# Complexity of word problems for HNN-extensions 

Markus Lohrey ${ }^{1}$<br>Universität Siegen, Germany<br>\{lohrey\}@eti.uni-siegen.de


#### Abstract

The computational complexity of the word problem in HNNextension of groups is studied. HNN-extension is a fundamental construction in combinatorial group theory. It is shown that the word problem for an ascending HNN-extension of a group $H$ is logspace reducible to the so-called compressed word problem for $H$. The main result of the paper states that the word problem for an HNN-extension of a hyperbolic group $H$ with cyclic associated subgroups can be solved in polynomial time. This result can be easily extended to fundamental groups of graphs of groups with hyperbolic vertex groups and cyclic edge groups.


Keywords: word problems • HNN-extensions • hyperbolic groups

## 1 Introduction

The study of computational problems in group theory goes back more than 100 years. In a seminal paper from 1911, Dehn posed three decision problems [8]: The word problem, the conjugacy problem, and the isomorphism problem. In this paper, we mainly deal with the word problem: It is defined for a finitely generated group $G$. This means that there exists a finite subset $\Sigma \subseteq G$ such that every element of $G$ can be written as a finite product of elements from $\Sigma$. This allows to represent elements of $G$ by finite words over the alphabet $\Sigma$. For the word problem, the input consists of such a finite word $w \in \Sigma^{*}$ and the goal is to check whether $w$ represents the identity element of $G$.

In general the word problem is undecidable. By a classical result of Boone [5] and Novikov [30], there exist finitely presented groups (finitely generated groups that can be defined by finitely many equations) with an undecidable word problem; see [35] for an excellent exposition. On the positive side, there are many classes of groups with decidable word problems. In his paper from 1912 [9], Dehn presented an algorithm that solves the word problem for fundamental groups of orientable closed 2-dimensional manifolds. This result was extended to one-relator groups (finitely generated groups that can be defined by a single equation) by Dehn's student Magnus [24]. Other important classes of groups with a decidable word problem are:

- automatic groups [12] (including important classes like braid groups [1], Coxeter groups [4], right-angled Artin groups [7], hyperbolic groups [15]),
- finitely generated linear groups, i.e., finitely generated groups that can be faithfully represented by matrices over some field [31] (including polycyclic groups and nilpotent groups), and
- finitely generated metabelian groups (they can be embedded in direct products of linear groups [37]).

With the rise of computational complexity theory in the 1960's, also the computational complexity of group theoretic problems moved into the focus of research. From the very beginning, this field attracted researchers from mathematics as well as computer science. It turned out that for many interesting classes of groups the word problem admits quite efficient algorithms. Lipton and Zalcstein [20] and Simon [34] proved that deterministic logarithmic space (and hence polynomial time) suffices to solve the word problem for a linear group. For automatic groups, the word problem can be solved in quadratic time [12], and for the subclass of hyperbolic groups the word problem can be solved in linear time [18] and belongs to the complexity class LogCFL [21]. For one-relator groups in general, only a non-elementary algorithm is known for the word problem, but for important subclasses polynomial time algorithms are known, see [25, 29] for recent progress.

The complexity of the word problem is also preserved by several important group theoretic constructions, e.g. graph products (which generalize free products and direct products) [10] and wreath products [36]. Two other important constructions in group theory are $H N N$-extensions and amalgamated free products. A theorem of Seifert and van Kampen links these constructions 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 $H$ with two isomorphic subgroups $A$ and $B$ and an isomorphism $\varphi: A \rightarrow B$, the corresponding HNN-extension is the group

$$
\begin{equation*}
G=\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle \tag{1}
\end{equation*}
$$

Intuitively, it is obtained by adjoing to $H$ a new generator $t$ (the stable letter) in such a way that conjugation of $A$ by $t$ realizes $\varphi$. The subgroups $A$ and $B$ are also called the associated subgroups. If $H$ has a decidable word problem, $A$ and $B$ are finitely generated subgroups of $H$, and the subgroup membership problems for $A$ and $B$ are decidable, then also the word problem for $G$ in (1) is decidable via Britton reduction [6] (iterated application of rewriting steps $t^{-1} a t \rightarrow \varphi(a)$ and $t b t^{-1}=\varphi^{-1}(b)$ for $a \in A$ and $\left.b \in B\right)$. For the special case where $A=B$ and $\varphi$ is the identity, it is shown in [36] that the word problem for the HNN-extension $G$ in (1) is $\mathrm{NC}^{1}$-reducible to the following problems: (i) the word problem for $H$, (ii) the word problem for the free group of rank two, and (iii) the subgroup membership problem for $A$. On the other hand, it is not clear whether this result can be extended to arbitrary HNN-extensions (even if we allow polynomial time Turing reductions instead of $\mathrm{NC}^{1}$-reductions). A concrete open problem is the complexity of the word problem for an HNN-extension $\langle F, t| t^{-1} a t=\varphi(a)(a \in$ $A)\rangle$ of a free group $F$ with finitely generated associated subgroups $A$ and $B$. The word problem for a free group is known to be in logspace (it is a linear group) [20] and the subgroup membership problem for finitely generated subgroups of a free
group can be solved in polynomial time [2]. The problem with Britton reduction in the group $\left\langle F, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$ is that every Britton reduction step may increase the length of the word by a constant multiplicative factor. This may lead to words of exponential length. One might try to solve this problem by representing the exponentially long words by so-called straight-line programs (context-free grammars that produce a single word). This idea works for the word problems of automorphism groups and certain group extensions [22, Section 4.2]. But it is not clear whether the words that arise from Britton reduction can be compressed down to polynomial size using straight-line programs. The problem arises from the fact that both $A$ and $B$ might be proper subgroups of $H$. On the other hand, if one of the associated subgroups $A$ and $B$ coincides with the base group $H$ ( $G$ is then called an ascending $H N N$-extension) then one can show that the word problem for $G$ is logspace-reducible to the so-called compressed word problem for $H$ (Theorem 4). The latter problem asks whether a given straight-line program that produces a word over the generators of $H$ evaluates to the group identity of $H$. The compressed word problem is known to be solvable in polynomial time for nilpotent groups, virtually special groups, and hyperbolic groups. For every linear group one still has a randomized polynomial time algorithm for the compressed word problem; see [22] for details.

Our main result deals with HNN-extensions, where the associated subgroups $A$ and $B$ are allowed to be proper subgroups of the base group $H$ but are cyclic (i.e., generated by a single element) and undistored in $H$ (the latter is defined in Section 4). We show that in this situation the word problem for $G$ is polynomial time Turing-reducible to the compressed power problem for $H$ (Theorem 7). In the compressed power problem for $H$, the input consists of two elements $p, q \in H$, where $p$ is given explicitly as a word over a generating set and $q$ is given in compressed form by a straight-line program over a generating set. The question is whether there exists an integer $z \in \mathbb{Z}$ such that $p^{z}=q$ in $H$. Moreover, in the positive case we also want to compute such a $z$.

