# Algorithmic problems in limits of free and hyperbolic groups

Jeremy Macdonald

Doctor of Philosophy

Department of Mathematics and Statistics

McGill University

Montréal, Québec

November 15, 2011

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Doctor of Philosophy

## DEDICATION

For Sean. Though it isn't the Skyline in five hours, I think he would be proud of me nonetheless.

## ACKNOWLEDGEMENTS

I would like to thank the following people and organizations for their role in bringing this work to a successful and happy conclusion.

Olga Kharlampovich, for her guidance, patience, and kindness.

Don and Betty Macdonald, for their constant love and support.

Svetla Vassileva, for being the best part of Montréal.

Dani Wise and Alexei Myasnikov, for many excellent courses in geometric group theory.

Terry Gannon, for getting me started in mathematics.

Andrey Nikolaev, Nicholas Touikan, Montserrat Casals-Ruiz, Ilya Kazachkov, and Denis Serbin, for making geometric group theory at McGill so much fun.

The Natural Sciences and Engineering Research Council of Canada, the Institut des Sciences Mathématiques, and the Department of Mathematics and Statistics of McGill University for financial support.

## ABSTRACT

We prove two theorems regarding the algorithmic theory of groups. First, that the compressed word problem in every finitely generated fully residually free group can be decided in polynomial time. As a corollary, the word problem in the automorphism group of such a group has a polynomial time solution. Second, for any torsion-free hyperbolic group $\Gamma$ and any group $G$ that is finitely generated and fully residually $\Gamma$, we construct a finite collection of homomorphisms, at least one of which is injective, from $G$ to groups obtained from $\Gamma$ by extensions of centralizers. As corollaries, we obtain an effective embedding of any finitely generated residually $\Gamma$ group into a finite direct product of groups obtained from $\Gamma$ by extensions of centralizers, and we prove that the word problem in any finitely generated residually $\Gamma$ group can be decided in polynomial time.

# ABRÉGÉ

On prouve deux théorèmes dans le domaine de la théorie algorithmique des groupes. D'abord on démontre que le problème de l'identité des mots compressés est soluble en temps polynomial dans tout groupe de type fini et discriminé par un groupe libre. Il s'en suit que le problème de l'identité de mots dans le groupe d'automorphismes d'un tel groupe est soluble en temps polynomial. Ensuite, pour tout groupe hyperbolique sans torsion $\Gamma$ et tout groupe $G$ de type fini qui est discriminé par $\Gamma$, on construit une collection finie d'homomorphismes, au moins un desquels est injective, entre $G$ et des groupes obtenus de $\Gamma$ par des extensions des centralisateurs. De ce fait, on obtient une inclusion algorithmique de tout groupe de type fini et séparé par $\Gamma$ dans un produit direct fini de groupes obtenus de $\Gamma$ par extensions des centralisateurs et on démontre que le problème de l'identité dans tout groupe de type fini et séparé par $\Gamma$ est soluble en temps polynomial.

TABLE OF CONTENTS

# CHAPTER 1
# Introduction

A group $G$ satisfies *residual* properties depending on whether or not any element, or finite set of elements, of $G$ can be preserved under a homomorphism to a particular group $\Gamma$. The target $\Gamma$ may be a fixed group or be allowed to range over a class of groups: free groups, finite groups, solvable groups, or any other interesting class.

When $\Gamma$ is allowed to be any free group, $G$ is said to be *fully residually free*. The theory of these groups has been particularly well-developed since the mid-1990s when their connection with the famous *Tarski problems* on the elementary theory of free groups arose. In O. Kharlampovich and A. Miasnikov's solution to Tarski's problems, fully residually free groups appear in the context of algebraic geometry as *coordinate groups of irreducible affine varieties* and in Z. Sela's work on the Tarski problems they appear as *limit groups*, quotients obtained from a sequence of homomorphisms to free groups. Many equivalent characterizations of fully residually free groups are now known, coming from different contexts. Much of the work on fully residually free groups has also been generalized to the case when $\Gamma$ is a fixed hyperbolic group, in which case $G$ is said to be *fully residually* $\Gamma$ or a $\Gamma$-*limit group*. In particular, many of the same characterizations apply.

Our work concerns algorithmic problems in limit groups and $\Gamma$-limit groups, and we will prove two main results. Our first result, which we prove in Chapter 3, is a polynomial time algorithm to solve the word problem in the automorphism group of

a limit group. This problem was known to be decidable, but not in polynomial time. Our solution uses the technique of *compressed words* employed by S. Schleimer to solve the problem for the automorphism group of a free group.

Solutions to several algorithmic problems in limit groups, including the conjugacy problem, membership problem, and our own result in Chapter 3, make use of the fact that every limit group embeds into a group obtained from a free group by a series of *extensions of centralizers* and that this embedding can be computed effectively. For a $\Gamma$-limit group $G$, an embedding into a group obtained from $\Gamma$ by a series of extensions of centralizers was known to exist, but its effective construction was not known. Our second result is to effectively construct a finite collection of homomorphisms, at least one of which must be an embedding, from $G$ to groups obtained from $\Gamma$ by extensions of centralizers.

We will begin in Chapter 2 by providing some necessary background material. We will focus on a discussing limit groups, as the general reader is expected to be least familiar with this material.

### 1.1 Statement of originality

Chapter 2 consists entirely of previously known results. The results of Chapter 3 and Chapter 4 are original, except where otherwise mentioned. Chapter 3 was published by the author as [Mac10]. The presentation has been altered somewhat to fit the thesis format and some of the proofs have been improved. Chapter 4 is expected to form the basis of a future publication with O. Kharlampovich.

We use the terms 'Theorem' and 'Corollary' exclusively for the major original results of this thesis. Results that we have cited from other works, usually without

proof, are termed 'Propositions'. The reader should be aware that some these propositions are deep theorems. In Chapter 2 we have decided to include proofs of a few 'propositions' for the reader's benefit. All other results are labelled as 'lemmas' and may contain both original and non-original material: we have indicated in the proof when non-original material is used.

# CHAPTER 2
# Background

## 2.1 Some notation

For elements $g, h$ of a group $G$ we denote by $[g, h]$ the commutator $g^{-1}h^{-1}gh$. The elements $g$ and $h$ commute if and only if $[g, h] = 1$. The conjugate $g^{-1}hg$ of $h$ by $g$ is denoted $h^g$. The image of $g$ under a homomorphism $\phi$ is denoted $g^\phi$ or $\phi(g)$.

We will usually describe groups in terms of presentations. For a set $X$ we denote by $X^*$ the set of finite words over $X$ and by $F(X)$ the free group on $X$. If $\mathcal{S} \subset F(X)$, then $\langle X \,|\, \mathcal{S}\rangle$ denotes the quotient group $F(X)/\mathrm{ncl}\,(\mathcal{S})$ where $\mathrm{ncl}\,(\mathcal{S})$ is the normal closure of $\mathcal{S}$. If $G = \langle X \,|\, \mathcal{S}\rangle$ and $\mathcal{R} \subset F(X \cup Y)$ then we allow the notation $\langle G, Y \,|\, \mathcal{R}\rangle = \langle X \cup Y \,|\, \mathcal{S} \cup \mathcal{R}\rangle$.

Every word $w$ over the alphabet $X^{\pm}$ represents an element of $G = \langle X \,|\, \mathcal{S}\rangle$, which we may also refer to as $w$. As a word, $w$ has a *word length* $|g|$, which is the number of symbols in $w$, and as an element of $G$ it has a *geodesic length* $\|w\|$ defined by

$$\|w\| = \min\{|u| \mid u \in F(X) \text{ and } u = w \text{ in } G\}.$$

## 2.2 Algorithmic problems in groups

At present, there is considerable interest in the study of algorithmic problems in groups. Many of the classical problems are *decision problems*, that is, problems that admit a yes/no answer. A decision problem is said to be *decidable* if there exists an algorithm that, on every (valid) input, terminates and outputs the correct answer.

From the point of view of combinatorial group theory, the most fundamental decision problem is the *word problem*. Fix a group $G$ generated by $g_1, \ldots, g_n$. A solution to the word problem for $G$ is an algorithm that, given as input a word $w(g_1, \ldots, g_n)$ over the generators, outputs 'yes' if and only if $w$ represents the identity element of $G$. One may also consider the group $G$ to be part of the input, in which case $G$ is given by a finite presentation $G = \langle X \mid S \rangle$. Many such problems have been studied. To name a few, the *conjugacy problem* asks whether two elements $g$ and $h$ are conjugate, the *power problem* asks if $g$ is a power of $h$, and the *isomorphism problem* asks if two finitely presented input groups are isomorphic. In Chapter 3 we study the word problem in the automorphism group of $G$, where $G$ is any *limit group* (defined in §2.5).

Many interesting problems are not decision problems, since the output must consist of more than a simple yes/no answer. One may need to output a group presentation, a homomorphism, a group element, et cetera. For example, the *geodesic problem* for a group $G = \langle g_1, \ldots, g_n \rangle$ asks to find, for a given word $w(g_1, \ldots, g_n)$, a word $u(g_1, \ldots, g_n)$ of shortest word length such that $w = u$ in $G$. When there exists an algorithm to solve a given problem, we say that the problem has an *effective* or *algorithmic* solution. The main result of Chapter 4 (Theorem 4.4.17) is an algorithm of this type: it produces a finite set of homomorphisms from an input group, one of which must be injective.

The study of an algorithmic problem often proceeds as follows: first, determine whether or not there exists an algorithm that solves the problem and second, find the most efficient algorithm for doing so. There are problems that cannot be solved: the

most famous example in combinatorial group theory is the proof that there exists a finitely presented group such that no algorithm can decide its word problem [Nov58], [Boo59].

The efficiency of an algorithm is typically measured by its *time complexity*.[1] One may always assume that the input of an algorithm consists of a finite string of bits encoding the input. The length $n$ of the bit string is the *size* of the input, though any quantity that varies linearly with $n$ may be regarded as the size of the input. Then the *(worst case) time complexity* of an algorithm is the function $T : \mathbb{N} \to \mathbb{N}$ such that $T(n)$ is the maximum, over all inputs of size $n$, of the number of elementary operations[2] the algorithm performs before halting.

