem is to describe the set of all solutions of an equation (1.1). It turned out that for many groups this set is effectively semilinear for every exponent equation;[2] such groups are called *knapsack semilinear*. First of all, for a knapsack semilinear group one can decide whether a given system of exponent equations has a solution; see [15, Lemma 3.2]. Hyperbolic groups, virtually special groups, co-context-free groups, and free solvable groups are all knapsack semilinear; see [26, Theorem 8.1] for hyperbolic groups, [15] for free solvable groups, [25] for co-context-free groups,[3] and [13] for virtually special groups. In fact, it is shown in [13] that the class of knapsack semilinear groups is closed under finite extensions, graph products, amalgamated free products with finite amalgamated subgroups, and HNN-extensions with finite associated subgroups. In addition, it is shown in [15] that the class of knapsack semilinear groups is closed under wreath products, which implies that free solvable groups are knapsack semilinear (by Magnus embedding theorem a free solvable group can be embedded in an iterated wreath product of free abelian groups and the latter are knapsack semilinear).

In this paper we want to further elaborate HNN-extensions. HNN-extensions are a fundamental operation in all areas of geometric and combinatorial group theory. A theorem of Seifert and van Kampen links HNN-extensions to algebraic topology. Moreover, HNN-extensions are used in all modern proofs for the undecidability of the word problem in finitely presented groups. For a base group G with two isomorphic subgroups A and B and an isomorphism $\varphi\colon A \to B$, the corresponding HNN-extension is the group

$$H = \langle G, t \mid t^{-1}at = \varphi(a)\,(a \in A)\rangle. \tag{1.2}$$

Intuitively, it is obtained by adjoing to G a new generator t (the *stable letter*) in such a way that conjugation of A by t realizes φ. The subgroups A and B are also called the *associated subgroups*. Recall from the above discussion that if G is knapsack semilinear and A and B are finite then also H is knapsack semilinear [13]. For arbitrary HNN-extensions, this is not true. For instance, the Baumslag-Solitar group $\mathsf{BS}(1,2) = \langle a, t \mid t^{-1}at = a^2\rangle$ is not knapsack semilinear [28] but it is an HNN-extension of the knapsack semilinear group $\langle a\rangle \cong \mathbb{Z}$. This example shows that we have to drastically restrict HNN-extensions in order to get a transfer

[1] We will state in a moment more general results which allow to decide whether a system of exponential equations has a solution in a co-context-free group or a virtually special group.

[2] A subset of $\mathbb{N}^n$ is semilinear if it is a finite union of sets of shifted subsemigroups of $(\mathbb{N}^n, +)$. Effectively semilinear means that from a given exponent equation one can effectively compute the finitely many vectors from a semilinear description of the solution set. More details on these definitions can be found in Section 2.1.

[3] Knapsack semilinearity of co-context-free groups is not explicitly shown in [25] but follows directly from the decidability proof in [25] for the knapsack problem in a co-context-free group.

result for knapsack semilinearity beyond the case of finite associated subgroups. In this paper we study HNN-extensions of the form

$$H = \langle G, t \mid t^{-1}at = a\,(a \in A)\rangle, \tag{1.3}$$

where $A \leq H$ is a subgroup. In other words, we take in (1.2) for $\varphi : A \to B$ the identity on A. Intuitively: we add to the group G a free generator t together with commutation identities $at = ta$ for all $a \in A$. This operation interpolates between the free product $G * \langle t\rangle \cong G * \mathbb{Z}$ and the direct product $G \times \langle t\rangle \cong G \times \mathbb{Z}$.

Even HNN-extensions of the form (1.3) with f.g. A are too general for our purpose: if the subgroup membership problem for A is undecidable then H has an undecidable word problem. Hence, we also need some restriction on the subgroup $A \leq G$. We say that G is knapsack semilinear relative to the subgroup A if for every expression of the form $h_0 g_0^{x_1} h_1 g_1^{x_2} \cdots h_n g_n^{x_n} h_{n+1}$ (with $g_i, h_i \in G$) the set of all tuples $(c_1, \ldots, c_n) \in \mathbb{N}^n$ such that $h_0 g_0^{c_1} h_1 g_1^{c_2} \cdots h_n g_n^{c_n} h_{n+1} \in A$ is a semilinear set. Our main result states that if the group G is (i) knapsack semilinear as well as (ii) knapsack semilinear relative to the subgroup A, then the HNN-extension H in (1.3) is knapsack semilinear. In some situations we can even avoid the explicit assumption that G is knapsack semilinear relative to the subgroup A. HNN-extensions of the form (1.3), where A is the centralizer of a single element $g \in G$ are known as *free rank one extensions of centralizers* and were first studied in [32] in the context of so-called exponential groups. It is easy to observe that if G is knapsack semilinear and $A \leq G$ is the centralizer of a finite set of elements, then G is also knapsack semilinear relative to A. In particular the operation of free rank one extension of centralizers preserves knapsack semilinearity. A corollary of this result is that every fully residually free group is knapsack semilinear. The class of fully residually free groups is exactly the class of all groups that can be constructed from $\mathbb{Z}$ by the following operations: taking finitely generated subgroups, free products and free rank one extensions of centralizers. Knapsack semilinearity of fully residually free groups also follows from the fact that every fully residually free group is virtually special [39].

In the second part of the paper, we study HNN-extensions of the form (1.3), where G is a hyperbolic group. A group is hyperbolic if all geodesic triangles in the Cayley-graph are δ-slim for a constant δ. The class of hyperbolic groups has several alternative characterizations (e.g., it is the class of finitely generated groups with a linear Dehn function), which gives hyperbolic groups a prominent role in geometric group theory. Moreover, in a certain probabilistic sense, almost all finitely presented groups are hyperbolic [17, 34]. Also from a computational viewpoint, hyperbolic groups have nice properties: it is known that the word problem and the conjugacy problem can be solved in linear time [10, 21]. In [26] it was shown that hyperbolic groups are knapsack semilinear. Here we extend this result by showing that a hyperbolic group is knapsack semilinear relative to a quasiconvex subgroup. Quasiconvex subgroups in hyperbolic groups are known to have nice properties. Many algorithmic problems are decidable for quasiconvex subgroups, including the membership problem [24], whereas Rips constructed finitely generated subgroups of hyperbolic groups with an undecidable membership problem [36].

A short version of this paper was presented at the conference ISSAC 2022 [12].

2. Preliminaries

In the following three subsections we introduce some definitions concerning semilinear sets, finite automata, and groups.

2.1. **Semilinear sets.** Fix a dimension $d \geq 1$. We extend the operations of vector addition and multiplication of a vector by a matrix to sets of vectors in the obvious way. A *linear subset* of $\mathbb{N}^d$ is a set of the form

$$L = L(b, P) = b + P \cdot \mathbb{N}^k,$$

where $b \in \mathbb{N}^d$ and $P \in \mathbb{N}^{d \times k}$. A subset $S \subseteq \mathbb{N}^d$ is *semilinear*, if it is a finite union of linear sets. The class of semilinear sets is known to be effectively closed under boolean operations; quantitative results on the descriptional complexity of boolean operations on semi-linear sets can be found in [3]. If a semilinear set S is given as a union $\bigcup_{1 \leq i \leq k} L(b_i, P_i)$, we call the tuple $\mathcal{R} = (b_1, P_1, \ldots, b_k, P_k)$ a *semilinear representation* of S.

In the context of knapsack semilinearity (which will be introduced in a moment), we will consider semilinear subsets as sets of mappings $f : \{x_1, \ldots, x_d\} \to \mathbb{N}$ for a finite set of variables $U = \{x_1, \ldots, x_d\}$. Such a mapping f can be identified with the vector $(f(x_1), \ldots, f(x_d))^\mathsf{T}$. This allows to use all vector operations (e.g. addition and scalar multiplication) on the set $\mathbb{N}^U$ of all mappings from U to $\mathbb{N}$. In general, if $*$ is a binary operation on $\mathbb{N}$ (we only use addition or multiplication for $*$) we denote with $f * g$ (for $f, g \in \mathbb{N}^U$) the pointwise extension of the operation $*$ to $\mathbb{N}^U$, i.e., $(f * g)(x) = f(x) * g(x)$ for all $x \in U$. Moreover, for mappings $f \in \mathbb{N}^U$, $g \in \mathbb{N}^V$ with $U \cap V = \emptyset$ we define $f \oplus g \in \mathbb{N}^{U \cup V}$ by $(f \oplus g)(x) = f(x)$ for $x \in U$ and $(f \oplus g)(y) = g(y)$ for $y \in V$. All operations on $\mathbb{N}^U$ will be extended to subsets of $\mathbb{N}^U$ in the standard pointwise way. For $L \subseteq \mathbb{N}^U$ and $V \subseteq U$ we denote with $L{\restriction_V}$ the set $\{f{\restriction_V} \mid f \in L\}$ obtained by restricting every function $f \in L$ to the subset V of its domain. It is easy to see that the operations $\oplus$ and ${\restriction_V}$ preserve semilinearity in an effective way.

The semilinear sets are exactly those sets that are definable in first-order logic over the structure $(\mathbb{N}, +)$ (the so-called *Presburger definable sets*). All the above mentioned closure properties of semilinear sets follow from this characterization. A good survey on semilinear results and Presburger arithmetic with references for the above mentioned results is [18].

2.2. **Regular languages, rational relations, and Parikh images.** More details on finite automata can be found in the standard textbook [23]. Let Σ be a finite alphabet of symbols. As usual, Σ^* denotes the set of all finite words over the alphabet Σ. For a word $w = a_1 a_2 \cdots a_n$ with $a_1, \ldots, a_n \in \Sigma$ we denote with $|w| = n$ the length of w. We denote the empty word (the unique word of length 0) with ε; in group theoretic contexts we also write 1 for the empty word. A *factor* of a word $w \in \Sigma^*$ is any word u such that $w = suv$ for word some words s, v.

A *finite automaton* over the alphabet Σ is a tuple $\mathcal{A} = (Q, I, \delta, F)$, where Q is a finite set of states, $I \subseteq Q$ is the set of initial states, $\delta \subseteq Q \times \Sigma \times Q$ is the set of transitions, and $F \subseteq Q$ is the set of final states. A word $w = a_1 a_2 \cdots a_n$ is accepted by $\mathcal{A}$ if there are transitions $(q_{i-1}, a_i, q_i) \in \delta$ for $1 \leq i \leq n$ such that $q_0 \in I$ and $q_n \in F$. With $L(\mathcal{A})$ (the language accepted by $\mathcal{A}$) we denote the set of all words accepted by $\mathcal{A}$. A language L is called *regular* if it is accepted by a finite automaton.

We fix an arbitrary enumeration $a_1, \ldots, a_k$ of the alphabet Σ. For $w \in \Sigma^*$ and $1 \leq i \leq k$ let $|w|_{a_i}$ be the number of occurrences of a_i in w. The *Parikh image* of w is the tuple $P(w) =$

$(|w|_{a_1}, \ldots, |w|_{a_k}) \in \mathbb{N}^k$. For a language $L \subseteq \Sigma^*$ its Parikh image is $P(L) = \{P(w) \mid w \in L\}$. The following important result was shown by Parikh [35].

Theorem 2.1. *The semilinear sets are exactly the Parikh images of the regular languages. From a given finite automaton $\mathcal{A}$ one can compute a semilinear representation of $P(L(\mathcal{A}))$.*

We will also use the following simple lemma:

Lemma 2.2 (c.f. [13, Lemma 5.8])**.** *Let $p, q, r, s, u, v \in \Sigma^*$. Then the set*

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pq^x r = su^y v\}$$

is semilinear and a semilinear representation can be computed from p, q, r, s, u, v.