Our main application of Theorem 7 concerns hyperbolic groups. We show that the compressed power problem for a hyperbolic group can be solved in polynomial time (Theorem 6). For this, we make use of the well-known fact that cyclic subgroups of hyperbolic groups are undistorted. As a consequence of Theorems 6 and 7, the word problem for an HNN-extension of a hyperbolic group with cyclic associated subgroups can be solved in polynomial time (Corollary 1). One should remark that HNN-extensions of hyperbolic groups with cyclic associated subgroups are in general not even automatic; a well-known example is the Baumslag-Solitar group $\operatorname{BS}(1,2)=\left\langle a, t \mid t^{-1} a t=a^{2}\right\rangle[12$, Section 7.4].

Corollary 1 can be generalized to fundamental groups of graphs of groups (which generalize HNN-extensions and amalgamated free products) with hyperbolic vertex groups and cyclic edge groups, see the full version [23]. For the special case where all vertex groups are free, the existence of a polynomial time algorithm for the word problem has been stated in [38, Remark 5.11] without proof. For a fundamental group of a graph of groups, where all vertex groups are copies of $\mathbb{Z}$, the word problem can be even solved in logspace [39].

## 2 Groups

For real numbers $a \leq b$ we denote with $[a, b]=\{r \in \mathbb{R} \mid a \leq r \leq b\}$ the closed interval from $a$ to $b$. For $k, \ell \in \mathbb{N}$ we write $[k: \ell]$ for $\{i \in \mathbb{N} \mid k \leq i \leq \ell\}$. We use standard notations for words (over some alphabet $\Sigma$ ). As usual, the empty word is denoted with $\varepsilon$. Given a word $w=a_{1} a_{2} \cdots a_{n}$ (where $a_{1}, a_{2}, \ldots, a_{n} \in \Sigma$ ) and numbers $i, j \in \mathbb{N}$ with $1 \leq i \leq j$ we define $w[i: j]=a_{i} a_{i+1} \cdots a_{\min \{j, n\}}$.

For a group $G$ and a subset $\Sigma \subseteq G$, we denote with $\langle\Sigma\rangle$ the subgroup of $G$ generated by $\Sigma$. It is the smallest subgroup of $G$ containing $\Sigma$. If $G=\langle\Sigma\rangle$ then $\Sigma$ is a generating set for $G$. The group $G$ is finitely generated (f.g.) if it has a finite generating set. We mostly consider f.g. groups in this paper.

Assume that $G=\langle\Sigma\rangle$ and let $\Sigma^{-1}=\left\{a^{-1} \mid a \in \Sigma\right\}$. For a word $w=$ $a_{1} \cdots a_{n}$ with $a_{i} \in \Sigma \cup \Sigma^{-1}$ we define the word $w^{-1}=a_{n}^{-1} \cdots a_{1}^{-1}$. This defines an involution on the free monoid $\left(\Sigma \cup \Sigma^{-1}\right)^{*}$. We obtain a surjective monoid homomorphism $\pi:\left(\Sigma \cup \Sigma^{-1}\right)^{*} \rightarrow G$ that preserves the involution: $\pi\left(w^{-1}\right)=$ $\pi(w)^{-1}$. We also say that the word $w$ represents the group element $\pi(w)$. For words $u, v \in\left(\Sigma \cup \Sigma^{-1}\right)^{*}$ we say that $u=v$ in $G$ if $\pi(u)=\pi(v)$. For $g \in G$ one defines $|g|_{\Sigma}=\min \left\{|w|: w \in \pi^{-1}(g)\right\}$ as the length of a shortest word over $\Sigma \cup \Sigma^{-1}$ representing $g$. If $\Sigma$ is clear, we also write $|g|$ for $|g|_{\Sigma}$. If $\Sigma=\Sigma^{-1}$ then $\Sigma$ is a finite symmetric generating set for $G$.

We will describe groups by presentations. In general, if $H$ is a group and $R \subseteq H$ is a set of so-called relators, then we denote with $\langle H \mid R\rangle$ the quotient group $H / N_{R}$, where $N_{R}$ is the smallest normal subgroup of $H$ with $R \subseteq N_{R}$. Formally, we have $N_{R}=\left\langle\left\{h r h^{-1} \mid h \in H, r \in R\right\}\right\rangle$. For group elements $g_{i}, h_{i} \in H$ ( $i \in I$ ) we also write $\left\langle H \mid g_{i}=h_{i}(i \in I)\right\rangle$ for the group $\left\langle H \mid\left\{g_{i} h_{i}^{-1} \mid i \in I\right\}\right\rangle$.

In most cases, one takes a free group for the group $H$ from the previous paragraph. Fix a set $\Sigma$ and let $\Sigma^{-1}=\left\{a^{-1} \mid a \in \Sigma\right\}$ be a set of formal inverses of the elements in $\Sigma$ with $\Sigma \cap \Sigma^{-1}=\emptyset$. A word $w \in\left(\Sigma \cup \Sigma^{-1}\right)^{*}$ is called freely reduced if it neither contains a factor $a a^{-1}$ nor $a^{-1} a$ for $a \in \Sigma$. For every word $w \in\left(\Sigma \cup \Sigma^{-1}\right)^{*}$ there is a unique freely reduced word that is obtained from $w$ by deleting factors $a a^{-1}$ and $a^{-1} a(a \in \Sigma)$ as long as possible. The free group generated by $\Sigma$ consists of all freely reduced words together with the multiplication defined by $u \cdot v=\operatorname{nf}(u v)$ for $u, v$ freely reduced. For a set $R \subseteq F(\Sigma)$ of relators we also write $\langle\Sigma \mid R\rangle$ for the group $\langle F(\Sigma) \mid R\rangle$. Every group $G$ that is generated by $\Sigma$ can be written as $\langle\Sigma \mid R\rangle$ for some $R \subseteq F(\Sigma)$. A group $\langle\Sigma \mid R\rangle$ with $\Sigma$ and $R$ finite is called finitely presented, and the pair $(\Sigma, R)$ is a presentation for the group $\langle\Sigma \mid R\rangle$. Given two groups $G_{1}=\left\langle\Sigma_{1} \mid R_{1}\right\rangle$ and $G_{2}=\left\langle\Sigma_{2} \mid R_{2}\right\rangle$, where w.l.o.g. $\Sigma_{1} \cap \Sigma_{2}=\emptyset$, we define their free product $G_{1} * G_{2}=\left\langle\Sigma_{1} \cup \Sigma_{2} \mid R_{1} \cup R_{2}\right\rangle$.