Time complexity functions are usually classed according to *big-O notation*. This allows one to analyze algorithms independent of encoding and computation model and in terms of asymptotic behaviour. For any function $g : \mathbb{N} \to \mathbb{N}$, we set

$$O(g(n)) = \{f : \mathbb{N} \to \mathbb{N} \mid \exists\, N, m \in \mathbb{N}\, \forall n > m,\ f(n) \leq Ng(n)\}.$$

An algorithm is said to run in *polynomial time* if $T(n) \in O(n^d)$ for some $d \in \mathbb{N}$ and *exponential time* if $T(n) \in O(c^n)$ for some $c \in \mathbb{N}$. Usually, polynomial time algorithms are efficient enough to be useful in practice (at least for small values of $d$)

[1] *Space complexity* may also be considered.

[2] Exactly what constitutes an elementary operation depends on the model of computation used. One should have in mind a single Turing machine transition or a single CPU operation.

while non-polynomial time algorithms are not. In real-world applications however, big-O time complexity is only one factor in determining an algorithm's feasibility.

## 2.3 Hyperbolic and relatively hyperbolic groups

The classes of hyperbolic and relatively hyperbolic groups have been very influential since being introduced by Gromov in [Gro87]. We provide a brief introduction here.

### Hyperbolic groups

Let $G$ be a group generated by a finite set $X$ and denote $X^{-1} = \{x^{-1} \mid x \in X\}$ and $X^{\pm} = X \cup X^{-1}$. The *Cayley graph of $G$ with respect to $X$*, denoted $\mathrm{Cay}(G, X)$, is the directed graph with vertex set $G$ and edge set $\{(g, gx) \mid g \in G,\ x \in X^{\pm}\}$. Observe that if $(g, gx)$ is an edge then $(gx, g)$ is also an edge.

A metric space $(Y, d)$ is called a *geodesic metric space* if for every $x, y \in Y$ there exists a geodesic arc $[x, y]$ from $x$ to $y$ having length $d(x, y)$. We may realize $\mathrm{Cay}(G, X)$ as a geodesic metric space as follows: to each edge pair $\{(g, gx), (gx, g)\}$ we associate a copy of the unit interval $[0, 1]$ and identify the endpoint 0 with one of the vertices $g$ and 1 with the other vertex $gx$ (the choice here is arbitrary). The resulting object inherits a metric $d$ from the usual metric on $[0, 1]$ and forms a geodesic metric space which we may also refer to as the Cayley graph of $G$ with respect to $X$. Note that $d$ also makes $G$ into a metric space, with $d(g, h)$ being the length of the shortest word $x$ in the generators $X^{\pm}$ such that $gx = h$. The geodesic length $\|g\|$ of $g$ is precisely the distance $d(g, 1)$ from $g$ to the identity element.

Of course, the Cayley graph and resulting metric depend on the choice of generating set $X$. However, for any other *finite* generating set $Z$, one can show that

the Cayley graphs with respect to $Z$ and with respect to $X$ are quasi-isometric[3] as metric spaces. Consequently, it is only the quasi-isometry invariant properties of the Cayley graph that may give group theoretic information.

In a geodesic metric space $(Y, d)$ a *geodesic triangle* defined by three points $x, y, z$ is the union of three geodesic arcs $[x, y]$, $[y, z]$, $[z, x]$. Such a triangle is said to be $\delta$-*slim*, for a non-negative real $\delta$, if for every $w_1 \in [x, y]$ there exists $w_1' \in [y, z] \cup [z, x]$ such that

$$d(w_1, w_1') \leq \delta,$$

and similarly for every $w_2 \in [y, z]$ and $w_3 \in [z, x]$. The space $(Y, d)$ is $\delta$-*hyperbolic* if every geodesic triangle is $\delta$-slim.

**Definition 2.3.1.** A group $G$ is called *hyperbolic* if there exists a finite generating set $X$ of $G$ and a real number $\delta \geq 0$ such that the Cayley graph of $G$ with respect to $X$ is a $\delta$-hyperbolic metric space. □

The minimum $\delta$ such that $\mathrm{Cay}(G, X)$ is $\delta$-hyperbolic is referred to as the *hyperbolicity constant*. Though this constant depends of the generating set $X$, hyperbolicity of the group $G$ does not. Equivalent definitions of hyperbolicity may be found in [Aea91].

**Example 2.3.2.** Every finitely generated free group $F = \langle x_1, \ldots, x_n \,|\, - \rangle$ is hyperbolic: since the Cayley graph with respect to $\{x_1, \ldots, x_n\}$ is a tree, geodesic

[3] A map $\phi : X \to Y$ between metric spaces is a quasi-isometry if there exist constants $\lambda \geq 1$, $C \geq 0$, $D \geq 0$ such that for all $x, z \in X$, $\frac{1}{\lambda} d(x, z) - C \leq d(x^\phi, z^\phi) \leq \lambda d(x, z) + C$, and every point of $Y$ is within distance $D$ of a point of $X^\phi$.

triangles always take the degenerate form of 'tripods' and are 0-slim. The free abelian groups $\mathbb{Z}^n$ are not hyperbolic unless $n = 1$. Indeed, for $\mathbb{Z}^2 = \langle a, b \,|\, [a, b] \rangle$ the Cayley graph with respect to $\{a, b\}$ is a grid, and a square of side length $m + 1$ is a geodesic triangle for any three of its corners and is not $m$-slim. The fundamental group of a surface with negative Euler characteristic is hyperbolic. $\square$

**Relatively hyperbolic groups**

Relatively hyperbolic groups are a generalization of hyperbolic groups in which controlled non-hyperbolicity is permitted. We review here the definition developed in [Bow99] (see also [GM08]) stating that the *coned-off Cayley graph* should be hyperbolic and *fine*. Equivalent definitions are given in [Gro87], [Osi06b], and [Far98].

Let $G$ be generated by the finite set $X$ and let $\mathcal{H} = \{H_1, \ldots, H_k\}$ be a collection of finitely generated subgroups of $G$. For every $i = 1, \ldots, k$ and every coset $gH_i$ we add to $\mathrm{Cay}(G, X)$ a vertex labelled by $gH_i$ and for each $h \in gH_i$ we add an edge between $h$ and $gH_i$. This forms the *coned-off Cayley graph* of $G$ with respect to $\mathcal{H}$ and $X$.

A *simple cycle* in a directed graph is a sequence of vertices $v_1, \ldots, v_n$ such that $(v_i, v_{i+1})$ is an edge for $i = 1, \ldots, n-1$ and all $v_i$ are distinct except $v_1$ and $v_n$ which coincide. A graph is said to be *fine* if for every edge $e$ and integer $L > 0$ there are only finitely many simple cycles of length $L$ that contain $e$.

**Definition 2.3.3.** A finitely generated group $G$ is said to be *hyperbolic relative to a finite collection* $\mathcal{H} = \{H_1, \ldots, H_k\}$ of finitely generated subgroups if there exists a finite generating set $X$ of $G$ and a real number $\delta$ such that the coned-off Cayley

graph of $G$ with respect to $\mathcal{H}$ and $X$ is fine (as a graph) and $\delta$-hyperbolic (as a metric space). $\square$

**Example 2.3.4.** The group $\mathbb{Z} * \mathbb{Z}^2$ is hyperbolic relative to $\mathbb{Z}^2$. The group $\mathbb{Z}^2 = \langle x, y \,|\, [x, y] \rangle$ is not hyperbolic relative to $\mathbb{Z} = \langle x \rangle$. Though the coned-off Cayley graph is hyperbolic, it is not fine. $\square$

The subgroups $H_i$, and their conjugates, are referred to as *parabolic* subgroups. An element $g \in G$ is called *parabolic* if it is an element of a parabolic subgroup, otherwise it is *hyperbolic*.

The relatively hyperbolic groups appearing in this work have the property that all parabolic subgroups are free abelian groups.

**Definition 2.3.5.** A group $G$ is called *toral relatively hyperbolic* if $G$ is torsion-free and hyperbolic relative to a collection $\mathcal{H}$ of (free) abelian proper subgroups of $G$. $\square$

If $G$ is toral relatively hyperbolic, then for each maximal abelian non-cyclic subgroup $M \leq G$, the collection $\mathcal{H}$ must include exactly one subgroup conjugate to $M$, and must not include any proper non-trivial subgroup of any conjugate of $M$. Indeed, one can show that including in $\mathcal{H}$ two conjugates of $M$, or including a proper subgroup of a conjugate, leads to non-fineness of the coned-off Cayley graph. Excluding all conjugates of $M$ leads to non-hyperbolicity.

**Properties of relatively hyperbolic groups**

A group $G$ is called a *CSA group*[4] if every maximal abelian subgroup $M$ of $G$ is *malnormal*, meaning $M^g \cap M = 1$ for all $g \in G \setminus M$. Torsion-free hyperbolic groups are CSA (see Proposition 12 of [MR96]), and in fact all toral relatively hyperbolic groups are CSA (see 1.4 of [KM09] or Lemma 2.5 of [Gro09]). CSA groups play an important role in algebraic geometry over groups, as we will see shortly. They have the useful property that commutation is a transitive (binary) relation on the set of non-trivial elements, i.e. for every triple of non-trivial elements $x, y, z$ if $[x, y] = 1$ and $[y, z] = 1$ then $[x, z] = 1$. Details on CSA groups can be read in [MR96].

Much work has been done on algorithmic problems in relatively hyperbolic groups. We take note of the following for later use.

**Lemma 2.3.6.** *Let $G$ be a toral relatively hyperbolic group. The following hold.*

*(1) The conjugacy problem in $G$, and hence the word problem, is decidable.*

*(2) If $G$ is non-abelian then we may effectively construct two non-commuting elements of.*

*(3) If $g \in \Gamma$ is a hyperbolic element, then the centralizer $C(g)$ of $g$ is an infinite cyclic group. Further, a generator for $C(g)$ can be effectively constructed.*

*Proof.* The first statement is the main theorem of [Bum04]. For the second, we need only enumerate pairs $(g, h) \in G \times G$ until we find a pair with $[g, h] \neq 1$.