A *finite state transducer* $\mathcal{T}$ over the alphabet Σ is a tuple $\mathcal{T} = (Q, I, \delta, F)$ where I and F have the same meaning as for a finite automaton and

$$\delta \subseteq (Q \times \Sigma \times \{\varepsilon\} \times Q) \cup (Q \times \{\varepsilon\} \times \Sigma \times Q).$$

A pair $(u, v) \in \Sigma^* \times \Sigma^*$ is accepted by $\mathcal{T}$ if there are transitions $(q_{i-1}, a_i, b_i, q_i) \in \delta$ for $1 \leq i \leq |u| + |v|$ (where $a_i, b_i \in \Sigma \cup \{\varepsilon\}$) such that $u = a_1 \cdots a_{|u|+|v|}$, $v = b_1 \cdots b_{|u|+|v|}$, $q_0 \in I$ and $q_{|u|+|v|} \in F$. With $R(\mathcal{T})$ we denote the set of all pairs accepted by $\mathcal{T}$. A relation $R \subseteq \Sigma^* \times \Sigma^*$ is a *rational relation* if it is accepted by a finite state transducer.

2.3. **Groups.** For more details on group theory we refer the reader to [29]. Infinite groups are usually given by presentations. Take an arbitrary non-empty set Ω and let $\Omega^{-1} = \{a^{-1} \mid a \in \Omega\}$ be a set of formal inverses such that $\Omega \cap \Omega^{-1} = \emptyset$. Let $\Sigma = \Omega \cup \Omega^{-1}$. The bijection $a \mapsto a^{-1}$ from Ω to Ω^{-1} can be extended to a natural involution $w \mapsto w^{-1}$ on Σ^*. For this we set $(a^{-1})^{-1} = a$ for $a \in \Omega$ and $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ for $a_1, \ldots, a_n \in \Sigma$. A word $w \in \Sigma^*$ is called *reduced* if it does not contain an occurrence of a word aa^{-1} or $a^{-1}a$ $(a \in \Sigma)$. Applying the cancellation rules $aa^{-1} \to \varepsilon$ or $a^{-1}a \to \varepsilon$ as long as possible, every word $w \in \Sigma^*$ can be mapped to a unique reduced word $\mathsf{red}(w)$. The *free group* $F(\Omega)$ consists of all reduced words together with the group multiplication $u \cdot v = \mathsf{red}(uv)$ for reduced words u and v. The mapping red can be also viewed as a monoid morphism from Σ^* to $F(\Omega)$. For a subset $R \subseteq \Sigma^*$ one defines the group $\langle \Sigma \mid R \rangle$ as the quotient group $F(\Omega)/N_R$, where N_R is the smallest normal subgroup that contains $\mathsf{red}(R) \subseteq F(\Omega)$. In other words, $F(\Omega)/N_R$ is the intersection of all normal subgroups of $F(\Omega)$ that contain $\mathsf{red}(R)$. Clearly, every group is (isomorphic to a group) of the form $\langle \Sigma \mid R \rangle$.

Let $G = \langle \Sigma \mid R \rangle$ in the following. If Σ is finite then G is called *finitely generated* (f.g. for short) and Σ is called a *finite symmetric generating set* for G. If both Σ and R are finite, then G is called *finitely presented*. The surjective monoid morphism $\mathsf{red} \colon \Sigma^* \to F(\Omega)$ extends to a surjective monoid morphism $h \colon \Sigma^* \to G$, called the *evaluation morphism*. For two words $u, v \in \Sigma^*$ we write $u =_G v$ if $h(u) = h(v)$. For a subset $S \subseteq G$ we write $u \in_G S$ if $h(u) \in S$.

3. Knapsack and exponent equations

Let G be a finitely generated group with the finite symmetric generating set Σ. Moreover, let X be a set of formal variables that take values from $\mathbb{N}$. For a subset $U \subseteq X$, we call a mapping $\sigma : U \to \mathbb{N}$ a *valuation* for U. An *exponent expression* over Σ is a formal expression of the form $e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ with $k \geq 1$, words $u_i, v_i \in \Sigma^*$ and exponent variables $x_1, \ldots, x_k \in X$. Here, we allow $x_i = x_j$ for $i \neq j$. We also write $e(x_1, \ldots, x_k)$ in order to

make the exponent variables explicit. We can assume that $u_i \neq \varepsilon$ for all $1 \leq i \leq k$. If every exponent variable occurs at most once in e, then e is called a *knapsack expression*. Let $X_e = \{x_1, \ldots, x_k\}$ be the set of exponent variables that occur in e. For a valuation $\sigma : U \to \mathbb{N}$ such that $X_e \subseteq U$ (in which case we also say that σ is a valuation for e), we define $\sigma(e) = v_0 u_1^{\sigma(x_1)} v_1 u_2^{\sigma(x_2)} v_2 \cdots u_k^{\sigma(x_k)} v_k \in \Sigma^*$. We say that σ is a *G-solution* of the equation $e = 1$ if $\sigma(e) =_G 1$ holds. With $\mathsf{sol}_G(e)$ we denote the set of all G-solutions $\sigma : X_e \to \mathbb{N}$ of e. We can view $\mathsf{sol}_G(e)$ as a subset of $\mathbb{N}^m$ for $m = |X_e| \leq k$. We define *solvability of systems of exponent equations over G* as the following decision problem:

Input: A finite list of exponent expressions $e_1, \ldots, e_n$ over Σ.
Question: Is $\bigcap_{1 \leq i \leq n} \mathsf{sol}_G(e_i)$ non-empty?

The *knapsack problem for G* is the following decision problem:

Input: A single knapsack expression e over Σ.
Question: Is $\mathsf{sol}_G(e)$ non-empty?

It is easy to observe that the concrete choice of the generating set Σ has no influence on the decidability and complexity status of these problems.

For the above decision problems one could restrict to exponent expressions of the form $e = u_1^{x_1} u_2^{x_2} \cdots u_k^{x_k} v$: for $e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ and

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

we have $\sigma(e) =_G \sigma(e')$ for every valuation σ.

The group G is called *knapsack semilinear* if for every knapsack expression e over Σ, the set $\mathsf{sol}_G(e)$ is a semilinear set of vectors and a semilinear representation can be effectively computed from e. This implies that for every exponent expression e over Σ, the set $\mathsf{sol}_G(e)$ is semilinear as well and a semilinear representation can be effectively computed from e. This fact can be easily deduced from the known effective closure properties of semilinear set, see e.g. [13].

Since the semilinear sets are effectively closed under intersection, solvability of systems of exponent equations is decidable for every knapsack semilinear group. As mentioned in the introduction, the class of knapsack semilinear groups is very rich. Examples of a groups, where knapsack is decidable but solvability of systems of exponent equations is undecidable are the Heisenberg group $H_3(\mathbb{Z})$ (the group of all upper triangular (3×3)-matrices over the integers, where all diagonal entries are 1) [25] and the Baumslag-Solitar group $\mathsf{BS}(1,2)$ [5, 28, Theorem E.1]. These groups are not knapsack semilinear in a strong sense: there are knapsack expressions e such that $\mathsf{sol}_{H_3(\mathbb{Z})}(e)$ (resp. $\mathsf{sol}_{\mathsf{BS}(1,2)}(e)$) is not semilinear.

Let $S \subseteq G$. We say that G is *knapsack semilinear relative to S* if for every knapsack expression e over Σ, the set $\{\sigma : X_e \to \mathbb{N} \mid \sigma(e) \in_G S\}$ is a semilinear set of vectors and a semilinear representation can be effectively computed from e. We are mainly interested in the case where S is a subgroup of G. For sets $\{S_1, \ldots, S_k\} \subseteq G$ we say that G is knapsack semilinear relative to $\{S_1, \ldots, S_k\}$ if for every $1 \leq i \leq k$, G is knapsack semilinear relative to S_i. Note that G is knapsack semilinear if and only if it is knapsack semilinear relative to 1.

4. HNN-extensions

In this section we introduce the important operation of HNN-extension. Suppose $G = \langle \Sigma \mid R \rangle$ is a finitely generated group with the finite symmetric generating set $\Sigma = \Omega \cup \Omega^{-1}$ and $R \subseteq \Sigma^*$.

Fix two isomorphic subgroups A and B of G together with an isomorphism $\varphi\colon A \to B$. Let $t \notin \Sigma$ be a new letter. Then the corresponding *HNN-extension* is the group

$$H = \langle \Sigma \cup \{t, t^{-1}\} \mid R \cup \{t^{-1}a^{-1}t\varphi(a) \mid a \in A\}\rangle$$

(formally, we identify here every element $g \in A \cup B$ with a word over Σ that evaluates to g). This group is usually denoted by

$$H = \langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle. \tag{4.1}$$

Intuitively, H is obtained from G by adding a new element t such that conjugating elements of A with t applies the isomorphism φ. Here, t is called the *stable letter* and the groups A and B are the *associated subgroups*. A basic fact about HNN-extensions is that the group G embeds naturally into H [20].

In this paper, we consider HNN-extensions $H = \langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle$, where $A \leq G$ is a subgroup of $G = \langle \Sigma \mid R\rangle$ and $\varphi : A \to A$ is the identity mapping. Thus, H can be written as

$$H = \langle G, t \mid t^{-1}at = a\ (a \in A)\rangle. \tag{4.2}$$

Let us fix this HNN-extension for the further consideration. Let us denote with

$$h : (\Sigma \cup \{t, t^{-1}\})^* \to H$$

the evaluation morphism.

A word $u \in (\Sigma \cup \{t, t^{-1}\})^*$ is called *Britton-reduced* if it does not contain a factor of the form $t^{-\alpha}wt^{\alpha}$ with $\alpha \in \{-1, 1\}$, $w \in \Sigma^*$ and $w \in_G A$. A factor of the form $t^{-\alpha}wt^{\alpha}$ with $\alpha \in \{-1, 1\}$, $w \in \Sigma^*$ and $w \in_G A$ is also called a *pin*, which we can replace by w. Since this decreases the number of t's in the word, we can reduce every word to an equivalent Britton-reduced word. We denote the set of all Britton-reduced words in the HNN-extension (4.2) by $\mathsf{BR}(H)$. For $u \in (\Sigma \cup \{t, t^{-1}\})^*$ we define $\pi_t(u)$ as the projection of the word u onto the alphabet $\{t, t^{-1}\}$ and $\pi_\Sigma(u)$ as the projection of the word u onto the alphabet Σ. Britton's lemma states that if $u =_H 1$ ($u \in (\Sigma \cup \{t, t^{-1}\})^*$) then u contains a pin or $u \in \Sigma^*$ and $u =_G 1$. Note that a consequence of this is that if $u \in_H G$ then u contains a pin or $u \in \Sigma^*$. To see this, note that $u \in_H G$ implies that $uv =_H 1$ for a word $v \in \Sigma^*$. Britton's lemma implies that uv must contain a pin (i.e., u must contain a pin) or $uv \in \Sigma^*$ (i.e., $u \in \Sigma^*$). In particular, a Britton-reduced word that contains $t^{\pm 1}$ cannot represent an element of the base group G.

Note that $H/N(t) \cong G$, where $N(t)$ is the smallest normal subgroup of H containing t. By $\pi_G : H \to G$ we denote the canonical projection. We have $\pi_G(g_0t^{\delta_1}g_1 \cdots t^{\delta_k}g_k) = g_0g_1 \cdots g_k$ for $g_0, \ldots, g_k \in G$. Hence, on the level of words, π_G is computed by the projection $\pi_\Sigma : (\Sigma \cup \{t, t^{-1}\})^* \to \Sigma^*$.