Consider a group $G$ with the finite symmetric generating set $\Sigma$. The word problem for $G$ w.r.t. $\Sigma$ is the following decision problem:
input: a word $w \in \Sigma^{*}$.
question: does $w=1$ hold in $G$ ?
It is well known that if $\Sigma^{\prime}$ is another finite symmetric generating set for $G$, then the word problem for $G$ w.r.t. $\Sigma^{\prime}$ is logspace many-one reducible to the word
problem for $G$ w.r.t. $\Sigma$. This justifies one to speak just of the word problem for the group $G$.

HNN-extensions. HNN-extension is an extremely important operation for constructing groups that arises in all parts of combinatorial group theory. Take a group $H$ and a generator $t \notin H$, from which we obtain the free product $H *\langle t\rangle \cong H * \mathbb{Z}$. Assume that $A, B \leq H$ are two isomorphic subgroups of $H$ and let $\varphi: A \rightarrow B$ be an isomorphism. Then, the group $\left\langle H *\langle t\rangle \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$ is called the $H N N$-extension of $A$ with associated subgroups $A$ and $B$ (usually, the isomorphism $\varphi$ is not mentioned explicitly). The above HNN-extension is usually written as $\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$. Britton [6] proved the following fundamental result for HNN-extensions. Let us fix a finite symmetric generating set $\Sigma$ for $H$.

Theorem 1 (Britton's lemma [6]). Let $G=\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$ be an HNN-extension. If a word $w \in\left(\Sigma \cup\left\{t, t^{-1}\right\}\right)^{*}$ represents the identity of $G$ then $w$ contains a factor of the form $t^{-1} u t$ (resp., tut ${ }^{-1}$ ), where $u \in \Sigma^{*}$ represents an element of $A$ (resp., $B$ ).

A subword of the form $t^{-1} u t$ (resp., $t u t^{-1}$ ), where $u \in \Sigma^{*}$ represents an element of $A$ (resp., $B$ ) is also called a pin.

A simple corollary of Britton's lemma is that $H$ is a subgroup of the HNNextension $\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$. Britton's lemma can be also used to solve the word problem for an HNN-extension $\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$. For this we need several assumptions:

- The word problem for $H$ is decidable.
- There is an algorithm that decides whether a given word $u \in \Sigma^{*}$ represents an element of $A$ (resp., $B$ ).
- Given a word $u \in \Sigma^{*}$ that represents an element $a \in A$ (resp., $b \in B$ ), one can compute a word $v \in \Sigma^{*}$ that represents the element $\varphi(a)$ (resp., $\varphi^{-1}(b)$ ). Let us denote this word $v$ with $\varphi(u)$ (resp., $\varphi^{-1}(u)$ ).

Then, given a word $w \in\left(\Sigma \cup\left\{t, t^{-1}\right\}\right)^{*}$ one replaces pins $t^{-1} u t$ (resp., tut $t^{-1}$ ) by $\varphi(u)$ (resp., $\varphi^{-1}(u)$ ) in any order, until no more pins occur. If the final word does not belong to $\Sigma^{*}$ then we have $w \neq 1$ in the HNN-extension. If the final word belongs to $\Sigma^{*}$ then one uses the algorithm for the word problem of $H$ to check whether it represents the group identity. This algorithm is known as Britton reduction.

An HNN-extension $G=\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in A)\right\rangle$ with $\varphi: A \rightarrow B$ is called ascending if $A=H$ (it is also called the mapping torus of $\varphi$ ). Note that we do not require $B=H$. Ascending HNN-extensions play an important role in many group theoretical results. For instance, Bieri and Strebel [3] proved that if $N$ is a normal subgroup of a finitely presented group $G$ such that $G / N \cong \mathbb{Z}$ then $G$ is an ascending HNN-extension of a finitely generated group or contains a free subgroup of rank two.


Fig. 1. The shape of a geodesic triangle in a hyperbolic group

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

Paths can be defined in a very general way for metric spaces, but we only need paths that are induced by words over $\Sigma$. Given a word $w \in \Sigma^{*}$ of length $n$, one obtains a unique path $P[w]:[0, n] \rightarrow \Gamma$, which is a continuous mapping from the real interval $[0, n]$ to $\Gamma$. It maps the subinterval $[i, i+1] \subseteq[0, n]$ isometrically onto the edge $\left(g_{i}, g_{i+1}\right)$ of $\Gamma$, where $g_{i}$ (resp., $g_{i+1}$ ) is the group element represented by the word $w[1: i]$ (resp., $w[1: i+1]$ ). The path $P[w]$ starts in $1=g_{0}$ and ends in $g_{n}$ (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 $g \cdot P[w]$, where $g$ is the group element represented by $u$.

Let $\lambda, \zeta>0, \epsilon \geq 0$ be real constants. A path $P$ colon $[0, n] \rightarrow \Gamma$ of the above form is geodesic if $d_{\Gamma}(P(0), P(n))=n$; it is a $(\lambda, \epsilon)$-quasigeodesic if for all points $p=P(a)$ and $q=P(b)$ we have $|a-b| \leq$ $\lambda \cdot d_{\Gamma}(p, q)+\epsilon$; and it is $\zeta$-local $(\lambda, \epsilon)$-quasigeodesic if for all points $p=P(a)$ and $q=P(b)$ with $|a-b| \leq \zeta$ we have $|a-b| \leq \lambda \cdot d_{\Gamma}(p, q)+\epsilon$.

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 ( $\zeta$-local) $(\lambda, \epsilon)$-quasigeodesic words. A word $w \in \Sigma^{*}$ is shortlex reduced if it is the length-lexicographically smallest word that represents the same group element as $w$. For this, we have to fix an arbitrary linear order on $\Sigma$. Note that if $u=x y$ is shortlex reduced then $x$ and $y$ are shortlex reduced too. For a word $u \in \Sigma^{*}$ we denote with $\operatorname{shlex}(u)$ the unique shortlex reduced


Fig. 2. Paths that asynchronously $K$-fellow travel
word that represents the same group element as $u$ (the underlying group $G$ will be always clear from the context).

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 $\delta$-slim for $\delta \geq 0$, if for all $i \in\{1,2,3\}$, every point on $P_{i}$ has distance at most $\delta$ from a point on $P_{j} \cup P_{k}$, where $\{j, k\}=\{1,2,3\} \backslash\{i\}$. The group $G$ is called $\delta$-hyperbolic, if every geodesic triangle is $\delta$-slim. Finally, $G$ is hyperbolic, if it is $\delta$-hyperbolic for some $\delta \geq 0$. Figure 1 shows the shape of a geodesic triangle in a hyperbolic group. Finitely generated free groups are for instance 0 -hyperbolic. The property of being hyperbolic is independent of the chosen generating set $\Sigma$. The word problem for every hyperbolic group can be decided in real time [18].