[4] CSA stands for 'conjugately separated maximal abelian'.

For the third statement, let $g \in \Gamma$ be a hyperbolic element. Theorem 4.3 of [Osi06a] shows that the subgroup

$$E(g) = \{h \in \Gamma \mid \exists\, n \in \mathbb{N} :\ h^{-1} g^n h = g^n\}$$

has a cyclic subgroup of finite index. Since $\Gamma$ is torsion-free, $E(g)$ must be infinite cyclic (see for example the proof of Proposition 12 of [MR96]). Clearly $C(g) \leq E(g)$, hence $C(g)$ is infinite cyclic.

To construct a generator for $C(g)$, consider the following results of D. Osin in [Osi06a] (see Lemma 5.16 and the proof of Theorem 5.17):

(i) there exists a constant $N$, which depends on $\Gamma$ and $|g|$ and can be computed, such that if $g = f^n$ for some $f \in \Gamma$ and $n \in \mathbb{Z}$ then $n \leq N$;

(ii) there is a computable function $\beta : \mathbb{N} \to \mathbb{N}$ such that if $f$ is an element of $\Gamma$ with $f^n = g$ for some $n \in \mathbb{N}$, then $f$ is conjugate to some element $f_0$ satisfying $|f_0| \leq \beta(|g|)$.

We proceed as follows. For every element $f$ in the ball of radius $\beta(|g|)$ in $\mathrm{Cay}(\Gamma, A)$, check whether or not $f^n$ is conjugate to $g$ for any $1 \leq n \leq N$. Of these, choose $f$ with $n$ maximum and find a conjugating element $h$ (we may do so by enumerating elements of $\Gamma$ until a conjugating element is found). Let $\overline{g}$ be a generator of $C(g)$. We claim that $h^{-1} f h = \overline{g}$ or $h^{-1} f h = \overline{g}^{-1}$. Indeed, $h^{-1} f h$ commutes with $g$, hence $h^{-1} f h = \overline{g}^k$ for some $k$ and so

$$g = (h^{-1} f h)^n = \overline{g}^{kn}. \tag{2.1}$$

Suppose $k > 0$. Since $\overline{g}^{kn} = g$, (ii) implies that $\overline{g}$ is conjugate to some element $g_0$ in the ball of radius $\beta(|g|)$, hence $g_0^{kn}$ is conjugate to $g$. By maximality of $n$, $k$ must be 1 and $h^{-1}fh = \overline{g}$. If $k < 0$, we see that $h^{-1}fh = \overline{g}^{-1}$. □

## 2.4 Algebraic geometry over groups

Following [BMR99] and [KM98a] we introduce some basic notions of algebraic geometry over groups.

### Basic definitions

Let $\Gamma$ be a group generated by a finite set $A$ and $F(X)$ the free group with basis $X = \{x_1, x_2, \dots x_n\}$. In analogy with the polynomial ring $\mathbb{R}[X]$ we define

$$\Gamma[X] = \Gamma * F(X),$$

where $*$ denotes the free product. For an element $s$ of $\Gamma[X]$, the expression

$$s = 1$$

is called an *equation* over $\Gamma$. As an element of the free product, $s$ can be written as a product of elements from $X^{\pm}$, which we call *variables*, and elements from $A^{\pm}$, which we call *constants*. To emphasize this we sometimes write $s(X, A) = 1$ or $s(x_1, \dots, x_n) = 1$. Every subset $S \subset \Gamma[X]$ corresponds to the *system of equations* $\{s = 1 \mid s \in S\}$, which we denote simply by $S$, or by $S = 1$ for emphasis. A *solution* of the system $S$ over a group $\Gamma$ is a tuple of elements $g_1, \dots, g_n \in \Gamma$ such that after replacement of each $x_i$ by $g_i$ the left hand side of every equation in $S(X, A) = 1$ represents the trivial element of $\Gamma$, i.e. $s(g_1, \dots, g_n) = 1$ in $G$ for all $s \in S$.

To study equations over a fixed group $\Gamma$ it is convenient to consider the *category of* $\Gamma$*-groups*. These are groups which contain $\Gamma$ as a distinguished subgroup, i.e. an object is a group $H$ together with a monomorphism $\Gamma \hookrightarrow H$. A morphism from $H$ to $K$ is a $\Gamma$-*homomorphism*, which is a homomorphism $\phi : H \to K$ such that $g^\phi = g$ for every $g \in \Gamma$. We always assume that a homomorphism between two $\Gamma$ groups is a $\Gamma$-homomorphism, and we denote by $\mathrm{Hom}_\Gamma(H, K)$ the set of all $\Gamma$-homomorphisms from $H$ to $K$. The group $\Gamma[X]$ is a $\Gamma$-group[5] .

A solution to the system $S$ over $\Gamma$ can be described as a $\Gamma$-homomorphism $\phi : \Gamma[X] \to \Gamma$ such that $s^\phi = 1$ for all $s \in S$. Let $\mathrm{ncl}\,(S)$ be the normal closure of $S$ in $\Gamma[X]$ and

$$\Gamma_S = \Gamma[X]/\mathrm{ncl}\,(S)\,.$$

Then every solution of $S$ in $\Gamma$ gives rise to a $\Gamma$-homomorphism $\Gamma_S \to \Gamma$, and vice versa. We use the notation $\bar{g} = (g_1, \ldots, g_n)$ for elements of $\Gamma^n$ and write $S(\bar{g}) = 1$ if $\bar{g}$ is a solution to $S$. The set of all solutions in $\Gamma$ of the system $S = 1$ is called the *algebraic variety* defined by $S$ and is denoted $V_\Gamma(S)$ or $V(S)$. To $V_\Gamma(S)$, or rather to $S$, we associate a normal subgroup $R_\Gamma(S)$ (or $R(S)$) of $\Gamma[X]$ called the *radical* of $S$ and defined by

$$R_\Gamma(S) = \{T(x) \in \Gamma[X] \,|\, \forall\, \bar{g} \in \Gamma^n \,(S(\bar{g}) = 1 \implies T(\bar{g}) = 1)\}.$$

[5] Further, it is a free object in the category of $\Gamma$-groups.

Equivalently, $R_\Gamma(S)$ is the intersection of the kernels of all $\phi \in \mathrm{Hom}(\Gamma_S, \Gamma)$. Note that $\mathrm{ncl}\,(S) \subset R_\Gamma(S)$. The quotient of $\Gamma[X]$ by $R_\Gamma(S)$ is called the *coordinate group* of the algebraic variety $V_\Gamma(S)$ (or of $S$) and denoted

$$\Gamma_{R_\Gamma(S)} = \Gamma[X]/R_\Gamma(S).$$

Again, every solution of $S$ in $\Gamma$ can be described as a $\Gamma$-homomorphism $\Gamma_{R_\Gamma(S)} \to \Gamma$.

**Example 2.4.1.** Let $\Gamma$ be any torsion-free group and consider the system of equations (corresponding to) $S = \{x^2\}$. If $x \to g$ is any solution to $S$ over $\Gamma$, then $g^2 = 1$ hence $g = 1$. Consequently, $x \in R_\Gamma(S)$ so $\Gamma_{R(S)} = \langle \Gamma, x \,|\, x\rangle \simeq \Gamma$ whereas $\Gamma_S = \langle \Gamma, x \,|\, x^2 = 1\rangle \simeq \Gamma * \mathbb{Z}_2$. $\square$

**Systems without coefficients**

When a system of equations $S$ is a subset of the free subgroup $F(X)$ of $\Gamma[X]$ we say that $S$ is a system *without coefficients*. In this case, we may choose to work in the category of groups rather that $\Gamma$-groups. The radical $R(S)$ is then defined as a subset of $F(X)$ and the coordinate group is defined as $F(X)/R(S)$.

Systems of equations without coefficients arise naturally in the study of the set of homomorphisms $\mathrm{Hom}(G, \Gamma)$ from an arbitrary finitely presented group $G = \langle X \,|\, S\rangle$ to a fixed group $\Gamma$. We may think of the relators $S$ as a system of equations, without coefficients. The set of solutions to $S$ over $\Gamma$ is precisely $\mathrm{Hom}(G, \Gamma)$. Notice that since the inclusion $\mathrm{ncl}\,(S) \subset R(S)$ may be proper, the coordinate group $F(X)/R(S)$ may be a proper quotient of $G = F(X)/\mathrm{ncl}\,(S)$.

In the same manner, a system of equations $S(X, A) = 1$ with coefficients corresponds to the presentation $\langle X, A \,|\, S, \mathcal{R}\rangle$ of the $\Gamma$-group $\Gamma_S$, where $\Gamma = \langle A|\mathcal{R}\rangle$. Again, the coordinate group may be a proper quotient of $\Gamma_S$.

**Zariski topology and equational Noetherian property**

Let $\Gamma$ be a non-abelian CSA group. We define the *Zariski topology* on $\Gamma^n$ by taking algebraic varieties as the collection of closed sets. The entire space $\Gamma^n$ is closed since $V(\emptyset) = \Gamma^n$, and the empty set is closed since $V(\{xg^{-1}, xh^{-1}\}) = \emptyset$ for $g, h \in \Gamma$ with $g \neq h$. If $S$ and $T$ are systems of equations, then $V(S) \cap V(T) = V(S \cup T)$ and it follows that arbitrary intersections of algebraic sets are algebraic. The CSA property is needed to prove that union of two algebraic sets is algebraic[6] : if $g$ and $h$ are non-commuting elements of $\Gamma$ the system

$$\{[s, t] = 1,\ [s, t^g] = 1,\ [s, t^h] = 1,\ \ | \ s \in S,\ t \in T\}$$

defines the same variety as $V(S) \cup V(T)$.

We say that two systems of equations $S, T \subset \Gamma[X]$ are *equivalent* (over $\Gamma$) if $V(S) = V(T)$. A group $\Gamma$ is called *equationally Noetherian* if every system of equations $S$ over $\Gamma$ is equivalent to a finite subsystem $S_0 \subset S$.