Lemma 4.1. *Let $w \in (\Sigma \cup \{t, t^{-1}\})^*$. Then $w =_H 1$ if and only if $w \in_H G$ and $\pi_\Sigma(w) =_G 1$.*

Proof. If $w =_H 1$, i.e., $h(w) = 1$, then clearly $w \in_H G$. Moreover, by Britton's lemma, w can be reduced to a word from Σ^* using Britton reduction. But this word must be $\pi_\Sigma(w)$. Hence, we have $\pi_\Sigma(w) =_G 1$. On the other hand, if $w \in_H G$ and $\pi_\Sigma(w) =_G 1$, then, again, w can be reduced to $\pi_\Sigma(w) =_G 1$ using Britton reduction, which implies $w =_H 1$. □

We will also need the following lemma (cf. Lemma 2.3 of [19]):

Lemma 4.2. *Assume that $u = u_0t^{\delta_1}u_1 \cdots t^{\delta_k}u_k$ and $v = v_0t^{\varepsilon_1}v_1 \cdots t^{\varepsilon_\ell}v_\ell$ are Britton-reduced words with $u_i, v_j \in \Sigma^*$. Let $0 \leq m \leq \max\{k, \ell\}$ be the largest number such that*

- *$\delta_{k-i} = -\varepsilon_{i+1}$ for all $0 \leq i \leq m-1$ and*

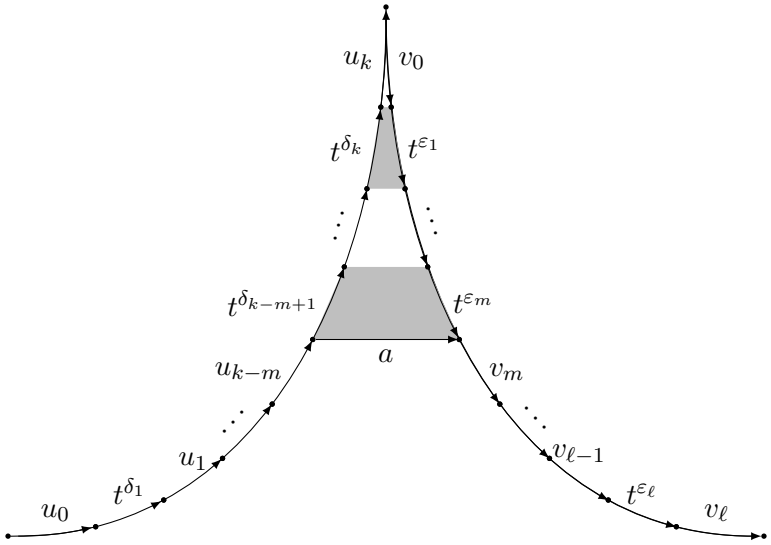

Figure 1: The situation from Lemma 4.2.

- $u_{k-i+1} \cdots u_k v_0 \cdots v_{i-1} \in_G A$ *for all* $0 \leq i \leq m$ *(for* $i = 0$ *this condition is trivially satisfied).*

Then $w := u_0 t^{\delta_1} u_1 \cdots t^{\delta_{k-m}} (u_{k-m} \cdots u_k v_0 \cdots v_m) t^{\varepsilon_{m+1}} v_{m+1} \cdots t^{\varepsilon_\ell} v_\ell$ *is a Britton-reduced word with* $w =_H uv$.

The above lemma is visualized in Figure 1, where

$$a = u_{k-m+1} \cdots u_k v_0 \cdots v_{m-1} \in_H A.$$

5. Knapsack semilinearity of HNN-extensions

The goal of this section is show that the HNN-extension (4.2) is knapsack semilinear provided G is knapsack semilinear relative to $\{1, A\}$. We first introduce some concepts that can be found in a similar form in [13].

We call a word $w \in \mathsf{BR}(H)$ *well-behaved*, if w^m is Britton-reduced for every $m \geq 0$. Note that w is well-behaved if and only if w and w^2 are Britton-reduced. Note that every word $w \in \Sigma^*$ is well-behaved.

Lemma 5.1 (c.f. [13, Lemma 6.3])**.** *From a given word* $u \in \mathsf{BR}(H)$ *we can compute words* $s, p, v \in \mathsf{BR}(H)$ *such that* $u^m =_H sv^m p$ *for every* $m \geq 0$ *and* v *is well-behaved.*

In the following we assume that G is knapsack semilinear relative to $\{1, A\}$. For a knapsack expression $e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ over the alphabet $\Sigma \cup \{t, t^{-1}\}$ we define the knapsack expression

$$\pi_\Sigma(e) = \pi_\Sigma(v_0)\pi_\Sigma(u_1)^{x_1}\pi_\Sigma(v_1)\pi_\Sigma(u_2)^{x_2}\pi_\Sigma(v_2)\cdots\pi_\Sigma(u_k)^{x_k}\pi_\Sigma(v_k)$$

over the alphabet Σ.

For an exponent expression $e(x_1, \ldots, x_n)$ over the alphabet $\Sigma \cup \{t, t^{-1}\}$ we call

$$e(x_1, \ldots, x_n) \in_H G$$

a *G-constraint*. If e is an exponent expression over the alphabet Σ, then $e \in_G A$ is called an A-constraint. Since G is knapsack semilinear relative to A, the set of solutions of an A-constraint is semilinear.

Lemma 5.2. *Let $u, v \in \mathsf{BR}(H)$ be well-behaved, u' (resp., v'') be a proper prefix of u (resp., v) and u'' (resp., v') be a proper suffix of u (resp., v). Let $e = e(z_1, \ldots, z_k)$ be a knapsack expression over the alphabet Σ. Then the set of all $(x, y, z_1, \ldots, z_k) \in \mathbb{N}^{k+2}$ such that the G-constraint*

$$u''u^x u' e(z_1, \ldots, z_k)\, v'v^y v'' \in_H G \tag{5.1}$$

holds is semilinear and a semilinear representation can be effectively computed from the words $u, v, u', u'', v', v'', e$.

Proof. We first claim that by cyclically rotating u and v we can assume that $u'' = v'' = \varepsilon$. We only prove this for u'', for v'' we can argue analogously. We can write $u = ru''$ for some word r. Then for all $x \in \mathbb{N}$ we have $u''u^x u' = u''(ru'')^x u' = (u''r)^x u''u'$. The word $u''u'$ is either a prefix of $u''r$ or we can write $u''u' = (u''r)\tilde{u}$ for some prefix $\tilde{u}$ of $u''r$. In the first case, we can simply replace $u''u^x u'$ in (5.1) by $(u''r)^x u''u'$ (note that $u''r$ is well-behaved since it is a cyclic rotation of the well-behaved word $u = ru''$). In the second case (where $u''u' = (u''r)\tilde{u}$ for some prefix $\tilde{u}$ of $u''r$), we replace $u''u^x u'$ in (5.1) by $(u''r)^x \tilde{u}$. If $L \subseteq \mathbb{N}^{\{x,y,z_1,\ldots,z_k\}}$ is the set of solutions of the resulting G-constraint, then the formula $(x+1, y, z_1, \ldots, z_k) \in L$ describes the set of solution of (5.1). Clearly, a Presburger formula for L immediately yields a Presburger formula for $(x+1, y, z_1, \ldots, z_k) \in L$.

By the previous paragraph, it suffices to consider the set of solutions of the G-constraint

$$u^x u' e(z_1, \ldots, z_k)\, v'v^y \in_H G.$$

This constraint holds (for certain values of $x, y, z_1, \ldots, z_k$) if and only if $u^x u' e(z_1, \ldots, z_k)\, v'v^y$ can be Britton-reduced to a word from Σ^* which must be $\pi_\Sigma(u^x u' e(z_1, \ldots, z_k)\, v'v^y)$. Since u^x and v^y are Britton-reduced for every $x, y \in \mathbb{N}$ we can apply Lemma 4.2.

Let S_u be the set of suffixes of u that start with $t^{\pm 1}$ and let P_v be the set of prefixes of v that end with $t^{\pm 1}$. We define $S_{u'}$ and $P_{v'}$ analogously. Then by Lemma 4.2 the following formula is equivalent to $u^x u' e(z_1, \ldots, z_n)\, v'v^y \in_H G$ (as usual, $\wedge$ denotes logical conjunction and $\Rightarrow$ denotes logical implication):

$$\begin{aligned}
&\pi_t(u^x u') = \pi_t(v'v^y)^{-1} \ \wedge \\
&\forall x' < x\, \forall y' < y : \bigwedge_{s \in S_u} \bigwedge_{p \in P_v} \pi_t(s\, u^{x'} u') = \pi_t(v'v^{y'}p)^{-1} \ \Rightarrow\ \pi_\Sigma(s\, u^{x'} u'\, e\, v'v^{y'}p) \in_G A \\
&\qquad\qquad \bigwedge_{s \in S_u} \bigwedge_{p \in P_{v'}} \pi_t(s\, u^{x'} u') = \pi_t(p)^{-1} \ \Rightarrow\ \pi_\Sigma(s\, u^{x'} u'\, e\, p) \in_G A \\
&\qquad\qquad \bigwedge_{s \in S_{u'}} \bigwedge_{p \in P_v} \pi_t(s) = \pi_t(v'v^{y'}p)^{-1} \ \Rightarrow\ \pi_\Sigma(s\, e\, v'v^{y'}p) \in_G A \\
&\qquad\qquad \bigwedge_{s \in S_{u'}} \bigwedge_{p \in P_{v'}} \pi_t(s) = \pi_t(p)^{-1} \ \Rightarrow\ \pi_\Sigma(s\, e\, p) \in_G A.
\end{aligned}$$

Let us explain the intuition behind this formula; see also Figure 2 which shows a van Kampen diagram for $u^8 u' e(z_1, \ldots, z_k)\, v'v^5 =_H g$.

The formula $\pi_t(u^x u') = \pi_t(v'v^y)^{-1}$ expresses that every t (resp., t^{-1}) in $u^x u'$ cancels with a t^{-1} (resp., t) in $v'v^y$. If this is not the case, then $u^x u' e(z_1, \ldots, z_k)\, v'v^y$ cannot be

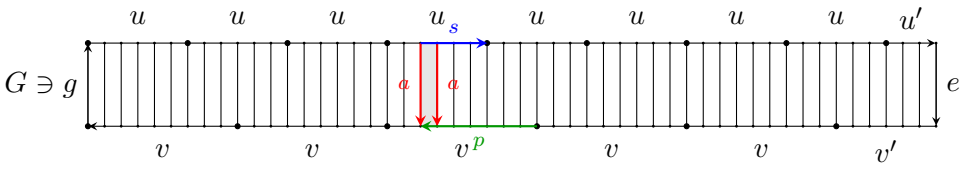

Figure 2: The idea behind the proof of Lemma 5.2. The fact that all vertical lines represent elements from the subgroup A is expressed by the formula from the proof.

Britton-reduced to a word over Σ. The other four lines of the formula ensure that the Britton-reduction of $u^x u' e(z_1, \ldots, z_k)\, v' v^y$ to a word over Σ actually exists. This Britton-reduction proceeds from right to left in Figure 2. In each reduction step, the right-most slice in Figure 2 is eliminated. Assume that the Britton-reduction has already eliminated the part to the right of the shaded slice. The special form of our HNN-extension (4.2) implies that if a word $w \in (\Sigma \cup \{t, t^{-1}\})^*$ is Britton-reduced to a word over Σ, then we have $w =_H \pi_\Sigma(w)$ (every Britton-reduction step is of the form $t^{-1}at \to a$ or $tat^{-1} \to a$ for $a \in A$). Hence, we must have $a =_G \pi_\Sigma(s\, u^4 u'\, e\, v' v^2 p)$ in Figure 2. In order to eliminate the shaded slice, the following must hold:

- a must belong to the subgroup A, i.e., $\pi_\Sigma(s\, u^4 u'\, e\, v' v^2 p) \in_G A$,
- the first letter of s (a suffix of u) must be t (or t^{-1}), and
- the last letter of p (a prefix of v) must be t^{-1} (or t); note that v goes from right to left.

The second line in the above formula ensures that $\pi_\Sigma(s\, u^{x'} u'\, e\, v' v^{y'} p) \in_G A$ whenever $x' < x$, $y' < y$, s is a suffix of u that starts with $t^{\pm 1}$, p is a prefix of v that ends with $t^{\pm 1}$ and $\pi_t(s\, u^{x'} u') = \pi_t(v' v^{y'} p)^{-1}$ holds. This ensures that $s\, u^{x'} u'\, e\, v' v^{y'} p$ is the group element represented by one of the vertical edges in Figure 2. The other parts of the above formula deal with the cases where the vertical edge has an endpoint in u' or v'. Altogether this ensures that all the vertical edges in Figure 2 represent elements of the subgroup A.