Fix a $\delta$-hyperbolic group $G$ with the finite symmetric generating set $\Sigma$ for the rest of the section, and let $\Gamma$ be the corresponding geodesic metric space. Consider two paths $P_{1}:\left[0, n_{1}\right] \rightarrow \Gamma, P_{2}:\left[0, n_{2}\right] \rightarrow \Gamma$ and let $K \in \mathbb{R}, K \geq 0$. The paths $P_{1}$ and $P_{2}$ asynchronously $K$-fellow travel if there exist two continuous non-decreasing mappings $\varphi_{1}:[0,1] \rightarrow\left[0, n_{1}\right]$ and $\varphi_{2}:[0,1] \rightarrow\left[0, n_{2}\right]$ such that $\varphi_{1}(0)=\varphi_{2}(0)=0, \varphi_{1}(1)=n_{1}, \varphi_{2}(1)=n_{2}$ and for all $0 \leq t \leq 1$, $d_{\Gamma}\left(P_{1}\left(\varphi_{1}(t)\right), P_{2}\left(\varphi_{2}(t)\right)\right) \leq K$. Intuitively, this means that one can travel along the paths $P_{1}$ and $P_{2}$ asynchronously with variable speeds such that at any time instant the current points have distance at most $K$. If $P_{1}$ and $P_{2}$ asynchronously $K$-fellow travel, then by slightly increasing $K$ one obtains a subset $E \subseteq\left[0: n_{1}\right] \times\left[0: n_{2}\right]$ with (i) $(0,0),\left(n_{1}, n_{2}\right) \in E, d_{\Gamma}\left(P_{1}(i), P_{2}(j)\right) \leq K$ for all $(i, j) \in E$ and (iii) if $(i, j) \in E \backslash\left\{\left(n_{1}, n_{2}\right)\right\}$ then $(i+1, j) \in E$ or $(i, j+1) \in E$. We write $P_{1} \approx_{K} P_{2}$ in this case. Intuitively, this means that a ladder graph as shown in Figure 2 exists, where the edges connecting the horizontal $P_{1}$ - and $P_{2}$-labelled paths represent paths of length $\leq K$ that connect elements from $G$.

Lemma 1 (c.f. [27, Lemma 1]). Let $P_{1}$ and $P_{2}$ be $(\lambda, \epsilon)$-quasigeodesic paths in $\Gamma$ and assume that $P_{i}$ starts in $g_{i}$, ends in $h_{i}$, and $d_{\Gamma}\left(g_{1}, g_{2}\right), d_{\Gamma}\left(h_{1}, h_{2}\right) \leq h$. Then there is a constant $K=K(\delta, \lambda, \epsilon, h) \geq h$ such that $P_{1} \approx_{K} P_{2}$.

### 2.1 Compressed words and the compressed word problem

Straight-line programs offer succinct representations of long words that contain many repeated substrings. We here review the basics, referring to [22] for a more in-depth introduction.

Fix a finite alphabet $\Sigma$. A straight-line program $\mathcal{G}$ (SLP for short) is a contextfree grammar that generates exactly one word $\operatorname{val}(\mathcal{G}) \in \Sigma^{*}$. More formally, an SLP over $\Sigma$ is a triple $\mathcal{G}=(V, S, \rho)$ where

- $V$ is a finite set of variables, disjoint from $\Sigma$,
$-S \in V$ is the start variable, and
$-\rho: V \rightarrow(V \cup \Sigma)^{*}$ is the right-hand side mapping, which is acyclic in the sense that the binary relation $\{(A, B) \in V \times V \mid B$ appears in $\rho(A)\}$ is acyclic.

We define the size $|\mathcal{G}|$ of $\mathcal{G}$ as $\sum_{A \in V}|\rho(A)|$. The evaluation function val $=$ $\operatorname{val}_{\mathcal{G}}:(V \cup \Sigma)^{*} \rightarrow \Sigma^{*}$ is the unique homomorphism between free monoids such that (i) $\operatorname{val}(a)=a$ for $a \in \Sigma$, and (ii) $\operatorname{val}(A)=\operatorname{val}(\rho(A))$ for $A \in V$. We finally take $\operatorname{val}(\mathcal{G})=\operatorname{val}(S)$. We call $\operatorname{val}(\mathcal{G})$ the word defined by the SLP $\mathcal{G}$.

Example 1. Let $\Sigma=\{a, b\}$ and fix $n \geq 0$. We define $\mathcal{G}_{n}=\left(\left\{A_{0}, \ldots, A_{n}\right\}, A_{n}, \rho\right)$, where $\rho\left(A_{0}\right)=a b$ and $\rho\left(A_{i+1}\right)=A_{i} A_{i}$ for $0 \leq i \leq n-1$. It is an SLP of size $2(n+1)$. We have $\operatorname{val}\left(A_{0}\right)=a b$ and more generally $\operatorname{val}\left(A_{i}\right)=(a b)^{2^{2}}$. Thus $\operatorname{val}\left(\mathcal{G}_{n}\right)=\operatorname{val}\left(A_{n}\right)=(a b)^{2^{n}}$.

The SLP $\mathcal{G}=(V, S, \rho)$ is trivial if $S$ is the only variable and $\rho(S)=\varepsilon=\operatorname{val}(\mathcal{G})$. An SLP is in Chomsky normal form if it is either trivial or all right-hand sides $\rho(A)$ are of the form $a \in \Sigma$ or $B C$ with $B, C \in V$. There is a linear-time algorithm that transforms a given SLP $\mathcal{G}$ into an SLP $\mathcal{G}^{\prime}$ in Chomsky normal such that $\operatorname{val}(\mathcal{G})=\operatorname{val}\left(\mathcal{G}^{\prime}\right)$; see [22, Proposition 3.8].

The following theorem is the technical main result from [19]:
Theorem 2 (c.f. [19]). Let $G$ be a hyperbolic group with the finite symmetric generating set $\Sigma$. Given an $S L P \mathcal{G}$ over $\Sigma$ one can compute in polynomial time an $S L P \mathcal{H}$ over $\Sigma$ such that $\operatorname{val}(\mathcal{H})=\operatorname{shlex}(\operatorname{val}(\mathcal{G}))$.