When $\Gamma$ is equationally Noetherian, the Zariski topology on $\Gamma^n$ (for any $n \in \mathbb{N}$) is Noetherian, i.e. every properly descending chain of closed (algebraic) subsets is finite. An algebraic variety is *irreducible* if it is irreducible in the Zariski topology,

[6] If $\Gamma$ is not CSA, one may take algebraic varieties as a sub-basis for the closed sets and obtain a topology.

i.e. it cannot be written as the union of two proper non-empty algebraic varieties. In a Noetherian topology, every closed set $V$ may be decomposed uniquely as a union of finitely many irreducible varieties, which are called the *irreducible components* of $V$.

Equationally Noetherian groups are abundant, and include all of the following: linear groups ([Bry77], [BMR99]), in particular finite rank free groups [Gub86]; hyperbolic groups, both torsion-free [Sel09] and with torsion [RW10]; toral relatively hyperbolic groups [Gro05].

## 2.5 Limit groups

Our results are primarily concerned with the class of groups known as $\Gamma$-limit groups, where $\Gamma$ is any torsion-free hyperbolic group. The case when $\Gamma$ is a free group $F$ has been widely studied, and these groups are simply called limit groups. Chapter 3 is concerned with limit groups, and Chapter 4 with $\Gamma$-limit groups. We discuss the theory of limit groups in this section, and postpone discussion of the general case of $\Gamma$-limit groups until Chapter 4. Much of the material here is based on the presentation given in [KM10].

Limit groups have appeared in a variety of contexts, and as such have several (equivalent) definitions. We give four of these in the Propositions 2.5.1 and 2.5.2, the terminology of which will be explained, and proof given, in the following sections as we explore the related theory. Limit groups may be defined both in the category of groups and the category of $F$-groups, so we have two sets of definitions.

**Proposition 2.5.1** (definitions of limit groups, category of groups)**.** *Let $G$ be a finitely generated group. Then the statements below are equivalent.*

1. *$G$ is a non-abelian limit group.*
2. *$G$ is non-abelian and fully residually free.*
3. *$\mathrm{Th}_\exists(G) = \mathrm{Th}_\exists(F_2)$ in the language of group theory without constants.*
4. *There exists a system of equations $S$, without coefficients, over $F$ such that $V(S)$ is irreducible and $G \simeq F(X)/R(S)$.*

*Proof.* See below. □

**Proposition 2.5.2** (definitions of limit groups, category of $F$-groups)**.** *Let $F$ be a non-abelian free group and $G$ be a finitely generated $F$-group. Then the statements below are equivalent.*

1. *$G$ is a non-abelian limit group, in the category of $F$-groups ('restricted limit group').*
2. *$G$ is a non-abelian fully residually free (in the category of $F$-groups).*
3. *$\mathrm{Th}_\exists(G) = \mathrm{Th}_\exists(F)$ in the language of group theory with constants from $F$.*
4. *There exists a system of equations $S$ (possibly with coefficients) over $F$ such that $V(S)$ is irreducible and $G \simeq F_{R(S)}$.*

*Proof.* See below. □

Limit groups may also be described as topological limits of *marked groups* in the *Gromov-Hausdorff topology*, as groups which embed in ultrapowers of free groups, and as finitely generated subgroups of Lyndon's groups $F^{\mathbb{Z}[t]}$. We will not discuss the first and second description, referring the reader instead to [CG05],[KM10]. Subgroups of Lyndon's group will be discussed in Chapter 3. We list below some properties of limit groups.

**Proposition 2.5.3.** *Let $G$ be a limit group, either in the category of groups or $F$-groups, for a non-abelian free group $F$. Then the following statements are true.*

1. *$G$ is torsion-free.*
2. *Every subgroup of $G$ is a limit group.*
3. *For all $g, h \in G$ the subgroup $\langle g, h \rangle$ is either free of rank two or abelian.*
4. *$G$ has the CSA property.*
5. *$G$ is toral relatively hyperbolic.*

*Proof.* Items (1), (2), and (3) are not hard to prove, as we will see shortly. Item (4) is proved in [MR96] and (5) is proved in [Ali05] and [Dah03]. □

**Fully residually free groups**

The study of residual properties in groups dates back at least to Marshall Hall, Jr. [Hal59]. Let $\Gamma$ be any group.

**Definition 2.5.4.** A group $G$ is *fully residually* $\Gamma$, or $\Gamma$-*discriminated*, if for every finite subset $\{g_1, \ldots, g_n\}$ of non-trivial elements of $G$ there exists a homomorphism $\phi : G \to \Gamma$ such that $g_i^\phi \neq 1$ for all $i$. Equivalently, for every finite subset $\mathcal{F}$ of $G$ there is a homomorphism from $G$ to $\Gamma$ that is injective on $\mathcal{F}$. □

If the homomorphism $\phi$ can always be chosen from a set of homomorphisms $\Phi$ then we say that $\Phi$ *discriminates* $G$ into $\Gamma$. If the definition is only known to hold for $n = 1$ then we say that $G$ is *residually* $\Gamma$ or $\Gamma$-*separated*. When $\Gamma$ is a free group we say that $G$ is *fully residually free*. In this case, we may assume that $\Gamma$ is a free group two generators $F_2$. Indeed, $\Gamma$ need not be infinite rank since in any finite collection of elements of $\Gamma$ only a finite number $m$ of generators appear hence we may take $F = F_m$. Since $F_m$ is a subgroup of $F_2$, we may take $F = F_2$. We may consider fully

residually $\Gamma$ groups in the category of $\Gamma$-groups, interpreting 'homomorphism' in the definition as '$\Gamma$-homomorphism'.

**Example 2.5.5.** The free abelian groups $\mathbb{Z}^n$ are fully residually free. For $\mathbb{Z}^2$, suppose we are given a finite subset $\{(a_i, b_i)\}_{i=1}^m \subset \mathbb{Z}^2$ of non-zero elements. Then for any $N > \max_i\{|b_i|\}$, the homomorphism $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ defined by $\phi(1,0) = N$, $\phi(0,1) = 1$ meets the requirements since $\phi(a_i, b_i) = Na_i + b_i \neq 0$. $\square$

We can easily prove items (1), (2), and (3) of Proposition 2.5.3. Let $G$ be residually free. Then $G$ is torsion-free since for any non-trivial $g \in G$, any map $\phi : G \to F$ with $g^\phi \neq 1$ will fail to be a homomorphism if $g^n = 1$ for some $n \neq 0$. Property (2) is immediate.

For (3), let $g, h \in G$ and assume $\langle g, h\rangle$ is not abelian. Then $[g, h] \neq 1$ and there exists a homomorphism $\phi : G \to F$ that does not send any element of the set $\{g, h, [g, h]\}$ to 1. Consider the subgroup $H = \langle g^\phi, h^\phi\rangle \leq F$. Since $[g^\phi, h^\phi] \neq 1$, $H$ is not cyclic hence is free on $\{g^\phi, h^\phi\}$. If $\langle g, h\rangle$ is not free of rank 2, then there is a non-trivial word $w(g, h)$ in generators $g, h$ that represents the identity of $G$. But then

$$1 = w(g, h)^\phi = w(g^\phi, h^\phi),$$

which contradicts the fact that $H$ is a free group on $\{g^\phi, h^\phi\}$.

**Elementary theory of groups**

A *first order sentence* in the language of group theory is a (well-formed) formula in first order logic without free variables and using a binary function symbol '$\cdot$', a

unary function symbol ‘ $^{-1}$’, and a constant ‘1’. For example, the expression

$$\forall x \forall y \; (x^{-1}y^{-1}xy = 1) \tag{2.2}$$

is a first order sentence (we have omitted the binary function symbol ‘$\cdot$’). A sentence may be interpreted in a group $G$ in the obvious way: ‘1’ is interpreted as the group identity, ‘$\cdot$’ as group multiplication, ‘ $^{-1}$’ as group inversion, and the quantifiers range over elements of $G$. Consequently, the sentence above is assigned the value ‘true’ if and only if $G$ is abelian. We say the sentence is *true in* $G$.

**Definition 2.5.6.** The *elementary theory* of a group $G$ is the set of first order sentences that are true in $G$, and is denoted $\mathrm{Th}(G)$. The *existential theory* of $G$ is the set of sentences of the form ‘$\exists x_1 \exists x_2 \ldots \exists x_m \; S$’ that are true in $G$, where $S$ is any quantifier-free formula, and is denoted $\mathrm{Th}_\exists(G)$. The *universal theory* is defined analogously. □

In the category of $\Gamma$-groups, where $\Gamma$ is generated by a set $A$, we allow symbols from $A$ to appear in sentences as constant symbols. In this case, we refer to $\mathrm{Th}(G)$ as the *elementary theory of* $G$ *with constants*.

Note that two groups have the same existential theory if and only if they have the universal theory, since the negation of the existential sentence ‘$\exists x_1 \exists x_2 \ldots \exists x_m \; S$’ is the universal sentence ‘$\forall x_1 \forall x_2 \ldots \forall x_m \; \neg S$’.

**Example 2.5.7.** The existence of torsion in a group is encoded in its existential theory. The group $G$ has torsion if and only if for some $n \geq 2$ the sentence

$$\exists x \; (x \neq 1) \wedge (\overbrace{x \cdot x \cdot \cdots \cdot x}^{n} = 1)$$

is in $\mathrm{Th}_\exists(G)$. $\square$

**Example 2.5.8.** The free abelian groups $\mathbb{Z}$ and $\mathbb{Z}^2$ do not have the same elementary theory. For every three integers, two must have the same parity, hence the sentence

$$\forall x \forall y \forall z \exists w \left( (xy = w^2) \vee (xz = w^2) \vee (yz = w^2) \right)$$

is in $\mathrm{Th}(\mathbb{Z})$. This sentence is not true in $\mathbb{Z}^2$, though a similar sentence regarding any set of 5 elements serves to distinguish $\mathrm{Th}(\mathbb{Z}^2)$ from $\mathrm{Th}(\mathbb{Z}^3)$. $\square$

Two questions posed by Alfred Tarski around 1945 provided motivation for studying the elementary theory of groups:

1. Do all finite-rank non-abelian free groups have the same elementary theory?
2. Is the elementary theory of a finite-rank free group decidable?