By Lemma 2.2 the solution set of the equation $\pi_t(u^x u') = \pi_t(v' v^y)^{-1}$ (which is interpreted over the free monoid $\{t, t^{-1}\}^*$) is semilinear. To see this let $w = v^{-1}$ and $w' = (v')^{-1}$. Then $\pi_t(u^x u') = \pi_t(v' v^y)^{-1}$ is equivalent to $\pi_t(u)^x \pi_t(u') = \pi_t(w)^y \pi_t(w')$. For the same reason, also the equation $\pi_t(s\, u^{x'} u') = \pi_t(v' v^{y'} p)^{-1}$ is equivalent to a semilinear constraint. The solution sets of the equations $\pi_t(s) = \pi_t(v' v^{y'} p)^{-1}$ and $\pi_t(s) = \pi_t(v' v^{y'} p)^{-1}$ are finite. Moreover, each of the A-constraints ($\pi_\Sigma(s\, u^{x'} u'\, e\, v' v^{y'} p) \in_G A$ etc.) is equivalent to a semilinear constraint because G is knapsack semilinear relative to A. Hence, the above formula is equivalent to a Presburger formula and therefore defines a semilinear set. □

Remark 5.3. There are variations of Lemma 5.2, where the G-constraint has one of the following forms:

$$u' e(z_1, \ldots, z_k)\, v' v^y v'' \in_H G,$$
$$u' u^x u'' e(z_1, \ldots, z_k)\, v' \in_H G,$$
$$\text{or } u' e(z_1, \ldots, z_k)\, v' \in_H G$$

with u, u', u'', v, v', v'' as in Lemma 5.2. In all cases, the set of solutions of the G-constraint can be shown to be effectively semilinear using the arguments from the proof of Lemma 5.2.

Definition 5.4. We define a reduction relation on tuples over $\mathsf{BR}(H)$ of arbitrary length. Take $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$ and $1 \leq i < j \leq m$. Then we have

$$(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(u_j), u_{j+1}, \ldots, u_m)$$

if $\pi_t(u_i) \neq \varepsilon \neq \pi_t(u_j)$, $u_{i+1} \cdots u_{j-1} \in \Sigma^*$ and $u_i u_{i+1} \cdots u_{j-1} u_j \in_H G$. Note that this implies that $u_i u_{i+1} \cdots u_{j-1} u_j =_H \pi_\Sigma(u_i) u_{i+1} \cdots u_{j-1} \pi_\Sigma(u_j)$. A concrete sequence of such rewrite steps leading to a tuple where all entries belong to Σ^* is a *G-reduction* of the initial tuple, and the initial tuple is called *G-reducible*. We also say that u_i and u_j *matched in a G-reduction*.

A G-reduction of a tuple $(u_1, u_2, \ldots, u_m)$ can be seen as a witness for the fact that $u_1 u_2 \cdots u_m \in_H G$. On the other hand, $u_1 u_2 \cdots u_m \in_H G$ does not necessarily imply that $(u_1, u_2, \ldots, u_m)$ has a G-reduction. But we can show that $u_1 u_2 \cdots u_m \in_H G$ implies that $(u_1, u_2, \ldots, u_m)$ can refined (by factorizing the u_i) such that the resulting refined tuple has a G-reduction. Moreover, it is important that we have an upper bound on the length of the refined tuple ($4m$ in Lemma 5.5 below) that only depends on m and not on the words $u_1, u_2, \ldots, u_m$.

We say that the tuple $(v_1, v_2, \ldots, v_n)$ is a *refinement* of the tuple $(u_1, u_2, \ldots, u_m)$ if there exist factorizations $u_i = u_{i,1} \cdots u_{i,k_i}$ in $(\Sigma \cup \{t, t^{-1}\})^*$ such that $k_i = 1$ whenever $u_i \in \Sigma^*$ and $(v_1, v_2, \ldots, v_n) = (u_{1,1}, \ldots, u_{1,k_1}, \ldots, u_{m,1}, \ldots, u_{m,k_m})$.

Lemma 5.5. *Let $m \geq 2$ and $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$. If $u_1 u_2 \cdots u_m \in_H G$, then there exists a G-reducible refinement of $(u_1, u_2, \ldots, u_m)$ that has length at most $4m$.*

Proof. Let $\overline{u} = (u_1, u_2, \ldots, u_m)$. Let us define $\gamma(\overline{u})$ as the number of pairs (i, j) with $1 \leq i < j \leq m$ such that $u_i u_{i+1} \cdots u_j$ is not Britton-reduced and $u_{i+1} \cdots u_{j-1} \in \Sigma^*$. Note that $\pi_t(u_i) \neq \varepsilon \neq \pi_t(u_j)$ for such a pair (i, j). Moreover, if we have two pairs (i, j) and (k, ℓ) of this form, then either $j \leq k$ or $\ell \leq i$. Let $\tau(\overline{u})$ be the number of i such that $\pi_t(u_i) \neq \varepsilon$.

We prove by induction over $\gamma(\overline{u}) + \tau(\overline{u})$ that there exists a G-reducible refinement of $\overline{u}$ that has length at most $2\gamma(\overline{u}) + \tau(\overline{u}) + m \leq 4m$.

The case $m = 2$ is trivial: either $\gamma(u_1, u_2) = \tau(u_1, u_2) = 0$ and $u_1, u_2 \in \Sigma^*$ or $\gamma(u_1, u_2) = 1$, $\tau(u_1, u_2) = 2$ in which case (u_1, u_2) must reduce in one step to $(\pi_\Sigma(u_1), \pi_\Sigma(u_2))$. If $m \geq 3$ then $u_1 u_2 \cdots u_m$ must contain a pin. Since every u_i is Britton-reduced, there must exist $i < j$ such that $u_i u_{i+1} \cdots u_j$ is not Britton-reduced and $u_{i+1} \cdots u_{j-1} \in \Sigma^*$. By Lemma 4.2 we can factorize u_i and u_j in $(\Sigma \cup \{t, t^{-1}\})^*$ as $u_i = u_i' r$ and $u_j = s u_j'$ such that $rs \in_H G$ and $u_i u_{i+1} \cdots u_{j-1} u_j =_H u_i' \pi_\Sigma(r) u_{i+1} \cdots u_{j-1} \pi_\Sigma(s) u_j'$ is Britton-reduced. Note that r and s must contain t or t^{-1}. Moreover, we can assume that either $u_i' = \varepsilon$ or u_i' ends with $t^{\pm 1}$ (if u_i' ends with a non-empty word over Σ, we can remove this word from u_i' and add it to r) and, similarly, either $u_j' = \varepsilon$ or u_j' begins with $t^{\pm 1}$.

Case 1. u_i' and u_j' both contain $t^{\pm 1}$. Then we have

$$\gamma(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) < \gamma(\overline{u})$$

since $u_i' \pi_\Sigma(r) u_{i+1} \cdots u_{j-1} \pi_\Sigma(s) u_j'$ is Britton-reduced and u_i' and u_j' both contain $t^{\pm 1}$. Moreover, we have

$$\tau(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) = \tau(\overline{u}).$$

Hence, we can apply the induction hypothesis to the tuple

$$(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m). \tag{5.2}$$

It must have a G-reducible refinement of length at most

$$2(\gamma(\overline{u}) - 1) + \tau(\overline{u}) + m + 2 = 2\gamma(\overline{u}) + \tau(\overline{u}) + m.$$

In this refinement $\pi_\Sigma(r), \pi_\Sigma(s) \in \Sigma^*$ will not be factorized into more than one factor. We therefore can take the refinement of (5.2) and replace $\pi_\Sigma(r)$ and $\pi_\Sigma(s)$ by r and s, respectively. This leads to a G-reducible of our original tuple $\overline{u}$ having length at most $2\gamma(\overline{u}) + \tau(\overline{u}) + m$.

Case 2. $u_i' = \varepsilon$ and u_j' begins with $t^{\pm 1}$. Then we have

$$\gamma(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) \leq \gamma(\overline{u})$$

and

$$\tau(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) < \tau(\overline{u}).$$

We can therefore apply the induction hypothesis to the tuple

$$(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) \tag{5.3}$$

and obtain a G-reducible refinement of length at most

$$2\gamma(\overline{u}) + \tau(\overline{u}) - 1 + m + 1 = 2\gamma(\overline{u}) + \tau(\overline{u}) + m.$$

Replacing $\pi_\Sigma(u_i)$ by u_i and $\pi_\Sigma(s)$ by s in this refinement yields a G-reducible refinement of $\overline{u}$.

The remaining cases where (i) $u_j' = \varepsilon$ and u_i' ends with $t^{\pm 1}$ or (ii) $u_i' = u_j' = \varepsilon$ are analogous to case 2. This concludes the proof of the lemma. □

Now we are able to prove the main theorem of this section.

Theorem 5.6. *Let $H = \langle G, t \mid t^{-1}at = a \ (a \in A)\rangle$ be an HNN-extension, where G is knapsack semilinear relative to $\{1, A\}$. Then H is knapsack semilinear.*

Proof. The proof of the theorem is based on ideas from [13]. Consider a knapsack expression

$$e(x_2, x_4, \ldots, x_m) = u_1 u_2^{x_2} u_3 u_4^{x_4} u_5 \cdots u_m^{x_m} u_{m+1}$$

with m even (later it will convenient to have only variables with an even index). We can assume that all u_i are Britton reduced. Moreover, by Lemma 5.1, we can assume that every u_i with i even is well-behaved and moreover non-empty (otherwise we can remove the power $u_i^{x_i}$).

In the following we describe an algorithm that computes a semilinear representation of $\mathsf{sol}_H(e)$ in three main steps. The algorithm transforms logical statements into equivalent logical statements (we do not have to define the precise logical language; the meaning of the statements should be always clear). Every statement contains the variables $x_2, x_4, \ldots, x_m$ from our knapsack expression and equivalence of two statements means that for every valuation $\sigma : \{x_2, x_4, \ldots, x_m\} \to \mathbb{N}$ the two statements yield the same truth value. We start with the statement $e(x_2, x_4, \ldots, x_m) =_H 1$ and end with a Presburger formula. In each of the three steps we transform the current statement Φ into an equivalent disjunction $\bigvee_{i=1}^n \Phi_i$. We can therefore view the whole process as a branching tree of depth three, where the nodes are labelled with statements. If a node is labelled with Φ and its children are labelled with $\Phi_1, \ldots, \Phi_n$ then Φ is equivalent to $\bigvee_{i=1}^n \Phi_i$. The leaves of the tree are labelled with Presburger formulas with free variables $x_2, x_4, \ldots, x_m$. We will concentrate on a single branch of this tree, which can be viewed as a sequence of nondeterministic guesses.

Let $N_\Sigma \subseteq [1, m+1]$ be the set of indices such that $u_i \in \Sigma^*$ and let $N_t = [1, m+1] \setminus N_\Sigma$ be the set of indices such that $\pi_t(u_i) \neq \varepsilon$. Moreover, let us define $w_i = u_i$ for i odd and $w_i = u_i^{x_i}$ for i even.

By Lemma 4.1, $e =_H 1$ is equivalent to $e \in_H G \wedge \pi_\Sigma(e) =_G 1$. Since G is knapsack semilinear, the set $\mathsf{sol}_G(\pi_\Sigma(e))$ is semilinear. Hence, it suffices to show that the set of all $(x_2, x_4, \ldots, x_m) \in \mathbb{N}^{m/2}$ with $e(x_2, x_4 \ldots, x_m) \in_H G$ is semilinear. Here, we will use the assumption that G is knapsack semilinear relative to A.