If $G$ is a f.g. group with the finite and symmetric generating set $\Sigma$, then we define the compressed word problem of $G$ as the following problem:
input: an SLP $\mathcal{G}$ over $\Sigma$.
question: does $\operatorname{val}(\mathcal{G})$ represent the group identity of $G$ ?
An immediate consequence of Theorem 2 is the following result:
Theorem 3 (c.f. [19]). The compressed word problem for a hyperbolic group can be solved in polynomial time.

The compressed word problem turns out to be useful for the solution of the word problem for an ascending HNN-extension:

Theorem 4. Let $H$ be a finitely generated group. The word problem for an ascending $H N N$-extension $G=\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in H)\right\rangle$ is logspace-reducible to the compressed word problem for $H$.

The proof is similar to corresponding results for automorphism groups and semidirect products [22, Section 4.2]; see the full version [23] for details.

We will also need a generalization of straight-line programs, known as composition systems [16, Definition 8.1.2] (in [22] they are called cut straight-line programs). A composition system over $\Sigma$ is a tuple $\mathcal{G}=(V, S, \rho)$, with $V$ and $S$ as for an SLP, and where we also allow, as right-hand sides for $\rho$, expressions of the form $B[i: j]$, with $B \in V$ and $i, j \in \mathbb{N}, 1 \leq i \leq j$. The numbers $i$ and $j$ are stored in binary encoding. We again require $\rho$ to be acyclic. When $\rho(A)=B[i: j]$ we define $\operatorname{val}(A)=\operatorname{val}(B)[i: j]$. We define the size $|\mathcal{G}|$ of the composition system $\mathcal{G}$ as the total number of occurrences of symbols from $V \cup \Sigma$ in all right-hand sides. Hence, a right-hand $B[i: j]$ contributes 1 to the size, and we ignore the numbers $i, j$. Adding the bit lengths of the numbers $i$ and $j$ to the size $|\mathcal{G}|$ would only lead to a polynomial blow-up for $|\mathcal{G}|$. To see this, first normalize the composition system so that all right-hand sides have the form $a$, $B C$ or $B[i: j]$ with $a \in \Sigma$ and $B, C \in V$; analogously to the Chomsky normal form of SLPs this can be achieved in polynomial time. If $n$ is the number of variables of the resulting composition system, then every variable produces a string of length at most $2^{n}$. Hence, we can assume that all numbers $i, j$ that appear in a right-hand side $B[i: j]$ are of bit length $\mathcal{O}(n)$.

We can now state an important result of Hagenah; see [16, Algorithmus 8.1.4] as well as [22, Theorem 3.14].

Theorem 5. There is a polynomial-time algorithm that, given a composition system $\mathcal{G}$, computes an SLP $\mathcal{G}^{\prime}$ such that $\operatorname{val}(\mathcal{G})=\operatorname{val}\left(\mathcal{G}^{\prime}\right)$.
It will be convenient to allow in composition systems also more complex righthand sides. For instance $(A B C)[i: j] D$ would first concatenate the strings produced from $A, B$, and $C$. From the resulting string the substring from position $i$ to position $j$ is cut out and this substring is concatenated with the string produced by $D$.

## 3 The compressed power problem

In the next section we want to study the word problem in HNN-extensions with cyclic associated subgroups. For this, the following computational problem turns out to be important. Let $G$ be a f.g. group with the finite symmetric generating set $\Sigma$. We define the compressed power problem for $G$ as the following problem:
input: a word $w \in \Sigma^{*}$ and an SLP $\mathcal{G}$ over $\Sigma$.
output: the binary coding of an integer $z \in \mathbb{Z}$ such that $w^{z}=\operatorname{val}(\mathcal{G})$ in $G$ if such an integer exists, and no otherwise.

Theorem 6. For every hyperbolic group $G$, the compressed power problem can be solved in polynomial time.

Proof. Fix the word $w \in \Sigma^{*}$ and the $\operatorname{SLP} \mathcal{G}=(V, \rho, S)$ over $\Sigma$, w.l.o.g. in Chomsky normal form. We have to check whether the equation

$$
\begin{equation*}
w^{z}=\operatorname{val}(\mathcal{G}) \tag{2}
\end{equation*}
$$

has a solution in $G$, and compute in the positive case a solution $z \in \mathbb{Z}$. Let $g$ be the group element represented by $w$.

In a hyperbolic group $G$ the order of torsion elements is bounded by a fixed constant that only depends on $G$, see also the proof of [28, Theorem 6.7]. This allows to check in polynomial time whether $g$ has finite order in $G$. If $g$ has finite order, say $d$, then it remains to check for all $0 \leq i \leq d-1$ whether $w^{i}=\operatorname{val}(\mathcal{G})$ in $G$, which can be done in polynomial time by Theorem 3 . This solves the case where $g$ has finite order in $G$.

Now assume that $g$ has infinite order in $G$. Then (2) has at most one solution. By considering also the equation $\left(w^{-1}\right)^{z}=\operatorname{val}(\mathcal{G})$, it suffices to search for a solution $z \in \mathbb{N}$. We can also assume that $w$ is shortlex-reduced. Using techniques from [13] one can further ensure that for every $n \in \mathbb{N}, w^{n}$ is $(\lambda, \epsilon)$-quasigeodesic for fixed constants $\lambda$ and $\epsilon$ that only depend on the group $G$; see [23] for details. Finally, by Theorem 2 we can also assume that the word $\operatorname{val}(\mathcal{G})$ (and hence every word $\operatorname{val}(X)$ for $X$ a variable of $\mathcal{G})$ is shortlex-reduced. Hence, if $w^{z}=\operatorname{val}(\mathcal{G})$ for some $z \in \mathbb{N}$, then by Lemma 1 we have $P\left[w^{z}\right] \approx_{K} P[\operatorname{val}(\mathcal{G})]$ for a fixed constant $K$ that only depends on $G$. We proceed in two steps.

Step 1. We compute in polynomial time for all variables $X \in V$ of the SLP $\mathcal{G}$, all group elements $a, b \in \mathcal{B}_{K}(1)$ (there are only constantly many), and all factors $w^{\prime}$ of $w$ a bit $\beta\left[X, a, b, w^{\prime}\right] \in\{0,1\}$ which is set to 1 if and only if (i) $\operatorname{val}(X)=a w^{\prime} b$ in $G$ and (ii) $P[\operatorname{val}(X)] \approx_{K} a \cdot P\left[w^{\prime}\right]$.