A theory $\mathcal{T}$ is *decidable* if there exists an algorithm that determines, for any sentence $s$, whether or not $s \in \mathcal{T}$. The abelian free group $\mathbb{Z}$ is excluded from the first question since being abelian is determined by the universal theory, hence $\mathbb{Z}$ has a distinct theory. Both questions have been answered in the affirmative by Kharlampovich and Myasnikov [KM06], and the first question also by Sela [Sel06]. The authors described the class of finitely generated groups with the same elementary theory as $F_2$ as *coordinate groups of regular NTQ systems* (or *hyperbolic $\omega$-residually free towers* in Sela's description). We will discuss NTQ systems in Chapter 4.

The same questions may be asked of the existential theory of non-abelian free groups. We will prove the equivalence (3) $\iff$ (2) of Proposition 2.5.1, showing that the non-abelian group with the same existential theory of $F_2$ are precisely the non-abelian fully residually free groups. Note that since $F_n \hookrightarrow F_2 \hookrightarrow F_n$ (for $n \geq 2$),

any existential sentence which holds in $F_n$ must also hold in $F_2$, and conversely, hence all non-abelian free groups have the same existential theory.

Let $G$ be non-abelian and fully residually free. By Proposition 2.5.3 (3), there exist $g, h \in G$ such that $\langle g, h\rangle \simeq F_2$. Any existential sentence that holds in $F_2$ also holds in $G$, so $\mathrm{Th}_\exists(F_2) \subset \mathrm{Th}_\exists(G)$.

Now take any sentence $\exists z_1 \ldots \exists z_m \, S(\bar{z})$ in $\mathrm{Th}_\exists(G)$, where $S(\bar{z})$ is a formula without quantifiers and $\bar{z} = (z_1, \ldots, z_m)$. We may assume that $S(\bar{z})$ is written in disjunctive normal form. Then there exists a (conjunctive) clause

$$(s_1(\bar{z}) = 1) \wedge \ldots \wedge (s_k(\bar{z}) = 1) \wedge (t_1(\bar{z}) \neq 1) \wedge \ldots \wedge (t_l(\bar{z}) \neq 1)$$

in $S(\bar{z})$ and an $m$-tuple $\bar{g} = (g_1, \ldots, g_m) \in G^m$ satisfying the clause. Since the words $t_1(\bar{g}), \ldots, t_l(\bar{g})$ represent non-trivial elements of $G$, there exists a homomorphism $\phi : G \to F_2$ such that

$$t_i(\bar{g})^\phi = t_i(g_1^\phi, \ldots, g_m^\phi) \neq 1$$

for $i = 1, \ldots, l$. Since $\phi$ is a homomorphism, we also have $s_j(g_1^\phi, \ldots, g_m^\phi) = 1$ for $j = 1, \ldots, k$. Consequently, the sentence $\exists z_1 \ldots \exists z_m \, S(\bar{z})$ is satisfied by $\bar{g}^\phi = (g_1^\phi, \ldots, g_m^\phi) \in F_2^m$ hence is in $\mathrm{Th}_\exists(F_2)$.

Conversely, suppose $\mathrm{Th}_\exists(G) = \mathrm{Th}_\exists(F_2)$ and let $\{g_1, \ldots, g_n\}$ be a set of non-trivial elements of $G$. Since $G$ is finitely generated, it has a presentation $G = \langle X \mid S\rangle$, with $S$ possibly infinite. Consider $S$ as a system of equations over $F_2$ (without coefficiets). Since $F_2$ is equationally Noetherian, there exists a finite subsystem $T = \{t_1, \ldots, t_k\} \subset S$ such that $V_{F_2}(S) = V_{F_2}(T)$. Express each $g_i$ as a word $w_i(\bar{x})$ in

generators $\bar{x} = (x_1, \ldots, x_m)$ of $X$ and consider the sentence

$$\sigma : \exists z_1 \ldots \exists z_m (w_1(\bar{z}) \neq 1) \wedge \ldots \wedge (w_n(\bar{z}) \neq 1) \wedge (t_1(\bar{z}) = 1) \wedge \ldots \wedge (t_k(\bar{z}) = 1).$$

Then $\sigma \in \mathrm{Th}_\exists(G)$, witnessed by $\bar{z} = \bar{x}$, since all $g_i$ are non-trivial and $T \subset S$. Hence $\sigma \in \mathrm{Th}_\exists(F_2)$, so there exists $\bar{a} = (a_1, \ldots, a_n) \in F_2^n$ such that $w_i(\bar{a}) \neq 1$ and $t_j(\bar{a}) = 1$ for all $i, j$. Since $\bar{a}$ is a solution to $T$ and $V(S) = V(T)$, it is also a solution to $S$ and the corresponding map $\phi : G \to F_2$, i.e. the map defined by $g_i^\phi = a_i$, is a homomorphism. Since $w_i(\bar{a}) = w_i(\bar{x})^\phi$ the image of each $g_i$ under $\phi$ is non-trivial and $G$ is fully residually free.

Makanin proved that the existential theory of non-abelian free groups is decidable [Mak84]. An existential sentence

$$\exists \bar{z} \bigvee_{i=1}^{n} ((s_{i1}(\bar{z}) = 1) \wedge \ldots \wedge (s_{il_i}(\bar{z}) = 1) \wedge (t_{i1}(\bar{z}) \neq 1) \wedge \ldots \wedge (t_{im_i}(\bar{z}) \neq 1))$$

is true in a group $\Gamma$ if and only if one of the system of equations and inequations

$$\{s_{i1}(\bar{z}) = 1, \ldots, s_{il_i}(\bar{z}) = 1, t_{i1}(\bar{z}) \neq 1, \ldots, t_{im_i}(\bar{z}) \neq 1\}$$

has a solution in $\Gamma$. Makanin described an algorithm that decides if a given system of equations has a solution in a free group $F$. Razborov showed that one can find all of the solutions, giving an algorithm that produces a diagram that 'encodes' all solutions [Raz84]. These are now known as *Makanin-Razborov diagrams* and we will discuss them in Chapter 4. An extension of this algorithm by Kharlampovich and Miasnikov, which they call an *elimination process* [KM98b], plays an essential role in the solution to Tarski's second question.

Makanin's result on decidability of existential theory was extended to the case of torsion-free hyperbolic groups by Sela, and to relatively hyperbolic groups by Dahmani.

**Proposition 2.5.9** ([Sel09], [Dah09])**.** *The existential theory, with constants, of every toral relatively hyperbolic group is decidable.*

**Coordinate groups of algebraic varieties**

Coordinate groups of algebraic varieties over $\Gamma$ have a major role in algebraic geometry over $\Gamma$, and appear in the construction of Makanin-Razborov diagrams. They also completely describe the class of groups that are residually $\Gamma$ and fully residually $\Gamma$.

**Proposition 2.5.10.** *Let $\Gamma = \langle A|\mathcal{R}\rangle$ be an equationally Noetherian group generated by the finite set $A$ and let $G$ be a finitely generated $\Gamma$-group. Then*

1. *$G$ is residually $\Gamma$ if and only if $G$ is isomorphic to the coordinate group an algebraic variety over $\Gamma$, and*
2. *$G$ is fully residually $\Gamma$ if and only if $G$ is isomorphic to the coordinate group of an irreducible algebraic variety over $\Gamma$.*

*Proof.* Let $G$ be presented by $\langle X, A \,|\, S\rangle$. Since $G$ is a $\Gamma$-group, we may assume $\mathcal{R} \subset S$. Considering $S$ as a system of equations over $\Gamma$, we have $G \simeq \Gamma_S$.

An important fact, which we will use often in Chapter 4, is that

$$\mathrm{ncl}\,(S) = R(S) \iff \Gamma_S \text{ is residually } \Gamma,$$

which proves statement (1). To prove this fact, suppose there exists $w \in R(S) \setminus \mathrm{ncl}\,(S)$. Then $w \neq 1$ in $\Gamma_S$, but for every solution $\phi$ of $S$ we have $w^\phi = 1$, hence $\Gamma_S$ is

not residually $\Gamma$. Conversely, if $\Gamma_S$ is not residually $\Gamma$ then some non-trivial element $w \in \Gamma_S$ is sent to 1 under every solution of $S$ hence is in $R(S) \setminus \mathrm{ncl}\,(S)$.

Now assume that $G$ is fully residually $\Gamma$, so in particular $G$ is residually $\Gamma$ and $G \simeq \Gamma_{R(S)}$. Suppose, for contradiction, that $V(S)$ is reducible. Since $\Gamma$ is equationally Noetherian, closed set are algebraic so there exist systems $S_1, S_2$ such that

$$V(S) = V(S_1) \cup V(S_2) \tag{2.3}$$

with $V(S_1)$ and $V(S_2)$ both proper subsets of $V(S)$. It follows that neither $R(S_1)$ nor $R(S_2)$ is a subset of the other. Indeed, if say $R(S_1) \subset R(S_2)$, then any solution of $S_2$ would also be a solution of $S_1$ and we would have $V(S_2) \subset V(S_1)$. Hence there exist $w_1 \in R(S_1) \setminus R(S_2)$ and $w_2 \in R(S_2) \setminus R(S_1)$. But then every homomorphism $\phi : \Gamma_{R(S)} \to \Gamma$ is, by (2.3), either a solution to $S_1$, in which case $w_1^\phi = 1$, or a solution to $S_2$, in which case $w_2^\phi = 1$. So the set $\{w_1, w_2\}$ witnesses the fact that $\Gamma_{R(S)}$ is not fully residually $\Gamma$, a contradiction.