Step 1: Applying Lemma 5.5. We construct a disjunction Ψ from the knapsack expression e using Lemma 5.5. More precisely, we construct Ψ by nondeterministically guessing the following data:

(i) symbolic factorizations $w_i = y_{i,1} \cdots y_{i,k_i}$ in $(\Sigma \cup \{t, t^{-1}\})^*$ for all $i \in [1, m+1]$. Here the $y_{i,j}$ are existentially quantified variables that take values in $\mathsf{BR}(H)$. Later, these variables will be eliminated. The guessed k_i must satisfy $k_i \geq 1$ for all i, $k_i = 1$ for all $i \in N_\Sigma$, and $\sum_{1 \leq i \leq m+1} k_i \leq 4(m+1)$.

(ii) a G-reduction (according to Definition 5.4) of the tuple

$$(y_{1,1} \cdots y_{1,k_1}, \ldots, y_{m+1,1} \cdots y_{m+1,k_{m+1}}).$$

For the w_i with i odd we can of course guess concrete words for the variables $y_{i,1}, \ldots, y_{i,k_i}$. Later, we will do this, but in order to simplify the notation, we will still use the names $y_{i,1}, \ldots, y_{i,k_i}$ for these words.

For every specific guess in (i) and (ii) we write down the conjunction of the following formulas:

- the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ from (i) (every variable $y_{i,j}$ is existentially quantified) and
- all G-constraints that result from G-reduction steps in the guessed G-reduction (this will made more precise in Step 2 below).

The formula Ψ is the disjunction of the above existentially quantified conjunctions, taken over all possible guesses in (i) and (ii). This formula is equivalent to the G-constraint $e \in_H G$.

Step 2: Eliminating the equations $w_i = y_{i,1} \cdots y_{i,k_i}$. For an odd i (i.e., $w_i = u_i$) we can eliminate this equation by guessing a concrete factorization $u_i = u_{i,1} \cdots u_{i,k_i}$ and then replace the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ by the conjunction

$$\bigwedge_{j=1}^{k_i} y_{i,j} = u_{i,j}.$$

For an even i (i.e., $w_i = u_i^{x_i}$) we can eliminate the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ by guessing a symbolic factorization of $u_i^{x_i}$ into k_i factors. A specific guess leads to a formula

$$\bigwedge_{j=1}^{k_i} y_{i,j} = u''_{i,j} u_i^{x_{i,j}} u'_{i,j+1} \ \wedge \ x_i = c_i + \sum_{j=1}^{k_i} x_{i,j}. \tag{5.4}$$

Here, every $u'_{i,j}$ $(2 \leq j \leq k_i)$ is a proper prefix of u_i and every $u''_{i,j}$ $(2 \leq j \leq k_i)$ is a proper suffix of u_i such that either $u_i = u'_{i,j} u''_{i,j}$ or $u'_{i,j} = u''_{i,j} = \varepsilon$ for all $2 \leq j \leq k_i$. We set $u'_{i,k_i+1} = u''_{i,1} = \varepsilon$ in the above formula. Moreover, c_i is the number of $2 \leq j \leq k_i$ for which $u'_{i,j} \neq \varepsilon \neq u''_{i,j}$ holds. The $u'_{i,j}$ and $u''_{i,j}$ are nondeterministically guessed.

We also guess which of the new exponent variables $x_{i,j}$ are zero and which of the $x_{i,j}$ are non-zero. If we guess $x_{i,j} = 0$, then we replace $x_{i,j}$ in (5.4) by 0. This yields the equation

$y_{i,j} = u''_{i,j}u'_{i,j+1}$. If we guess $x_{i,j} > 0$, then we add this constraint to (5.4). After this step, it is determined whether a $y_{i,j}$ contains t or t^{-1} (for i even as well as for i odd). Those $y_{i,j}$ must be matched by G-reduction steps in the G-reduction that we guessed in Step 1. In fact, what we guessed in Step 1 is such a matching.

Step 3: Eliminating G-constraints. Assume that $y_{i,j}$ and $y_{k,\ell}$ are matched in the guessed G-reduction. W.l.o.g. assume that $i < k$ or $i = k$ and $j < \ell$, i.e., (i,j) is lexicographically before (k,ℓ). Then our formula contains the G-constraint

$$y_{i,j}\left(\prod_{(i,j)\prec(p,q)\prec(k,\ell)} \pi_\Sigma(y_{p,q})\right) y_{k,\ell} \in_H G,$$

where $\prec$ is the strict lexicographic order on pairs of natural numbers. In this constraint, we can replace every $y_{a,b}$ with a even by $u''_{i,j}u_i^{x_{i,j}}u'_{i,j+1}$ (or $u''_{a,b}u'_{a,b+1}$ in case $x_{i,j} = 0$ was guessed), whereas every $y_{a,b}$ with a odd can be replaced by the concrete word $u_{a,b}$. If both $y_{i,j}$ and $y_{k,\ell}$ contain an exponent variable we obtain a G-constraint of the form (5.1). If $y_{i,j}$ or $y_{k,\ell}$ is a concrete word we obtain a G-constraint having one of the three forms listed in Remark 5.3. Lemma 5.2 and Remark 5.3 imply that in each case, the set of solutions of the G-constraint is semilinear. This concludes the proof of the theorem. □

For a subset $S \subseteq G$ of the group G one defines the *centralizer*

$$C(S) = \{h \in G \mid gh = hg \text{ for all } g \in S\}.$$

The HNN-extension $H = \langle G, t \mid t^{-1}at = a\,(a \in C(S))\rangle$ is an *extension of the centralizer* $C(S)$. Extensions of centralizers were first studied in [32] in the context of exponential groups.

Theorem 5.7. *If G is knapsack semilinear and H is an extension of a centralizer $C(S)$ with S finite, then H is knapsack semilinear as well.*

Proof. We have to show that G is also knapsack semilinear relative to $C(S)$. Let $e = e(x_1, \ldots, x_n)$ be a knapsack expression. Then $e \in_G C(S)$ is equivalent to $\bigwedge_{a\in S} ea =_G ae$. Note that $ea =_G ae$ is equivalent to $eae^{-1}a^{-1} =_G 1$ and $eae^{-1}a^{-1}$ is an exponent expression. Since G is knapsack semilinear and semilinear sets are closed under finite intersections, the set of solutions of $\bigwedge_{a\in S} ea = ae$ is semilinear. □

Remark 5.8. It is straightforward to generalize Theorem 5.6 to a multiple HNN-extension

$$H = \langle G, t_1, \ldots, t_n \mid t_i^{-1}at_i = a\ (a \in A_i, 1 \le i \le n)\rangle.$$

If G is knapsack semilinear relative to $\{1, A_1, \ldots, A_n\}$ then H is knapsack semilinear.

6. Quasi-convex subgroups of hyperbolic groups

In this section we show that hyperbolic groups are knapsack semilinear relative to quasiconvex subgroups. We start with the definition hyperbolic groups.

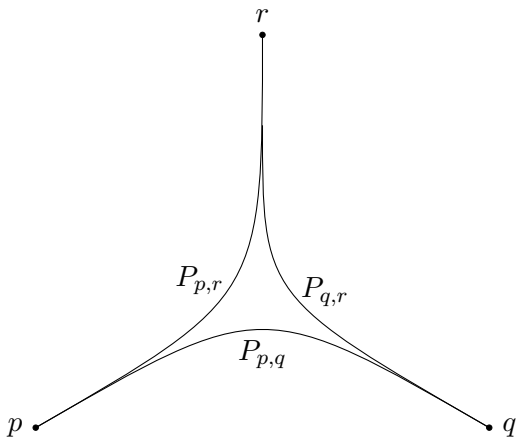

Figure 3: The shape of a geodesic triangle in a hyperbolic group

6.1. **Cayley-graphs and hyperbolic groups.** Let G be a finitely generated group with the finite symmetric generating set Σ and let $h : \Sigma^* \to G$ be the evaluation morphism. The *Cayley-graph* of G (with respect to Σ) is the graph $\Gamma = \Gamma(G)$ with node set G and all edges (g, ga) for $g \in G$ and $a \in \Sigma$. We view Γ as a geodesic metric space, where every edge (g, ga) is identified with a unit-length interval. It is convenient to label the directed edge from g to ga with the generator a. Note that since Σ is symmetric, there is also an edge from ga to g labelled with a^{-1}. Therefore one can view Γ as an undirected graph. The distance between two points p, q is denoted with $d_\Gamma(p, q)$. For $g \in G$ let $|g| = d_\Gamma(1, g)$. For $\kappa \geq 0$ and $g \in G$ let $\mathcal{B}_\kappa(g) = \{h \in G \mid d_\Gamma(g, h) \leq \kappa\}$ be the ball of radius κ around g.

Paths can be defined in a very general way for metric spaces, but we only need paths that are induced by words over Σ. Given a word $w = a_1 a_2 \cdots a_n$ (with $a_i \in \Sigma$), one obtains a unique path $P[w] : [0, n] \to \Gamma$, which is a continuous mapping from the real interval $[0, n]$ to Γ. It maps the subinterval $[i, i+1] \subseteq [0, n]$ isometrically onto the edge $(h(a_1 \cdots a_i), h(a_1 \cdots a_{i+1}))$ of Γ. The path $P[w]$ starts in 1 and ends in $h(w)$ (the group element represented by w). We also say that $P[w]$ is the unique path that starts in 1 and is labelled with the word w. More generally, for $g \in G$ we denote with $g \cdot P[w]$ the path that starts in g and is labelled with w. When writing $u \cdot P[w]$ for a word $u \in \Sigma^*$, we mean the path $h(u) \cdot P[w]$. A path $P : [0, n] \to \Gamma$ of the above form is *geodesic* if $d_\Gamma(P(0), P(n)) = n$ and it is a (λ, ϵ)-*quasigeodesic* if for all points $p = P(a)$ and $q = P(b)$ we have $|a - b| \leq \lambda \cdot d_\Gamma(p, q) + \varepsilon$.

A word $w \in \Sigma^*$ is geodesic if the path $P[w]$ is geodesic, which means that there is no shorter word representing the same group element from G. Similarly, we define the notion of (λ, ϵ)-quasigeodesic words. A set (or language) of words $L \subseteq \Sigma^*$ is called geodesic (resp., (λ, ϵ)-quasigeodesic), if every $w \in L$ is geodesic (resp., (λ, ϵ)-quasigeodesic).

A *geodesic triangle* consists of three points $p, q, r \in G$ and geodesic paths $P_1 = P_{p,q}$, $P_2 = P_{p,r}$, $P_3 = P_{q,r}$ (the three sides of the triangle), where $P_{x,y}$ is a geodesic path from x to y. We call a geodesic triangle δ-*slim* for $\delta \geq 0$, if for all $i \in \{1, 2, 3\}$, every point on P_i has distance at most δ from a point on $P_j \cup P_k$, where $\{j, k\} = \{1, 2, 3\} \setminus \{i\}$. The group G is called δ-*hyperbolic*, if every geodesic triangle is δ-slim. Finally, G is hyperbolic, if it is δ-hyperbolic for some $\delta \geq 0$. Figure 3 shows the shape of a geodesic triangle in a hyperbolic group. Finitely generated free groups are for instance 0-hyperbolic with respect to a free finite

generating set. The property of being hyperbolic is independent of the chosen generating set Σ. The word problem for every hyperbolic group can be decided in real time [21].

6.2. **Asynchronous biautomatic structures.** Let G be a f.g. group with the finite symmetric generating set Σ and let $h : \Sigma^* \to G$ be the evaluation morphism. An *asynchronous biautomatic structure* for G consists of a regular language $L \subseteq \Sigma^*$ such that the following holds; see also [9, 33]:

- $G = h(L)$,
- the relation $\{(u, v) \in L \times L \mid u =_G v\}$ is rational, and
- for every generator $a \in \Sigma$ the relations

$$\{(u, v) \in L \times L \mid ua =_G v\} \text{ and } \{(u, v) \in L \times L \mid au =_G v\}$$

are rational.