We compute these bits $\beta\left[X, a, b, w^{\prime}\right]$ in a bottom-up process where we begin with variables $X$ such that $\rho(X)$ is a terminal symbol and end with the start variable $S$. So, let us start with a variable $X$ such that $\rho(X)=c \in \Sigma$ and let $a, b, w^{\prime}$ as above. Then we have to check whether $c=a w^{\prime} b$ in $G$ and $P[c] \approx_{K}$ $a \cdot P\left[w^{\prime}\right]$. The former can be checked in linear time (it is an instance of the word problem) and the latter can be done in polynomial time as well: we have to check whether the path $a \cdot P\left[w^{\prime}\right]$ splits into two parts, where all vertices in the first (resp., second) part belong to $\mathcal{B}_{K}(1)$ (resp., $\mathcal{B}_{K}(c)$ ).

Let us now consider a variable $X$ with $\rho(X)=Y Z$ such that all bits $\beta\left[Y, a, b, w^{\prime}\right]$ and $\beta\left[Z, a, b, w^{\prime}\right]$ have been computed. Let us fix $a, b \in \mathcal{B}_{K}(1)$ and a factor $w^{\prime}$ of $w$. We have $\beta\left[X, a, b, w^{\prime}\right]=1$ if and only if there exists a factorization $w^{\prime}=w_{1}^{\prime} w_{2}^{\prime}$ and $c \in \mathcal{B}_{K}(1)$ such that $\beta\left[Y, a, c, w_{1}^{\prime}\right]=1$ and $\beta\left[Z, c^{-1}, b, w_{2}^{\prime}\right]=1$. This allows us to compute $\beta\left[X, a, b, w^{\prime}\right]$ in polynomial time.
Step 2. We compute in polynomial time for all variables $X \in V$, all group elements $a, b \in \mathcal{B}_{K}(1)$, all proper suffixes $w_{2}$ of $w$, and all proper prefixes $w_{1}$ of $w$ the unique number $z=z\left[X, a, b, w_{2}, w_{1}\right] \in \mathbb{N}$ (if it exists) such that (i) $\operatorname{val}(X)=a w_{2} w^{z} w_{1} b$ in $G$ and (ii) $P[\operatorname{val}(X)] \approx_{K} a \cdot P\left[w_{2} w^{z} w_{1}\right]$. If such an integer $z$ does not exist we set $z\left[X, a, b, w_{2}, w_{1}\right]=\infty$. Note that the integers $z\left[X, a, b, w_{2}, w_{1}\right]$ are unique since $w$ represents a group element of infinite order. We represent $z\left[X, a, b, w_{2}, w_{1}\right]$ in binary encoding. As in step 1 , the computation of the numbers $z\left[X, a, b, w_{2}, w_{1}\right]$ begins with variables $X$ such that $\rho(X)$ is a terminal symbol and ends with the start variable $S$; see [23] for details. The bits $\beta\left[X, a, b, w^{\prime}\right]$ from step 1 are needed in the computation. Finally, $z[S, 1,1, \varepsilon, \varepsilon]$ is the unique solution of equation (2) if $z[S, 1,1, \varepsilon, \varepsilon]<\infty$.

## 4 HNN-extensions with cyclic associated subgroups

Let $H$ be a f.g. group and fix a generating set $\Sigma$ for $H$. We say that a cyclic subgroup $\langle g\rangle \leq H$ is undistorted in $H$ if there exists a constant $\delta$ such that for every $h \in\langle g\rangle$ there exists $z \in \mathbb{Z}$ with $h=g^{z}$ and $|z| \leq \delta \cdot|h|_{\Sigma}$ (this definition does not depend on the choice of $\Sigma) .{ }^{1}$ This is clearly the case if $\langle g\rangle$ is finite.

Note that if $g, h \in H$ are elements of the same order then the group $\langle H, t|$ $\left.t^{-1} g t=h\right\rangle$ is the HNN-extension $\left\langle H, t \mid t^{-1} a t=\varphi(a)(a \in\langle g\rangle)\right\rangle$, where $\varphi:\langle g\rangle \rightarrow$ $\langle h\rangle$ is the isomorphism with $\varphi\left(g^{z}\right)=h^{z}$ for all $z \in \mathbb{Z}$. In the following theorem we consider a slight extension of the word problem for such an HNN-extension $G=$ $\left\langle H, t \mid t^{-1} g t=h\right\rangle$ which we call the semi-compressed word problem for $G$. In this problem the input is a sequence $\mathcal{G}_{0} t^{\epsilon_{1}} \mathcal{G}_{1} t^{\epsilon_{2}} \mathcal{G}_{2} \cdots t^{\epsilon_{n}} \mathcal{G}_{n}$ where every $\mathcal{G}_{i}(0 \leq i \leq n)$ is an SLP (or a composition system) over the alphabet $\Sigma$ and $\epsilon_{i} \in\{-1,1\}$ for $1 \leq i \leq n$. The question is whether $\operatorname{val}\left(\mathcal{G}_{0}\right) t^{\epsilon_{1}} \operatorname{val}\left(\mathcal{G}_{1}\right) t^{\epsilon_{2}} \operatorname{val}\left(\mathcal{G}_{2}\right) \cdots t^{\epsilon_{n}} \operatorname{val}\left(\mathcal{G}_{n}\right)=1$ in $G$.

Theorem 7. Let $H$ be a fixed f.g. group and let $g, h \in H$ be elements with the same order in $H$ (so that the cyclic subgroups $\langle g\rangle$ and $\langle h\rangle$ are isomorphic) such that $\langle g\rangle$ and $\langle h\rangle$ are undistorted. Then the semi-compressed word problem for the HNN-extension $\left\langle H, t \mid t^{-1} g t=h\right\rangle$ is polynomial-time Turing-reducible to the compressed power problem for $H$.

Proof. The case where $\langle g\rangle$ and $\langle h\rangle$ are both finite is easy. In this case, by the main result of [17], even the compressed word problem for $\left\langle H, t \mid t^{-1} g t=h\right\rangle$ is polynomial time Turing-reducible to the compressed word problem for $H$, which is a special case of the compressed power problem.