Conversely, suppose that $G \simeq \Gamma_{R(S)}$ such that $V(S)$ is irreducible. Suppose, for contradiction, that there exists a finite subset $\{w_1, \ldots, w_m\} \subset \Gamma_{R(S)}$ of non-trivial elements such that for every homomorphism $\phi : \Gamma_{R(S)} \to \Gamma$ there exists a $j$ such that $w_j^\phi = 1$. Every solution of the system $S$ is a homomorphism from $\Gamma_{R(S)}$ to $\Gamma$, hence is a solution to one of the systems $S \cup \{w_1\}, \ldots, S \cup \{w_m\}$. Consequently,

$$V(S) = \bigcup_{i=1}^{m} V(S \cup \{w_i\}).$$

For every $i$, $w_i \notin R(S)$ so the system $S$ has a solution that does not solve $w_i$. Hence each $V(S \cup \{w_i\})$ is a proper subset and $V(S)$ is reducible, which is a contradiction. $\square$

The above lemma also holds in the category of groups, with a similar proof.

**Limit groups**

In his solution to Tarksi's first question, Sela constructed [Sel01], for any finitely presented group $G$, an action of $G$ on an $\mathbb{R}$-tree[7] . The quotient of $G$ by the kernel of this action was termed a *limit group*. We present a reformulation of this definition, given in [BF09].

**Definition 2.5.11.** Let $G$ and $\Gamma$ be finitely generated groups, and $\{\phi_n : G \to \Gamma\}_{n=1}^{\infty}$ a sequence of homomorphisms. The *stable kernel* of $\{\phi_n\}_{n=1}^{\infty}$ is defined as

$$\underrightarrow{\mathrm{Ker}}(\phi_n) = \{g \in G \mid g \in \ker(\phi_n) \text{ for all but finitely many } n\}.$$

The sequence $\{\phi_n\}_{n=1}^{\infty}$ is called *stable* if for all $g \in G$ there exists $N \in \mathbb{N}$ such that for all $n > N$, $g^{\phi_n} = 1$, or for all $n > N$, $g^{\phi_n} \neq 1$. $\square$

Since the stable kernel is a normal subgroup of $G$, we may make the following definition.

**Definition 2.5.12.** A finitely generated group $G$ is a $\Gamma$-*limit group* if there exists a finitely generated group $H$ and a stable sequence of homomorphisms $\{\phi_n :$

[7] An $\mathbb{R}$-tree is a 0-hyperbolic geodesic space.

$H \to \Gamma\}_{n=1}^{\infty}$ such that

$$G \simeq H/\varinjlim \mathrm{Ker}(\phi_n).$$

*Limit groups* are precisely $F$-limit groups, where $F$ is any finite-rank free group. $\square$

We may now prove the equivalence (2) $\iff$ (1) of Proposition 2.5.1. Assume $G$ is fully residually free and let $B_n$ be the ball of radius $n$ in the Cayley graph of $G$ with respect to a (finite) generating set $X$. Since $B_n$ is finite, there is a homomorphism $\phi_n : G \to F_2$ that is injective on $B_n$. Any element $g \in G$ is in $B_n$ for all $n \geq \|g\|$, so the sequence $\{\phi_n\}_{n=1}^{\infty}$ is stable with $\varinjlim \mathrm{Ker}(\phi_n) = 1$, hence

$$G/\varinjlim \mathrm{Ker}(\phi_n) \simeq G$$

and $G$ is a limit group.

Conversely, assume that $G = H/\varinjlim \mathrm{Ker}(\phi_n)$ is a limit group and let $\{h_1, \ldots, h_m\}$ be a set elements of $H$ not in $\varinjlim \mathrm{Ker}(\phi_n)$. For each $h_i$, there exists an integer $n_i$ such that $h_i^{\phi_k} \neq 1$ for all $k \geq n_i$. Set $N = \max\{n_i \mid i = 1, \ldots, m\}$. Then $h_i^{\phi_N} \neq 1$ for all $i$ hence $G$ is fully residually free.

In the category of $\Gamma$-groups, we may make the same definitions. Note that if $G$ is a $\Gamma$-group and $\{\phi_n\}$ a stable sequence of $\Gamma$-homomorphisms, then $\Gamma \cap \varinjlim \mathrm{Ker}(\phi_n) = 1$ so $G/\varinjlim \mathrm{Ker}(\phi_n)$ is again a $\Gamma$-group. Limit groups in the category of $F$-groups are referred to as *restricted limit groups* in Sela's work [Sel01].

# CHAPTER 3
## Compressed words in limit groups

Let $F$ be the free group on a finite set $X$. The word problem in $F$ is easy to solve: simply cancel all pairs of the form $xx^{-1}$ and $x^{-1}x$ and check whether or not the resulting word is empty. A naive implementation of this algorithm solves the problem in time $O(n^2)$.

The word problem in the automorphism group $\mathrm{Aut}(F)$ of $F$, however, presents an interesting computational complexity problem. A classical result of Nielsen shows that $\mathrm{Aut}(F)$ is finitely generated, with the generators being described as word mappings $X \to (X^{\pm})^*$ [Nie19]. Consequently, the word problem in $\mathrm{Aut}(F)$ is easily seen to be decidable: the composition of automorphisms $\phi_n \dots \phi_1$ is the identity if and only if it acts as the identity on each generator of $X$, so it suffices to check whether or not $\phi_n \dots \phi_1(x)$ is equal to $x$, for every $x \in X$. Finding an efficient (polynomial time) algorithm, however, is difficult since the word length of $\phi_n \dots \phi_1(x)$ may be exponential in $n$, and was posed as an open problem in [KMSS03].

The problem remained open until Schleimer provided a solution in [Sch08], making use of Plandowski's technique of *compressed words* from computer science [Pla94]. Compressed words provide an efficient encoding of certain long words with regular structure, and Plandowski's key result is a method to check equality of two such

words by examining their encodings. They have now been studied in several contexts in group theory, including partially commutative groups, free products, certain group extensions, and HNN-extensions [LS07], [HL08], [HLM10].

In this chapter we prove that the *compressed word problem in limit groups* (defined below) is decidable in polynomial time and consequently the word problem in the autmorphism group of a limit group is also decidable in polynomial time.

### 3.1 The compressed word problem

A *straight-line program* (SLP) is a tuple $\mathbb{A} = (X, \mathcal{A}, A_n, \mathcal{P})$ consisting of a finite alphabet $\mathcal{A} = \{A_n, \dots, A_1\}$ of *non-terminal symbols*, a finite alphabet $X$ of *terminal symbols*, a *root* non-terminal $A_n \in \mathcal{A}$, and a set of *productions*

$$\mathcal{P} = \{A_i \to W_i \mid 1 \leq i \leq n\}$$

where $W_i \in \{A_j \mid j < i\}^* \cup X \cup \{\phi\}$, where $\phi$ represents the empty word. Straight-line programs are a type of context-free grammar. We 'run' the program $\mathbb{A}$ by starting with the one-letter word $A_n$ and replacing each non-terminal $A_i$ by $W_i$ and continuing this replacement procedure until only terminal symbols remain. The condition $j < i$ ensures that the program terminates. The resulting word is denoted $w_{\mathbb{A}}$, and we denote by $w_{A_i}$ the result of running the same program starting with $A_i$ instead of the root $A_n$. We say that $A_i$ *produces* $w_{A_i}$, or that $w_{A_i}$ is the *expansion* of $A_i$. The SLP $\mathbb{A}$ (and, abusing language, $w_{\mathbb{A}}$) is also called a *compressed word* over $X$. The reader may consult [Sch08] for a more detailed introduction to compressed words.

The *size* $|\mathbb{A}|$ of an SLP is the sum $\sum_{i=1}^{n} |W_i|$, where $|\cdot|$ denotes word length. We will be interested in analyzing the time complexity of algorithms taking as input

SLPs. For our purposes, it will always be the case that there exists an integer $M$ such that $|W_i| \leq M$ for all $i$. Therefore $|\mathbb{A}|$ is linear in the number $n$ of non-terminal symbols, so for time complexity analysis we may simply assume that $|\mathbb{A}| = n$. An SLP with $n$ non-terminal symbols can encode a word $w_{\mathbb{A}}$ of length at most $M^n$, and this bound is attainable.

**Example 3.1.1.** Consider the SLP with $X = \{a, b\}$, $\mathcal{A} = \{A_i \mid i = 0, \ldots, 10\}$, root non-terminal $A_{10}$ and production rules $A_0 \to a$, $A_1 \to b$, and

$$\begin{aligned} A_{4n-2} &\to A_{4n-4}A_{4n-3}, \\ A_{4n-1} &\to A_{4n-3}, \\ A_{4n} &\to A_{4n-2}, \\ A_{4n+1} &\to A_{4n-1}A_{4n}, \end{aligned}$$

for $n \geq 1$. We run the program as follows:

$$\begin{aligned} A_{10} &\to A_8A_9 \to A_6A_7A_8 \to A_4A_5A_5A_6 \to A_2A_3A_4A_3A_4A_4A_5 \\ &\to A_0A_1A_1A_2A_1A_2A_2A_3A_4 \to abbA_0A_1bA_0A_1A_0A_1A_1A_2 \\ &\to abbabbababbA_0A_1 \to abbabbababbab, \end{aligned}$$

hence $w_{A_{10}} = abbabbababbab$. $\square$

**Remark 3.1.2.** We may use any finite linear ordered set instead of $\{A_n, \ldots, A_1\}$ for the set of non-terminal symbols. As the linear order only serves to ensure that the program terminates, we will not mention it.

Any algorithm that takes as input a word over the alphabet $X$ can be applied to compressed words over $X$ by simply running the algorithm on the expansion $w_{\mathbb{A}}$,

but this converts a time $T(n)$ algorithm to one that runs in time $O(T(M^{|\mathbb{A}|}))$. In order to obtain polynomial time algorithms, we need to work directly with the SLP without expanding it. A fundamental result of W. Plandowski allows us to compare compressed words without computing their expansions.