If in the last point it is only required that the relation $\{(u, v) \in L \times L \mid ua =_G v\}$ is rational, then L is called an asynchronous automatic structure for G. A f.g. group G is called asynchronously (bi)automatic if it has an asynchronous (bi)automatic structure. We need the following lemma.

Lemma 6.1. *Let L be an asynchronous biautomatic structure for G, let L_1 and L_2 be regular subsets of L and let $v_1, v_2 \in \Sigma^*$. Then the relation*

$$\{(u_1, u_2) \in L_1 \times L_2 \mid v_1u_1 =_G u_2v_2\}$$

is rational. Moreover, a finite state transducer for this relation can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

Proof. It suffices to show that the relation $R := \{(u_1, u_2) \in L \times L \mid v_1u_1 =_G u_2v_2\}$ is rational. The corresponding finite state transducer can in addition simulate the automaton for L_1 (resp., L_2) on the first (resp., second) tape. Rationality of the relation R can be shown by induction on $|v_1| + |v_2|$. The case $v_1 = v_2 = \varepsilon$ is clear. Assume w.l.o.g. that $v_1 \neq \varepsilon$ and let $v_1 = v_1'a$ with $a \in \Sigma$. By induction, the relation $R_1 = \{(u_1', u_2) \in L \times L \mid v_1'u_1' =_G u_2v_2\}$ is rational. Moreover, the relation $R_2 = \{(u_1, u_1') \in L \times L \mid au_1 =_G u_1'\}$ is rational as well. Finally, we have $R = R_2 \circ R_1$, where $\circ$ is relational composition. The lemma follows since the class of rational relations is closed under relational composition [38]. □

We also need the following result from [22]:

Lemma 6.2. *Let G be a hyperbolic group and let Σ be a finite symmetric generating set for G. Let λ and ϵ be fixed constants. Then the set of all (λ, ϵ)-quasigeodesic words over the alphabet Σ is an asynchronous biautomatic structure for G.*

In [22] it is only stated that the set of all (λ, ϵ)-quasigeodesic words is an asynchronous automatic structure for G. But since for every (λ, ϵ)-quasigeodesic word $w \in \Sigma^*$ also w^{-1} is (λ, ϵ)-quasigeodesic, it follows easily that the set of all (λ, ϵ)-quasigeodesic words is an asynchronous biautomatic structure for G. With Lemma 6.1 we obtain the following lemma.

Lemma 6.3. *Let G be a hyperbolic group with the finite symmetric generating set Σ and let λ and ϵ be fixed constants. Assume that $L_1, L_2 \subseteq \Sigma^*$ are (λ, ϵ)-quasigeodesic regular languages and $v_1, v_2 \in \Sigma^*$. Then the relation*

$$\{(u_1, u_2) \in L_1 \times L_2 \mid v_1u_1 =_G u_2v_2\}$$

is rational. Moreover, a finite state transducer for this relation can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

6.3. **Parikh images in hyperbolic groups.** Let us fix a hyperbolic group G with the finite symmetric generating set Σ for the rest of the section. We fix an arbitrary enumeration $a_1, \ldots, a_k$ of the alphabet Σ in order to make Parikh images well-defined. Recall that the semilinear sets are exactly the Parikh images of regular languages; see Theorem 2.1. Together with Lemma 6.3 we obtain the next result.

Lemma 6.4. *Let G be a hyperbolic group with the finite symmetric generating set Σ and let λ and ϵ be fixed constants. Assume that $L_1, L_2 \subseteq \Sigma^*$ are (λ, ϵ)-quasigeodesic regular languages and $v_1, v_2 \in \Sigma^*$. Then the set*

$$\{(P(u_1), P(u_2)) \in \mathbb{N}^{2k} \mid u_1 \in L_1, u_2 \in L_2, v_1 u_1 =_G u_2 v_2\} \tag{6.1}$$

is semilinear. Moreover, a semilinear representation for this set can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

Proof. Let $\Sigma' = \{a' \mid a \in \Sigma\}$ be a disjoint copy of the alphabet Σ. By Lemma 6.3 there is a finite state transducer $\mathcal{T}$ for the relation

$$\{(u_1, u_2) \in L_1 \times L_2 \mid v_1 u_1 =_G u_2 v_2\}.$$

From $\mathcal{T}$ we obtain a finite automaton $\mathcal{A}$ over the alphabet $\Sigma \cup \Sigma'$ by replacing every transition (p, a, ε, q) by (p, a, q) and every transition (p, ε, a, q) by (p, a', q). For the alphabet $\Sigma \cup \Sigma'$ we take the enumeration $a_1, \ldots, a_k, a'_1, \ldots, a'_k$. With this enumeration, the set (6.1) is the Parikh image of the language $L(\mathcal{A})$. Hence, the lemma follows from Theorem 2.1. □

6.4. **The main result.** We now come to the main technical result of this section.

Theorem 6.5. *Let G be a hyperbolic group with the finite symmetric generating set $\Sigma = \{a_1, \ldots, a_k\}$. Fix constants ϵ, λ. For $1 \leq i \leq n$ let $L_i \subseteq \Sigma^*$ be a regular (λ, ϵ)-quasigeodesic language. Then the set*

$$\{(P(w_1), \ldots, P(w_n)) \in \mathbb{N}^{nk} \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 w_2 \cdots w_n =_G 1\}$$

is semilinear and a semilinear representation of this set can be computed from finite automata for $L_1, \ldots, L_n$.

We postpone the proof of Theorem 6.5 and first derive some corollaries.

Theorem 6.6. *Let G be hyperbolic and let $S \subseteq \Sigma^*$ be a regular geodesic set. Then G is knapsack semilinear relative to $h(S)$, where $h : \Sigma^* \to G$ is the evaluation morphism.*

Proof. Let e be a knapsack expression over Σ. We want to find a semilinear representation for the set

$$\{\sigma : X_e \to \mathbb{N} \mid \exists w \in S : \sigma(e) =_G w\} = \bigcup_{w \in S} \mathsf{sol}_G(ew^{-1}). \tag{6.2}$$

In a first step we show that we can assume that for every power u^x that appears in e ($x \in X_e$) the language u^* is (λ, ϵ)-quasigeodesic for fixed constants λ, ϵ that only depend on the group G. For this we use [26, Proposition 8.4]. It states that from our given knapsack expression e

one can compute a finite list of knapsack expressions $e_1, \ldots, e_n$ with $X_{e_i} \subseteq X_e$ for $1 \leq i \leq n$, functions $m_i, d_i : X_{e_i} \to \mathbb{N}$ and semilinear sets $\mathcal{F}_i \subseteq \mathbb{N}^{X_e \setminus X_{e_i}}$ such that

$$\mathsf{sol}_G(e) = \bigcup_{1 \leq i \leq n} (m_i \cdot \mathsf{sol}_G(e_i) + d_i) \oplus \mathcal{F}_i. \tag{6.3}$$

Moreover, every knapsack expression e_i has the property that for every power u^x that appears in e_i, the language u^* is (λ, ϵ)-quasigeodesic for some fixed constants λ, ϵ that only depend on the group G.

Consider now for an arbitrary word $w \in S$ the knapsack expression ew^{-1}. From the construction in [26, Proposition 8.4], it follows that

$$\mathsf{sol}_G(ew^{-1}) = \bigcup_{1 \leq i \leq n} (m_i \cdot \mathsf{sol}_G(e_i w^{-1}) + d_i) \oplus \mathcal{F}_i. \tag{6.4}$$

The reason is that in the proof of [26, Proposition 8.4], every e_i is computed from e by replacing every power u^x in e either by a fixed power u^k for some $k \in \mathbb{N}$ or by $v\tilde{u}^x v'$ for a (λ, ϵ)-quasigeodesic word $\tilde{u}$ and words v and v'. The same replacements are also made for ew^{-1}. Therefore, the set (6.2) is equal to

$$\begin{aligned} \bigcup_{w \in S} \mathsf{sol}_G(ew^{-1}) &= \bigcup_{w \in S} \bigcup_{1 \leq i \leq n} (m_i \cdot \mathsf{sol}_G(e_i w^{-1}) + d_i) \oplus \mathcal{F}_i \\ &= \bigcup_{1 \leq i \leq n} \left(m_i \cdot \left(\bigcup_{w \in S} \mathsf{sol}_G(e_i w^{-1}) \right) + d_i \right) \oplus \mathcal{F}_i. \end{aligned}$$

The closure properties of semilinear sets imply that the set (6.2) is semilinear provided the set

$$\bigcup_{w \in S} \mathsf{sol}_G(e_i w^{-1}) = \{\sigma : X_{e_i} \to \mathbb{N} \mid \exists w \in S : \sigma(e_i) =_G w\}$$

is semilinear for all $1 \leq i \leq n$.

This shows that it suffices to find a semilinear representation of (6.2) for a knapsack expression $e = v_0 u_1^{x_1} v_1 u_1^{x_1} \cdots u_n^{x_n} v_n$ where all u_i have the property that u_i^* is a regular (λ, ϵ)-quasigeodesic language. Clearly, we can also assume that every u_i is non-empty and every v_i is geodesic. Moreover, since S is regular and geodesic, it is easy to see that also S^{-1} is regular and geodesic.

Let $(L_1, \ldots, L_m)$ be the tuple of languages $(\{v_0\}, u_1^*, \{v_1\}, \ldots, u_n^*, \{v_n\}, S^{-1})$ (with $m = 2(n+1)$). All these languages are regular and (λ, ϵ)-quasigeodesic. By Theorem 6.5, the set

$$\{(P(w_1), \ldots, P(w_m)) \in \mathbb{N}^{mk} \mid w_i \in L_i \text{ for } 1 \leq i \leq m, w_1 \cdots w_m =_G 1\}$$

is semilinear and a semilinear representation of this set can be computed. Applying a projection yields a semilinear representation of the set

$$\begin{aligned} \{(P(w_1), \ldots, P(w_n)) \in \mathbb{N}^{nk} \mid\ & w_i \in u_i^* \text{ for } 1 \leq i \leq n, \\ & \exists w \in S : v_0 w_1 v_1 \cdots w_n v_n =_G w\}. \end{aligned}$$

Choose for every u_i a symbol $a_{j_i} \in \Sigma$ such that $\ell_i := |u_i|_{a_{j_i}} > 0$ (recall that $u_i \neq \varepsilon$). Then we project every $P(w_i)$ in the above set to the j_i-th coordinate. The resulting projection is

$$\{(\ell_1 \cdot x_1, \ldots, \ell_n \cdot x_n) \in \mathbb{N}^n \mid\ \exists w \in S : v_0 u_1^{x_1} v_1 \cdots u_n^{x_n} v_n =_G w\}.$$

The semilinearity of this set easily implies the semilinearity of the set

$$\{(x_1, \ldots, x_n) \in \mathbb{N}^n \mid \exists w \in S : v_0 u_1^{x_1} v_1 \cdots u_n^{x_n} v_n =_G w\}.$$

This concludes the proof. □

A subset $A \subseteq G$ is called *quasiconvex* if there exists a constant $\kappa \geq 0$ such that every geodesic path from 1 to some $g \in A$ is contained in $\bigcup_{h \in A} B_\kappa(h)$. The following result can be found in [16] (h denotes the evaluation morphism):

Lemma 6.7. *A subset $A \subseteq G$ is quasiconvex if and only if the language of all geodesic words in $h^{-1}(A)$ is regular.*

Theorem 6.8. *Let G be hyperbolic and let H be a quasiconvex subgroup of G. Then G is knapsack semilinear relative to H.*

Proof. Fix a finite symmetric generating set Σ for G and let h be the evaluation morphism. By Lemma 6.7 the set of all geodesic words in $h^{-1}(H)$ is a geodesic regular language. By Theorem 6.6, G is knapsack semilinear relative to H. □

It is known that every finitely generated free group F is locally quasiconvex, which means that every finitely generated subgroup of F is quasiconvex.