Let us now assume that $\langle g\rangle$ and $\langle h\rangle$ are infinite. Fix a symmetric finite generating set $\Sigma$ for $H$. Let $W=\mathcal{G}_{0} t^{\epsilon_{1}} \mathcal{G}_{1} t^{\epsilon_{2}} \mathcal{G}_{2} \cdots t^{\epsilon_{n}} \mathcal{G}_{n}$ be an input for the semi-compressed word problem for $\left\langle H, t \mid t^{-1} g t=h\right\rangle$, where $\mathcal{G}_{i}$ is a composition system over $\Sigma$ for $0 \leq i \leq n$ and $\epsilon_{i} \in\{-1,1\}$ for $1 \leq i \leq n$. Basically, we do Britton reduction in any order on the word $\operatorname{val}\left(\mathcal{G}_{0}\right) t^{\epsilon_{1}} \operatorname{val}\left(\mathcal{G}_{1}\right) t^{\epsilon_{2}} \operatorname{val}\left(\mathcal{G}_{2}\right) \cdots t^{\epsilon_{n}} \operatorname{val}\left(\mathcal{G}_{n}\right)$. The number of Britton reduction steps is bounded by $n / 2$. After the $i$-th step we have a sequence $U=\mathcal{H}_{0} t^{\zeta_{1}} \mathcal{H}_{1} t^{\zeta_{2}} \mathcal{H}_{2} \cdots t^{\zeta_{m}} \mathcal{H}_{m}$ where $m \leq n, \mathcal{H}_{i}=\left(V_{i}, S_{i}, \rho_{i}\right)$ is a composition system over $\Sigma$, and $\zeta_{i} \in\{-1,1\}$. Let $u_{i}=\operatorname{val}\left(\mathcal{H}_{i}\right), s_{i}=\left|\mathcal{H}_{i}\right|$ and define $s(U)=m+\sum_{i=0}^{m} s_{i}$, which is a measure for the encoding length of $U$. We then search for an $1 \leq i \leq m-1$ such that one of the following two cases holds:
(i) $\zeta_{i}=-1, \zeta_{i+1}=1$ and there is an $\ell \in \mathbb{Z}$ such that $u_{i}=g^{\ell}$ in $H$.
(ii) $\zeta_{i}=1, \zeta_{i+1}=-1$ and there is an $\ell \in \mathbb{Z}$ such that $u_{i}=h^{\ell}$ in $H$.

Using oracle access to the compressed power problem for $H$ we can check in polynomial time whether one of these cases holds and compute the corresponding integer $\ell$. We then replace the subsequence $\mathcal{H}_{i-1} t^{\zeta_{i}} \mathcal{H}_{i} t^{\zeta_{i+1}} \mathcal{H}_{i+1}$ by a composition system $\mathcal{H}_{i}^{\prime}$ where $\operatorname{val}\left(\mathcal{H}_{i}^{\prime}\right)$ is $u_{i-1} h^{\ell} u_{i+1}$ in case (i) and $u_{i-1} g^{\ell} u_{i+1}$ in case (ii). Let $U^{\prime}$ be the resulting sequence. It remains to bound $s\left(U^{\prime}\right)$. For this we have to

[^0]bound the size of the composition system $\mathcal{H}_{i}^{\prime}$. Assume that $\zeta_{i}=-1, \zeta_{i+1}=1$, and $u_{i}=g^{\ell}$ in $H$ (the case where $\zeta_{i}=1, \zeta_{i+1}=-1$ and $u_{i}=h^{\ell}$ in $H$ is analogous). It suffices to show that $h^{\ell}$ can be produced by a composition system $\mathcal{H}_{i}^{\prime \prime}$ of size $s_{i}+O(1)$. Then we can easily bound the size of $\mathcal{H}_{i}^{\prime}$ by $s_{i-1}+s_{i}+s_{i+1}+O(1)$, which yields $s\left(U^{\prime}\right) \leq s(U)+O(1)$. This shows that every sequence $V$ that occurs during the Britton reduction satisfies $S(V) \leq S(W)+O(n)$ (recall that $W$ is the initial sequence and that the number of Britton reductions is bounded by $n / 2$ ).

Fix the constant $\delta$ such that for every $g^{\prime} \in\langle g\rangle$ the unique (since $g$ has infinite order) $z \in \mathbb{Z}$ with $g^{\prime}=g^{z}$ satisfies $|z| \leq \delta \cdot\left|g^{\prime}\right|_{\Sigma}$. Hence, we have $|\ell| \leq \delta \cdot\left|u_{i}\right|$. W.l.o.g. we can assume that $\delta \in \mathbb{N}$. The variables of $\mathcal{H}_{i}^{\prime \prime}$ are the variables of $\mathcal{H}_{i}$ plus two new variables $A_{h}$ and $S_{i}^{\prime}$. Define a morphism $\eta$ by $\eta(a)=A_{h}$ for all $a \in \Sigma$ and $\eta(A)=A$ for every variable $A$ of $\mathcal{H}_{i}$. We define the right-hand side mapping $\rho_{i}^{\prime \prime}$ of $\mathcal{H}_{i}^{\prime \prime}$ by: $\rho_{i}^{\prime \prime}\left(A_{h}\right)=h$ if $\ell \geq 0$ and $\rho_{i}^{\prime \prime}\left(A_{h}\right)=h^{-1}$ if $\ell<0$, $\rho_{i}^{\prime \prime}\left(S_{i}^{\prime}\right)=\left(S_{i}^{\delta}\right)[1:|\ell| \cdot|h|]$ and $\rho_{i}^{\prime \prime}(A)=\eta\left(\rho_{i}(A)\right)$ for all variables $A$ of $\mathcal{H}_{i}$. Note that $S_{i}^{\delta}$ derives to $h^{\delta \cdot\left|u_{i}\right|}$ if $\ell \geq 0$ and to $h^{-\delta \cdot\left|u_{i}\right|}$ if $\ell<0$. Since $|\ell| \leq \delta \cdot\left|u_{i}\right|$, $\left(S_{i}^{\delta}\right)[1:|\ell| \cdot|h|]$ derives to $h^{\ell}$. The start variable of $\mathcal{H}_{i}^{\prime \prime}$ is $S_{i}^{\prime}$. The size of $\mathcal{H}_{i}^{\prime \prime}$ is $s_{i}+|h|+\delta=s_{i}+O(1)$, since $|h|$ and $\delta$ are constants.

A subgroup of a hyperbolic group is undistorted if and only if it is quasiconvex [26, Lemma 1.6]. That cyclic subgroups in hyperbolic groups are quasiconvex was shown by Gromov [15, Corollary 8.1.D]. Hence, infinite cyclic subgroups of a hyperbolic group are undistorted. Together with Theorems 6 and 7 we get:

Corollary 1. Let $H$ be a hyperbolic group and let $g, h \in H$ have the same order. Then the word problem for $\left\langle H, t \mid t^{-1} g t=h\right\rangle$ can be solved in polynomial time.

## 5 Future work

There is no hope to generalize Corollary 1 to the case of finitely generated associated subgroups (there exists a finitely generated subgroup $A$ of a hyperbolic group $G$ such that the membership problem for $A$ is undecidable [32]). On the other hand, it is known that the membership problem for quasiconvex subgroups of hyperbolic groups is decidable. What is the complexity of the word problem for an HNN-extension of a hyperbolic group $H$ with finitely generated quasiconvex associated subgroups? Even for the case where $H$ is free (where all subgroups are quasiconvex) the existence of a polynomial time algorithm is not clear.