**Proposition 3.1.3** ([Pla94])**.** *There is a polynomial time algorithm which, given straight-line programs $\mathbb{A}$ and $\mathbb{B}$ over an alphabet $X$, decides whether or not $w_{\mathbb{A}}$ and $w_{\mathbb{B}}$ are the same words, character-for-character.*

In the context of group theory, character-for-character inequality does not imply that the words represent different group elements. For a group $G$ generated by $g_1, \ldots, g_m$, we define the *compressed word problem for $G$* as the following: given an SLP $\mathbb{A}$ over $\{g_1^{\pm 1}, \ldots, g_m^{\pm 1}\}$ decide whether or not $w_{\mathbb{A}}$ represents the identity element of $G$. For free groups, the compressed word problem has a polynomial time solution.

**Proposition 3.1.4** ([Loh04])**.** *There is a polynomial time algorithm which, given a straight-line program $\mathbb{A}$ over the alphabet $X^{\pm}$, decides whether or not $w_{\mathbb{A}}$ represents the identity element of the free group on $X$.*

The reader may consult [Sch08] for highly accessible proofs of Propositions 3.1.3 and 3.1.4.

## 3.2 Extensions of centralizers and Lyndon's group $F^{\mathbb{Z}[t]}$

In order to study limit groups computationally, we make use of an embedding of limit groups into groups obtained from free groups by *extensions of centralizers* (Proposition 3.2.2). Extensions of centralizers give another equivalent characterization of limit groups (see Proposition 2.5.1).

Let $G$ be a group, $g \in G$, and let $C(g)$ be the centralizer of $g$ in $G$. The *free rank $m$ extension of the centralizer of $g$* is the group presented by

$$G' = \langle G, t_1, \ldots, t_m \,|\, [t_i, C(g)],\ [t_i, t_j],\ 1 \leq i, j \leq m \rangle.$$

Under certain conditions, $G'$ is fully residually $G$. A detailed study of these conditions is given in [BMR02], but we will only be interested here in the case of free groups and in Chapter 4 in the case of toral relatively hyperbolic groups.

**Proposition 3.2.1.** *Let $H$ be a toral relatively hyperbolic group, and consider a sequence of groups*

$$H = G_0 < G_1 < \ldots < G_n$$

*where $G_i$ is obtained from $G_{i-1}$ by a free extension of the centralizer of some element of $G_{i-1}$. Then $G_n$ is fully residually $H$.*

*Proof.* Follows immediately from the results of §5 of [BMR02] and Proposition 1.1 of [KM09]. □

In studying equations over free groups, R. Lyndon defined a group $F^{\mathbb{Z}[t]}$ that is central to the theory of limit groups and to our present purpose [Lyn60]. While Lyndon defined $F^{\mathbb{Z}[t]}$ in terms of 'parametric words', it is more useful for us to use a definition in terms of extensions of centralizers, given in [MR96].

For a group $G$, let $R(G)$ be a subset of $G$ such that no two elements of $R(G)$ are conjugate, and that if $g \in G$ and $C_G(g) = \langle g \rangle$ then there exists $u \in R(G)$ and $h \in G$ such that $C_G(g) = h^{-1} C_G(u) h$. The *extension of (all) cyclic centralizers of $G$*

is the group with presentation

$$\langle G, t_{u,i}\ (u \in R(G), i \in \mathbb{N}) \mid [t_{u,i}, u], [t_{u,i}, t_{u,j}],\ (u \in R(G), i, j \in \mathbb{N})\rangle. \tag{3.1}$$

Let $F$ be a free group of rank at least two. Then *Lyndon's group* $F^{\mathbb{Z}[t]}$ is the direct limit ('union') of the infinite chain of groups

$$F = H_0 < H_1 < H_2 < \dots \tag{3.2}$$

where $H_{i+1}$ is obtained from $H_i$ by extension of all cyclic centralizers.

Lyndon proved that $F^{\mathbb{Z}[t]}$ is fully residually free [Lyn60], hence so are all of its subgroups. Conversely, Kharlampovich and Miasnikov proved that every coordinate group of an irreducible affine variety over a free group embeds in $F^{\mathbb{Z}[t]}$, and that the embedding can be effectively constructed [KM98b],[KM99]. Recalling the equivalent definitions of limit groups given in Proposition 2.5.1, we have the following important result.

**Proposition 3.2.2** ([Lyn60],[KM98b],[KM99])**.** *Let $G$ be a finitely generated group. Then $G$ is fully residually free if and only if $G$ embeds into $F^{\mathbb{Z}[t]}$. Further, there exists an algorithm that, given a presentation of a fully residually free group $G$, computes an embedding of $G$ into $F^{\mathbb{Z}[t]}$.*

In [MRS05], the authors gave a construction of $F^{\mathbb{Z}[t]}$ using *infinite words* and using this were able to prove decidability of the conjugacy and power problems in $F^{\mathbb{Z}[t]}$. We will use two results from this construction: normal forms, which we discuss in detail in the next section, and a *Lyndon length function* on $F^{\mathbb{Z}[t]}$.

Let $l$ be a function $l : G \to A$, where $A$ is an ordered abelian group and let $g_1, g_2, g_3 \in G$. Define the *length of the maximum common prefix of* $g_1$ *and* $g_2$ as

$$c_p(g_1, g_2) = \frac{1}{2}\left(l(g_1) + l(g_2) - l(g_1^{-1}g_2)\right)$$

and define $\circ$ by

$$g_1 = g_2 \circ g_3 \iff (g_1 = g_2 g_3 \text{ and } l(g_1) = l(g_2) + l(g_3))\,.$$

The function $l$ is a *regular free Lyndon length function* on $G$ if it satisfies the following axioms:

(i) $\forall\, g \in G :\ l(g) \geq 0$ and $l(1) = 0$,

(ii) $\forall\, g \in G :\ l(g) = l(g^{-1})$,

(iii) $\forall\, g \in G :\ g \neq 1 \implies l(g^2) > l(g)$,

(iv) $\forall\, g_1, g_2 \in G :\ c_p(g_1, g_2) \in A$,

(v) $\forall\, g_1, g_2, g_3 \in G :\ c_p(g_1, g_2) > c_p(g_1, g_3) \implies c_p(g_1, g_3) = c_p(g_2, g_3)$ , and

(vi) $\forall\, g_1, g_2 \in G\ \exists\, h, g_1', g_2' \in G$ such that $l(h) = c_p(g_1, g_2)$ and $g_1 = h \circ g_1'$ and $g_2 = h \circ g_2'$.

For elements $g, h \in G$ we say that $h$ is a *prefix* of $g$ if there exists $g' \in G$ such that $g = h \circ g'$. It easily follows from the axioms that if $l(g) > 0$ then $g \neq 1$.

We consider the polynomial ring $\mathbb{Z}[t]$ as an ordered abelian group via the right lexicographic order induced by the direct sum decomposition $\mathbb{Z}[t] = \oplus_{m=0}^{\infty}\langle t^m \rangle$. We will use the natural isomorphism $\mathbb{Z}[t] \simeq \mathbb{Z}^\infty$ implicity, e.g. $(1, 2, -3) = 1 + 2t - 3t^2$. Using infinite words, [MRS05] proved that $F^{\mathbb{Z}[t]}$ admits a regular free Lyndon length

function $l : F^{\mathbb{Z}[t]} \to \mathbb{Z}[t]$. Though we will not need to know how $l$ is constructed, we give a brief example below to give the reader some intuition.

**Example 3.2.3.** Let $F = F(a, b)$ be the free group on generators $a, b$. We will describe a Lyndon length function $l : G \to \mathbb{Z}^2$ on the extension of centralizer $G = \langle a, b, t \mid [ab, t] \rangle$. The general construction, with proof, can be found in [KM05a] and [MRS05]. Let $w$ be a word over $G$. Since $G$ is an HNN-extension of $F$, $w$ may be written in *reduced form* as

$$w = g_1 t^{a_1} g_2 t^{a_2} \cdots g_m t^{a_m} g_{m+1},$$

where $g_i \in F$ for all $i$ and $[g_i, t] \neq 1$ for $i = 2, \ldots, m+1$. For any $M \in \mathbb{Z}$ set

$$l_1(w, M) = \|(g_1 (ab)^{\epsilon_1 M} g_2 \cdots g_m (ab)^{\epsilon_m M} g_{m+1}\| - m\|(ab)^M\|$$

where $\epsilon_i = \operatorname{sgn}(a_i)$ and $\|\cdot\|$ denotes geodesic length. There exists (see [MRS05]) a positive integer $M_0$ such that for any $M > M_0$, $l_1(w, M_0) = l_1(w, M)$. Then set the Lyndon length of $w$ to be

$$l(w) = \left( l_1(w, M_0), \sum_{i=1}^{m} |a_i| \right).$$

For example, the word $w = a(ab)^{11} t^{-1} aaba^{-1} t$ (which is in reduced form as written) has word length $|w| = 29$. For its Lyndon length, use $M = 30$ and compute

$$l_1(w, 30) = \|a(ab)^{11}(ab)^{-30} aaba^{-1}(ab)^{30}\| - 2\|(ab)^{30}\| = -21.$$

Hence $w$ has Lyndon length $l(w) = (-21, 2)$. $\square$

### 3.3 Normal forms for finitely generated subgroups of $F^{\mathbb{Z}[t]}$

Consider a chain of subgroups

$$F = G_0 < G_1 < \ldots < G_n, \tag{3.3}$$

where each $G_k$ is a subgroup of the group $H_k$ from (3.2) and is obtained from $G_{k-1}$ by free finite rank extensions of finitely many centralizers. Any such chain is specified by finite subsets $R(G_k) \subset R(H_k)$ and $T_k = \{t_{u,i} \mid u \in R(G_k),\ 1 \leq i \leq N_k(u)\}$, for $k \leq n$, such that

$$G_k = \langle G_{k-1}, T_k \,|\, [u, t_{u,j}],\ [t_{u,i}, t_{u,j}]\ \big(u \in R(G_{k-1}),\ 1 \leq i, j \leq N_k(u)\big)\ \rangle. \tag{3.4}$$

Any finitely generated subgroup of $F^{\mathbb{Z}[t]}$ is a subgroup of a group $G_n$ of this form. Let $X_0$ be a generating set of $F$ and set $X_k = X_0 \cup \bigcup_{i=1}^{k} T_i$. The set $X_k$ generates $G_k$. We will assume that each element $u \in \bigcup_{k=1}^{n} R(G_k)$ is given as a word in the alphabet $X_n^{\pm}$ such that $|u| = \|u\|$. Since the word problem in $F^{\mathbb{Z}[t]}$ is decidable[1] , we may find such representatives effectively using an exhaustive search.