Corollary 6.9. *Let G be a finitely generated free group and let H be a finitely generated subgroup of G. Then G is knapsack semilinear relative to H.*

This corollary can actually be generalized. Schupp proved that a group G, which is virtually an orientable surface group of genus at least two or virtually a Coxeter group satisfying a certain reduction hypothesis, is locally quasiconvex [37, Theorem IV]. Since these groups are hyperbolic, it follows that the groups considered by Schupp are knapsack semilinear relative to any finitely generated subgroup.

Theorems 5.6 and 6.8 yield the following result:

Corollary 6.10. *Let $H = \langle G, t \mid t^{-1}at = a \ (a \in A)\rangle$ be an HNN-extension where G is hyperbolic and $A \leq G$ is a quasiconvex subgroup of G. Then H is knapsack semilinear.*

It is known that every cyclic subgroup of a hyperbolic group is quasiconvex, see e.g. [1]. Hence, for every element $a \in G$ of a hyperbolic group G, the HNN-extension $\langle G, t \mid t^{-1}at = a\rangle$ is knapsack semilinear. It is also known that if the hyperbolic group G is non-elementary (i.e., it contains a copy of the free group F_2) then the centralizer of an element $g \in G$ is cyclic [1, Lemma 2]. Hence, we obtain Theorem 5.7 for the case of a centralizer of a single element in a non-elementary hyperbolic group.

7. Proof of Theorem 6.5

We now come to the proof of Theorem 6.5. Let G be δ-hyperbolic. For $1 \leq i \leq n$ let $L_i \subseteq \Sigma^*$ be a regular (λ, ϵ)-quasigeodesic language. Let $\mathcal{A}_i = (Q_i, S_i, \delta_i, T_i)$ be a finite automaton for L_i. Without loss of generality, we can assume that every $q \in Q_i$ belongs to a path from some initial state $q_0 \in S_i$ to some final state $q_1 \in T_i$. This ensures that every word that labels a path from a state p to a state q is a factor of a word from L_i. Since factors of (λ, ϵ)-quasigeodesic words are (λ, ϵ)-quasigeodesic as well, it follows that every word that labels a path between two states of $\mathcal{A}_i$ is (λ, ϵ)-quasigeodesic.

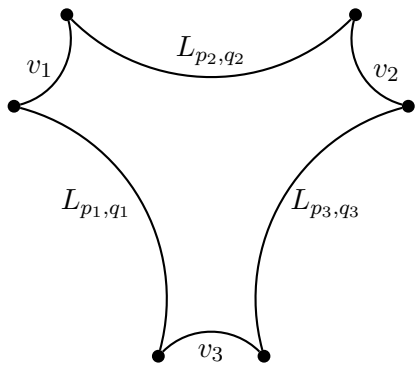

Figure 4: The $2n$-gon for $n = 3$ from the proof of Theorem 6.5

We want to show that the set

$$\{(P(w_1), \ldots, P(w_n)) \in \mathbb{N}^{nk} \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 w_2 \cdots w_n =_G 1\}$$

is semilinear. For this, we prove a slightly more general statement: For words $v_1, \ldots, v_n \in \Sigma^*$ we consider the set

$$\{(P(w_1), \ldots, P(w_n)) \in \mathbb{N}^{nk} \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 v_1 \cdots w_n v_n =_G 1\}.$$

By induction over n we show that this set is semilinear. For the case $n = 2$ we can directly use Lemma 6.4. This also covers the case $n = 1$ since we can take $L_2 = \{1\}$.

Now assume that $n \geq 3$. We can assume that the words v_i are geodesic. Define the automaton $\mathcal{A}$ as the disjoint union of the automata $\mathcal{A}_i$. Thus, the state set of $\mathcal{A}$ is $Q = \biguplus_{1 \leq i \leq n} Q_i$ and the transition set of $\mathcal{A}$ is $\delta = \biguplus_{1 \leq i \leq n} \delta_i$ (the sets of initial and final states of $\mathcal{A}$ are not important). Let us denote for $p, q \in Q$ with $L_{p,q}$ the set of all finite words that label a path from p to q in the automaton $\mathcal{A}$. The above properties of the automata $\mathcal{A}_i$ ensure that every language $L_{p,q}$ is (λ, ϵ)-quasigeodesic. Note that $L_i = \bigcup_{p \in S_i, q \in T_i} L_{p,q}$. Since the semilinear sets are effectively closed under union, it suffices to show for states $p_i, q_i \in Q$ $(1 \leq i \leq n)$ that the following set is semilinear:

$$\{(P(w_1), \ldots, P(w_n)) \in \mathbb{N}^{nk} \mid w_i \in L_{p_i,q_i} \text{ for } 1 \leq i \leq n, w_1 v_1 \cdots w_n v_n =_G 1\}.$$

In the following, we denote this set with $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$. We will construct a Presburger formula with free variables $x_{i,j}$ $(1 \leq i \leq n,\ 1 \leq j \leq k)$ for this set. The variables $x_{i,j}$ with $1 \leq j \leq k$ encode the Parikh image of the words from L_{p_i,q_i}. Let us write $\bar{x}_i = (x_{i,j})_{1 \leq j \leq k}$ in the following.

Recall from Section 6.1 the definition of the path $P[w]$ for a word $w \in \Sigma^*$. Consider a tuple $(w_1, \ldots, w_n) \in \prod_{i=1}^n L_{p_i,q_i}$ with $w_1 v_1 w_2 v_2 \cdots w_n v_n =_G 1$ and the corresponding $2n$-gon that is defined by the (λ, ϵ)-quasigeodesic paths $P_i = (w_1 v_1 \cdots w_{i-1} v_{i-1}) \cdot P[w_i]$ and the geodesic paths $Q_i = (w_1 v_1 \cdots w_i) \cdot P[v_i]$, see Figure 4 for the case $n = 3$. Since all paths P_i and Q_i are (λ, ϵ)-quasigeodesic, we can apply [31, Lemma 6.4]: Every side of the $2n$-gon is contained in the κ-neighborhoods of the other sides, where $\kappa = \xi + \xi \log(2n)$ for a constant ξ that only depends on the constants $\delta, \lambda, \varepsilon$.

Let us now consider the side P_2 of the quasigeodesic $2n$-gon. It is labelled with a word from L_{p_2,q_2}. Its neighboring sides are Q_1 and Q_2, which are labelled with v_1 and v_2, respectively. We distinguish several cases. In each case we cut the $2n$-gon into smaller pieces along paths of length $\leq \kappa$ (length $2\kappa + 1$ in Case 2). When we speak of a point on the $2n$-gon,

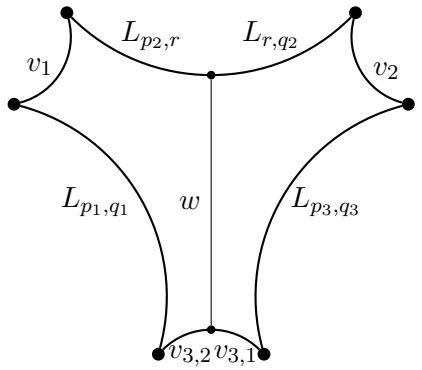

Figure 5: Case 1.1 from the proof of Theorem 6.5

we mean a node of the Cayley graph (i.e., an element of the group G) and not a point in the interior of an edge.

For each of the following six cases we construct a Presburger formula describing a semilinear set. The union of these six sets is $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$.

Case 1: There is a point $a \in P_2$ that has distance at most κ from a point b that does not belong to $P_1 \cup Q_1 \cup Q_2 \cup P_3$. Thus b must belong to one of the paths $Q_3, P_4, \ldots Q_{n-1}, P_n, Q_n$. Let w be a geodesic word of length at most κ that labels a path from a to b. There are two subcases:

Case 1.1: b belongs to a path Q_i with $3 \leq i \leq n$. The situation is shown in Figure 5 for $n = i = 3$. Let T be the set of all tuples $(r, v_{i,1}, v_{i,2}, w)$ such that $r \in Q$, $v_i = v_{i,1}v_{i,2}$, and $w \in \Sigma^*$ is of length at most κ. By induction, the following two sets are semilinear for every tuple $t = (r, v_{i,1}, v_{i,2}, w) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_1, q_1, v_1, p_2, r, wv_{i,2}, p_{i+1}, q_{i+1}, v_{i+1}, \ldots, p_n, q_n, v_n), \\ S_{t,2} &= P(r, q_2, v_2, p_3, q_3, v_3, \ldots, p_i, q_i, v_{i,1}w^{-1}). \end{aligned}$$

Intuitively, $S_{t,1}$ corresponds to the $2(n-1)$-gon (when $wv_{i,2}$ is viewed as a single side) on the left of the w-labelled edge in Figure 5, whereas $S_{t,2}$ corresponds to the $2(n-1)$-gon on the right of the w-labelled edge. We then define the formula

$$A_{1.1} = \bigvee_{t \in T} \exists \bar{y}_2, \bar{z}_2 : (\bar{x}_1, \bar{y}_2, \bar{x}_{i+1}, \ldots, \bar{x}_n) \in S_{t,1} \ \wedge \ (\bar{z}_2, \bar{x}_3, \ldots, \bar{x}_i) \in S_{t,2} \ \wedge \ \bar{x}_2 = \bar{y}_2 + \bar{z}_2.$$

Here $\bar{y}_2$ and $\bar{z}_2$ are k-tuples of new variables. The Presburger formula $A_{1.1}$ is one of the six formulas whose union is $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$.

Case 1.2: b belongs to the path P_i, where $4 \leq i \leq n$ (this case can only occur if $n \geq 4$). This case is analogous to Case 1.1. Let T be the set of all tuples (r, r', w) such that $r, r' \in Q$ and $w \in \Sigma^*$ is of length at most κ. By induction, the following two sets are semilinear for every tuple $t = (r, r', w) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_1, q_1, v_1, p_2, r, w, r', q_i, v_i, p_{i+1}, q_{i+1}, v_{i+1}, \ldots, p_n, q_n, v_n), \\ S_{t,2} &= P(r, q_2, v_2, p_3, q_3, v_3, \ldots, p_{i-1}, q_{i-1}, v_{i-1}, p_i, r', w^{-1}). \end{aligned}$$

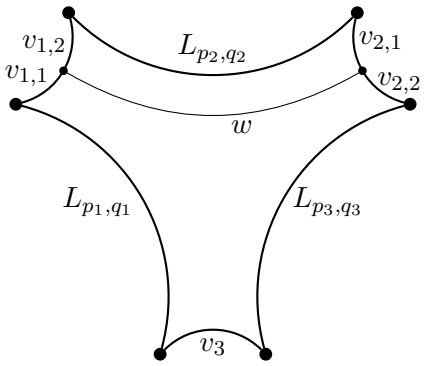

Figure 6: Case 2.1 from the proof of Theorem 6.5

Moreover, let $A_{1.2}$ be the formula

$$A_{1.2} = \bigvee_{t \in T} \exists \bar{y}_2, \bar{z}_2, \bar{y}_i, \bar{z}_i : (\bar{x}_1, \bar{y}_2, \bar{z}_i, \bar{x}_{i+1}, \ldots, \bar{x}_n) \in S_{t,1} \wedge (\bar{z}_2, \bar{x}_3, \ldots, \bar{x}_{i-1}, \bar{y}_i) \in S_{t,2} \wedge \bar{x}_2 = \bar{y}_2 + \bar{z}_2 \ \wedge \ \bar{x}_i = \bar{y}_i + \bar{z}_i.$$

Case 2: Every point on P_2 has distance at most κ from a point on $P_1 \cup Q_1 \cup Q_2 \cup P_3$. Since the starting point of P_2 has distance $0 \leq \kappa$ from $P_1 \cup Q_1$ and the end point of P_2 has distance $0 \leq \kappa$ from $Q_2 \cup P_3$, there must be points b_1 on $P_1 \cup Q_1$, b on P_2, and b_2 on $Q_2 \cup P_3$ such that the distance between b_1 and b is at most κ and the distance between b and b_2 is at most $\kappa + 1$. Hence, the distance between b_1 and b_2 is at most $2\kappa + 1$. Let w be a word that labels a geodesic path from b_1 to b_2 (thus, $|w| \leq 2\kappa + 1$). This leads to the following four subcases.