The best known complexity bound for the word problem of a hyperbolic group is LogCFL, which is contained in the circuit complexity class $\mathrm{NC}^{2}$. This leads to the question whether the complexity bound in Corollary 1 can be improved to NC. Also the complexity of the the compressed word problem for an HNNextension of a hyperbolic group $H$ with cyclic associated subgroups is open (even in the case where the base group $H$ is free). Recall that the compressed word problem for a hyperbolic group can be solved in polynomial time [19].

Acknowledgments. This work is supported by the DFG project LO748/12-1.

## References

1. Artin, E.: Theorie der Zöpfe. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 4(1), 47-72 (1925)
2. Avenhaus, J., Madlener, K.: The Nielsen reduction and P-complete problems in free groups. Theoretical Computer Science 32(1-2), 61-76 (1984)
3. Bieri, R., Strebel, R.: Almost finitely presented soluble groups. Commentarii Mathematici Helvetici 53, 258-278 (1978)
4. Björner, A., Brenti, F.: Combinatorics of Coxeter Groups, Graduate Texts in Mathematics, vol. 231. Springer, New York (2005)
5. Boone, W.W.: The word problem. Annals of Mathematics. Second Series 70, 207265 (1959)
6. Britton, J.L.: The word problem. Annals of Mathematics 77(1), 16-32 (1963)
7. Charney, R.: An introduction to right-angled Artin groups. Geometriae Dedicata 125, 141-158 (2007)
8. Dehn, M.: Über unendliche diskontinuierliche Gruppen. Mathematische Annalen 71, 116-144 (1911)
9. Dehn, M.: Transformation der Kurven auf zweiseitigen Flächen. Mathematische Annalen 72, 413-421 (1912)
10. Diekert, V., Kausch, J.: Logspace computations in graph products. Journal of Symbolic Computation 75, 94-109 (2016)
11. Diekert, V., Weiß, A.: Context-free groups and Bass-Serre theory. CoRR abs/1307.8297 (2013), https://arxiv.org/abs/1307.8297
12. Epstein, D.B.A., Cannon, J.W., Holt, D.F., Levy, S.V.F., Paterson, M.S., Thurston, W.P.: Word Processing in Groups. Jones and Bartlett (1992)
13. Epstein, D.B.A., Holt, D.F.: The linearity of the conjugacy problem in wordhyperbolic groups. International Journal of Algebra and Computation 16(2), 287306 (2006)
14. Ghys, É., de La Harpe, P.: Sur les groupes hyperboliques d'après Mikhael Gromov. Progress in mathematics, Birkhäuser (1990)
15. Gromov, M.: Hyperbolic groups. In: Gersten, S.M. (ed.) Essays in Group Theory. pp. 75-263. No. 8 in MSRI Publ., Springer (1987)
16. Hagenah, C.: Gleichungen mit regulären Randbedingungen über freien Gruppen. Ph.D. thesis, University of Stuttgart (2000)
17. Haubold, N., Lohrey, M.: Compressed word problems in HNN-extensions and amalgamated products. Theory of Computing Systems 49(2), 283-305 (2011)
18. Holt, D.: Word-hyperbolic groups have real-time word problem. International Journal of Algebra and Computation 10, 221-228 (2000)
19. Holt, D.F., Lohrey, M., Schleimer, S.: Compressed decision problems in hyperbolic groups. In: 36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019, March 13-16, 2019, Berlin, Germany. LIPIcs, vol. 126, pp. 37:1-37:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2019), http://www.dagstuhl.de/dagpub/978-3-95977-100-9
20. Lipton, R.J., Zalcstein, Y.: Word problems solvable in logspace. Journal of the ACM 24(3), 522-526 (1977)
21. Lohrey, M.: Decidability and complexity in automatic monoids. International Journal of Foundations of Computer Science 16(4), 707-722 (2005)
22. Lohrey, M.: The Compressed Word Problem for Groups. SpringerBriefs in Mathematics, Springer (2014)
23. Lohrey, M.: Complexity of word problems for HNN-extensions. CoRR abs/2107.01630 (2021), https://arxiv.org/abs/2107.01630
24. Magnus, W.: Das Identitätsproblem für Gruppen mit einer definierenden Relation. Mathematische Annalen 106(1), 295-307 (1932)
25. Mattes, C., Weiß, A.: Parallel algorithms for power circuits and the word problem of the Baumslag group. CoRR abs/2102.09921 (2021), https://arxiv.org/abs/2102.09921
26. Minasyan, A.: On products of quasiconvex subgroups in hyperbolic groups. International Journal of Algebra and Computation 14(2), 173-195 (2004)
27. Myasnikov, A., Nikolaev, A.: Verbal subgroups of hyperbolic groups have infinite width. Journal of the London Mathematical Society 90(2), 573-591 (2014)
28. Myasnikov, A., Nikolaev, A., Ushakov, A.: Knapsack problems in groups. Mathematics of Computation 84, 987-1016 (2015)
29. Myasnikov, A., Ushakov, A., Won, D.W.: The word problem in the Baumslag group with a non-elementary Dehn function is polynomial time decidable. Journal of Algebra 345(1), 324-342 (2011)
30. Novikov, P.S.: On the algorithmic unsolvability of the word problem in group theory. American Mathematical Society, Translations, II. Series 9, 1-122 (1958)
31. Rabin, M.O.: Computable algebra, general theory and theory of computable fields. Transactions of the American Mathematical Society 95, 341-360 (1960)
32. Rips, E.: Subgroups of small cancellation groups. Bulletin of the London Mathematical Society 14, 45-47 (1982)
33. Serre, J.P.: Trees. Springer (2003)
34. Simon, H.U.: Word problems for groups and contextfree recognition. In: Proceedings of Fundamentals of Computation Theory, FCT 1979. pp. 417-422. AkademieVerlag (1979)
35. Stillwell, J.: Classical Topology and Combinatorial Group Theory (2nd edition). Springer (1995)
36. Waack, S.: The parallel complexity of some constructions in combinatorial group theory. Journal of Information Processing and Cybernetics, EIK 26, 265-281 (1990)
37. Wehrfritz, B.A.F.: On finitely generated soluble linear groups. Mathematische Zeitschrift 170, 155-167 (1980)
38. Weiß, A.: On the complexity of conjugacy in amalgamated products and HNN extensions. Ph.D. thesis, University of Stuttgart (2015)
39. Weiß, A.: A logspace solution to the word and conjugacy problem of generalized Baumslag-Solitar groups. In: Algebra and Computer Science. Contemporary Mathematics, vol. 677. American Mathematical Society (2016)

[^0]:    ${ }^{1}$ The concept of undistorted subgroups is defined for arbitrary finitely generated subgroups but we will need it only for the cyclic case.