Case 2.1: $b_1 \in Q_1$ and $b_2 \in Q_2$. This case is shown in Figure 6. Let T be the set of all tuples $(v_{1,1}, v_{1,2}, w, v_{2,1}, v_{2,2})$ such that $v_1 = v_{1,1}v_{1,2}$, $v_2 = v_{2,1}v_{2,2}$ and $w \in \Sigma^*$ is of length at most $2\kappa + 1$. By induction, the following two sets are semilinear for every tuple $t = (v_{1,1}, v_{1,2}, w, v_{2,1}, v_{2,2}) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_2, q_2, v_{2,1}w^{-1}v_{1,2}), \\ S_{t,2} &= P(p_1, q_1, v_{1,1}wv_{2,2}, p_3, q_3, v_3, \ldots, p_n, q_n, v_n). \end{aligned}$$

We define the formula

$$A_{2.1} = \bigvee_{t \in T} \bar{x}_2 \in S_{t,1} \ \wedge \ (\bar{x}_1, \bar{x}_3 \ldots, \bar{x}_n) \in S_{t,2}.$$

Case 2.2: $b_1 \in P_1$ and $b_2 \in Q_2$, see Figure 7. This case is exactly the same as Case 1.1 with $i = 3$, if we replace the side P_2 in Case 1.1 by P_1; see Figure 5.

Case 2.3: $b_1 \in Q_1$ and $b_2 \in P_3$. This case is analogous to Case 2.2.

Case 2.4: $b_1 \in P_1$ and $b_2 \in P_3$, see Figure 8. Let T be the set of all tuples $(w_1, w_2, w, r_1, r_2, r_3)$ such that $|w| \leq 2\kappa + 1$, $|w_1| \leq \kappa$, $|w_2| \leq \kappa + 1$, $w = w_1^{-1}w_2$ in G, and $r_1, r_2, r_3 \in Q$. By induction, the following three sets are semilinear for every tuple $t = (w_1, w_2, w, r_1, r_2, r_3) \in T$:

$$\begin{aligned} S_{t,1} &= P(r_1, q_1, v_1, p_2, r_2, w_1), \\ S_{t,2} &= P(r_2, q_2, v_2, p_3, r_3, w_2^{-1}), \\ S_{t,3} &= P(p_1, r_1, w, r_3, q_3, v_3, p_4, q_4, v_4, \ldots, p_n, q_n, v_n). \end{aligned}$$

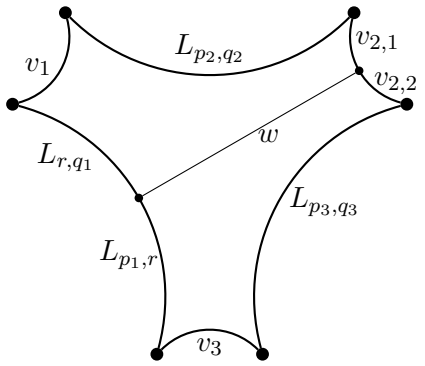

Figure 7: Case 2.2 from the proof of Theorem 6.5

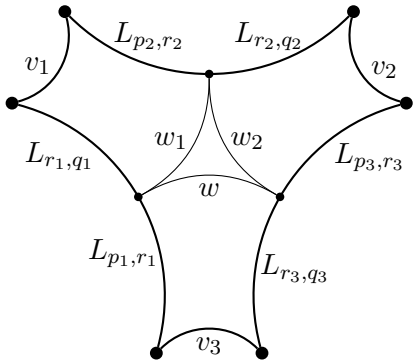

Figure 8: Case 2.4 from the proof of Theorem 6.5

We define the formula

$$A_{2.4} = \bigwedge_{t\in T} \exists \bar{y}_1, \bar{z}_1, \bar{y}_2, \bar{z}_2, \bar{y}_3, \bar{z}_3 : (\bar{z}_1, \bar{y}_2) \in S_{t,1} \ \wedge \ (\bar{z}_2, \bar{y}_3) \in S_{t,2} \ \wedge \\ (\bar{y}_1, \bar{z}_3, \bar{x}_4, \ldots, \bar{x}_n) \in S_{t,3} \ \wedge \ \bigwedge_{i=1}^{3} \bar{x}_i = \bar{y}_i + \bar{z}_i.$$

This concludes the case distinction.

A tuple $(\bar{x}_1, \ldots, \bar{x}_n) \in \mathbb{N}^{nk}$ belongs to the set $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$ if and only if $A_{1.1} \vee A_{1.2} \vee A_{2.1} \vee A_{2.2} \vee A_{2.3} \vee A_{2.4}$ holds. This yields a Presburger formula for $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$. □

Acknowledgment

Both authors were supported by the DFG research project LO 748/12-1.

References

[1] Goulnara N. Arzhantseva. On quasiconvex subgroups of word hyperbolic groups. *Geometriae Dedicata*, 87:191–208, 2001. doi:10.1023/A:1012040207144.

[2] László Babai, Robert Beals, Jin-Yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the 7th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 1996*, pages 498–507. ACM/SIAM, 1996. http://dl.acm.org/citation.cfm?id=313852.314109.

[3] Simon Beier, Markus Holzer, and Martin Kutrib. On the descriptional complexity of operations on semilinear sets. In *Proceedings of the 15th International Conference on Automata and Formal Languages, AFL 2017*, volume 252 of *EPTCS*, pages 41–55, 2017. doi:doi.org/10.4204/EPTCS.252.8.

[4] Pascal Bergsträßer, Moses Ganardi, and Georg Zetzsche. A characterization of wreath products where knapsack is decidable. In *Proceeding of the 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, volume 187 of *LIPIcs*, pages 11:1–11:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.STACS.2021.11.

[5] Pascal Bergsträßer, Moses Ganardi, and Georg Zetzsche. A characterization of wreath products where knapsack is decidable, 2021. arXiv:2101.06132.

[6] Agnieszka Bier and Oleg Bogopolski. Exponential equations in acylindrically hyperbolic groups, 2021. arXiv:2106.11385.

[7] Oleg Bogopolski and Aleksander Ivanov. Decidability problem for exponential equations in finitely presented groups. *Canadian Mathematical Bulletin*, 1–18, 2022. doi:10.4153/S0008439522000698.

[8] Fedor A. Dudkin and Alexander V. Treyer. Knapsack problem for Baumslag–Solitar groups. *Siberian Journal of Pure and Applied Mathematics*, 18(4):43–55, 2018. doi:10.33048/pam.2018.18.404.

[9] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word Processing in Groups*. Jones and Bartlett, Boston, 1992. doi:10.1201/9781439865699.

[10] David B. A. Epstein and Derek F. Holt. The linearity of the conjugacy problem in word-hyperbolic groups. *International Journal of Algebra and Computation*, 16(2):287–306, 2006. doi:10.1142/S0218196706002986.

[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. doi:10.4230/LIPIcs.ICALP.2020.126.

[12] Michael Figelius and Markus Lohrey,. Exponent Equations in HNN-extensions. In *Proceedings of the 47th International Symposium on Symbolic and Algebraic Computation, ISSAC 2022*, pages 293–301. ACM, 2022. doi:10.1145/3476446.3535482.

[13] Michael Figelius, Markus Lohrey, and Georg Zetzsche. Closure properties of knapsack semilinear groups. *Journal of Algebra*, 589(1):437–482, 2022. doi:10.1016/j.jalgebra.2021.08.016.

[14] Elizaveta Frenkel, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016. doi:10.1016/j.jsc.2015.05.006.

[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. doi:10.4230/LIPIcs.STACS.2018.32.

[16] Stephen M. Gersten and Hamish B. Short. Rational subgroups of biautomatic groups. *Annals of Mathematics*, 134(1):125–158, 1991. doi:10.2307/2944334.

[17] Mikhael Gromov. Hyperbolic groups. In S. M. Gersten, editor, *Essays in Group Theory*, number 8 in MSRI Publ., pages 75–263. Springer, 1987. doi:10.1007/978-1-4613-9586-7_3.

[18] Christoph Haase. A survival guide to Presburger arithmetic. *ACM SIGLOG News*, 5(3):67–82, 2018. doi:10.1145/3242953.3242964.

[19] Niko Haubold and Markus Lohrey. Compressed word problems in HNN-extensions and amalgamated products. *Theory of Computing Systems*, 49(2):283–305, 2011. doi:10.1007/s00224-010-9295-2.

[20] Graham Higman, Bernhard H. Neumann, and Hanna Neumann. Embedding theorems for groups. *Journal of the London Mathematical Society. Second Series*, 24:247–254, 1949. doi:10.1112/jlms/s1-24.4.247.

[21] Derek Holt. Word-hyperbolic groups have real-time word problem. *International Journal of Algebra and Computation*, 10:221–228, 2000. doi:10.1142/S0218196700000078.

[22] Derek F. Holt and Sarah Rees. Regularity of quasigeodesics in a hyperbolic group. *International Journal of Algebra and Computation*, 13(05):585–596, 2003. doi:10.1142/S0218196703001560.

[23] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison–Wesley, 1979.

[24] Olga Kharlampovich, Alexei Miasnikov, and Pascal Weil. Stallings graphs for quasi-convex subgroups. *Journal of Algebra*, 488:442–483, 2017. doi:10.1016/j.jalgebra.2017.05.037.

[25] 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. doi:10.1090/conm/677.

[26] Markus Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020. doi:10.1016/j.jalgebra.2019.04.008.

[27] Markus Lohrey and Georg Zetzsche. Knapsack in graph groups. *Theory of Computing Systems*, 62(1):192–246, 2018. doi:10.1007/s00224-017-9808-3.

[28] Markus Lohrey and Georg Zetzsche. Knapsack and the power word problem in solvable Baumslag-Solitar groups. In *Proceedings of the 45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020*, volume 170 of *LIPIcs*, pages 67:1–67:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.MFCS.2020.67.

[29] Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Springer, 1977. doi:10.1007/978-3-642-61896-3.

[30] Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017. doi:10.1515/gcc-2017-0006.

[31] Alexei Myasnikov, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015. doi:10.1090/S0025-5718-2014-02880-9.

[32] Alexei G. Myasnikov and Vladimir N. Remeslennikov. Exponential groups 2: Extensions of centralizers and tensor completion of CSA-groups. *International Journal of Algebra and Computation*, 6(6):687–712, 1996. doi:10.1142/S0218196796000398.

[33] Walter D. Neumann and Michael Shapiro. Automatic structures and boundaries for graphs of groups. *International Journal of Algebra and Computation*, 4(4):591–616, 1994. doi:10.1142/S0218196794000178.

[34] Alexander Yu. Ol′shanskiĭ. Almost every group is hyperbolic. *International Journal of Algebra and Computation*, 2(1):1–17, 1992. doi:10.1142/S0218196792000025.

[35] Rohit Parikh. On context-free languages. *Journal of the ACM*, 13(4):570–581, 1966. doi:10.1145/321356.321364.

[36] Eliyahu Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14:45–47, 1982. doi:10.1112/blms/14.1.45.

[37] Paul E. Schupp. Coxeter groups, 2-completion, perimeter reduction and subgroup separability. *Geometriae Dedicata*, 96:179–198, 2003. doi:10.1023/A:1022155823425.

[38] David Simplot and Alain Terlutte. Closure under union and composition of iterated rational transductions. *RAIRO - Theoretical Informatics and Applications - Informatique Théorique et Applications*, 34(3):183–212, 2000. doi:10.1051/ita:2000114.

[39] Daniel T. Wise. Research announcement: the structure of groups with a quasiconvex hierarchy. *Electronic Research Announcements in Mathematical Sciences*, 16:44–55, 2009. doi:10.3934/era.2009.16.44.