In this section we define a normal form for elements of $G_n$. It is based on the normal form for elements of $F^{\mathbb{Z}[t]}$, expressed as infinite words, given in [MRS05].

For $\beta = (\beta_0, \beta_1, \ldots) \in \mathbb{Z}[t]$, let $\sigma(\beta) = \operatorname{sgn}(\beta_d)$ where $d = \deg(\beta)$. A word $w$ over $X_0^{\pm}$ is declared to be in normal form if and only if it is freely reduced. A word

[1] The conjugacy problem is decidable, hence so is the word problem since $g = 1$ if and only if $g$ is conjugate to 1.

$w$ over $X_k^{\pm}$ is in normal form if and only if $w$ is written as

$$w = g_1 u_1^{c_1} \tau_1^{\alpha_1} \dots g_m u_m^{c_m} \tau_m^{\alpha_m} g_{m+1}, \tag{3.5}$$

where $c_i$ are integers, $\alpha_i = (\alpha_{i1}, \dots, \alpha_{iN_k(u_i)}) \in \mathbb{Z}^{N_k(u_i)}$, $u_i \in R(G_{k-1})$, $\tau_i^{\alpha_i} = t_{u_i,1}^{\alpha_{i1}} t_{u_i,2}^{\alpha_{i2}} \cdots t_{u_i,N_k(u_i)}^{\alpha_{iN_k(u_i)}}$ and

(I) for all $i$, $\alpha_i \neq 0$,

(II) for all $i$, $g_i$ is a word over $X_{k-1}^{\pm}$,

(III) for every $i = 1, \dots, m$, either $[u_i, u_{i+1}] \neq 1$ or $[u_i, g_{i+1}] \neq 1$,

(IV) for any integers $q_i \neq 0$ with $\operatorname{sgn}(q_i) = \sigma(\alpha_i)$ we have

$$g_1 u_1^{q_1} g_2 \dots g_m u_m^{q_m} g_{m+1} = g_1 \circ u_1^{q_1} \circ g_2 \circ \dots \circ g_m \circ u_m^{q_m} \circ g_{m+1}.$$

It is instructive to think of $\tau_i^{\alpha_i}$ as a very large power of $u_i$. Note that that we do not require the $g_i$ to be written in normal form for $G_{k-1}$. We call $m$ the number of *syllables* of $w$.

**Lemma 3.3.1.** *Let $L = \max\{|u| \mid u \in \bigcup_{i=0}^{n} R(G_i)\}$. For every word $w$ over $X_n^{\pm}$ there is a word $\mathrm{NF}(w)$ in normal form such that $w = \mathrm{NF}(w)$ in $G_n$ and $|\mathrm{NF}(w)| \leq 10L|w|$. Further, the number of syllables of $\mathrm{NF}(w)$ is at most $|w|$.*

*Proof.* In [MRS05], a similar normal form is constructed for elements of $F^{\mathbb{Z}[t]}$, viewed as infinite words. We need only make a few modifications to their result, to ensure that the bound on $|\mathrm{NF}(g)|$ is achieved.

Proceed by induction on $n$. For the base case, we have that $G_0$ is a free group and the free reduction of $w$ is a normal form of length at most $|w|$. We may define

the number of syllables of every element of $G_0$ to be 1. Assume now that the theorem holds for $G_{n-1}$.

Since $G_n$ has the commutation relations $[u, t_{u,i}] = [t_{u,i}, t_{u,j}] = 1$, there exists a word $w'$ of the form

$$w' = h_1 \tau_1^{\alpha_1} h_2 \dots h_m \tau_m^{\alpha_m} h_{m+1}, \tag{3.6}$$

where

(i) $\tau_i^{\alpha_i} = t_{u_i,1}^{\alpha_{i1}} t_{u_i,2}^{\alpha_{i2}} \cdots t_{u_i,N_k(u_i)}^{\alpha_{iN_k(u_i)}}$ and $\alpha_i \neq 0$ for all $i$,

(ii) each $h_i$ is a word over $X_{n-1}^{\pm}$,

(iii) for every $i = 1, \dots, m$ either $[u_i, u_{i+1}] \neq 1$ or $[u_i, h_{i+1}] \neq 1$,

(iv) $|w'| \leq |w|$.

We now construct a normal form from $w'$. The key fact we need is the following: for any word $g$ over $X_{n-1}^{\pm}$, any $u \in R(G_{n-1})$, and any $r > |g|$,

$$u^{r+1} g = u \circ (u^r g) \quad \text{and} \quad g u^{r+1} = (g u^r) \circ u. \tag{3.7}$$

From the proof of Lemma 7.1 of [MRS05], it follows that (3.7) holds as long as $r$ is greater than the number of syllables in a normal form of $g$. Since $g \in G_{n-1}$, we have by induction that $g$ has a normal form with at most $|g|$ syllables.

Using this fact, it follows from the proof of Lemma 6.9 of [MRS05] that for $r = |h_i| + 1$ we have that

(v) $h_1 u^{\sigma(\alpha_1)(r_1+1)} = \left(h_1 u^{\sigma(\alpha_1) r_1}\right) \circ u^{\sigma(\alpha_1)}$,

(vi) for $i = 2, \dots, m$,

$$u_{i-1}^{\sigma(\alpha_{i-1})(r_{i-1}+1)} h_i u_i^{\sigma(\alpha_i)(r_i+1)} = u_{i-1}^{\sigma(\alpha_{i-1})} \circ \left(u_{i-1}^{\sigma(\alpha_{i-1}) r_{i-1}} h_i u_i^{\sigma(\alpha_i) r_i}\right) \circ u_i^{\sigma(\alpha_i)},$$

and

(vii) $u^{\sigma(\alpha_m)(r_m+1)}h_{m+1} = u^{\sigma(\alpha_m)} \circ \left(u^{\sigma(\alpha_m)r_m}h_{m+1}\right)$.

Now consider the word

$$w'' = g_1 u_1^{c_1}\tau_1^{\alpha_1} \dots g_m u_m^{c_m}\tau_m^{\alpha_m} g_{m+1},$$

where $g_1 = h_1 u_1^{\sigma(\alpha_1)r_1}$, $g_i = u_{i-1}^{\sigma(\alpha_{i-1})r_{i-1}} h_i u_i^{\sigma(\alpha_i)r_i}$ for $i = 2, \dots, m$ and $c_i = -\sigma(\alpha_i)(r_i + r_{i+1})$ for $i = 1, \dots, m$, and $g_{m+1} = u_m^{\sigma(\alpha_m)r_m} h_{m+1}$.

We claim that $w''$ is a normal form for $w$. Clearly $w'' = w$ in $G_n$. Property (I) of normal forms is immediate from (i), and (II) holds since all $u_i$ and $h_i$ are words over $X_{n-1}^{\pm}$. For (III), let $i \in \{1, \dots, m\}$ and assume that $[u_i, u_{i+1}] = 1$. Then

$$[u_i, g_{i+1}] = [u_i, u_i^{\sigma(\alpha_i)r_i} h_{i+1} u_{i+1}^{\sigma(\alpha_{i+1})r_{i+1}}] = u_{i+1}^{-\sigma(\alpha_{i+1})r_{i+1}} [u_i, h_{i+1}] u_{i+1}^{\sigma(\alpha_{i+1})r_{i+1}},$$

and from (iii) we know that $[u_i, h_{i+1}] \neq 1$, hence $[u_i, g_{i+1}] \neq 1$. Property (IV) follows from (v), (vi), and (vii). Set $\mathrm{NF}(w) = w''$.

The number $m$ of syllables of $\mathrm{NF}(w)$ is equal to the number of syllables in $w'$, which is bounded above by $|w'|$, hence $m \leq |w|$. For the bound on $|\mathrm{NF}(w)|$, we have

$$\begin{aligned}
|\mathrm{NF}(w')| &= \sum_{i=1}^{m} |\tau_i^{\alpha_i}| + \sum_{i=1}^{m+1} |g_i| + \sum_{i=1}^{m} |c_i||u_i| \\
&\leq \sum_{i=1}^{m} |\tau_i^{\alpha_i}| + \left( \sum_{i=1}^{m+1} |h_i| + \sum_{i=1}^{m+1} 2r_i L \right) + \sum_{i=1}^{m} (r_i + r_{i+1})L \\
&\leq |w'| + 3L \sum_{i=1}^{m+1} r_i \\
&\leq |w'| + 3L|w'| + 3L(m+1) \leq 10L|w|
\end{aligned}$$

as required. □

**Example 3.3.2.** Consider again the word $w = a(ab)^{11}t^{-1}aaba^{-1}t$ from Example 3.2.3. A normal form for $w$ is given by

$$a\left((ab)^{12}\right)t^{-1}(b^{-1}a^{-1}aaba^{-1}ab)\left((ab)^{-1}\right)t$$

where $g_1 = a$, $c_1 = 12$, $g_2 = b^{-1}a^{-1}aaba^{-1}ab$, $c_2 = -1$. It is not necessray to freely reduce $g_2$, though we may do so if desired. Notice that for any $q_1 < 0$ and $q_2 > 0$,

$$a(ab)^{q_1}(b^{-1}a^{-1}aaba^{-1}ab)(ab)^{q_2} = a \circ (ab)^{q_1} \circ (b^{-1}a^{-1}aaba^{-1}ab) \circ (ab)^{q_2},$$

satisfying (IV). □

### 3.4 Algorithm for the compressed word problem

Let $G_n$ be a obtained from $F$ by a finite sequence of finite rank free extension of centralizers, as in (3.3). Recalling from (3.4) that $N_k(u)$ is the number of distinct letters $t_{u,i}$ for a given $u \in R(G_k)$, set

$$N = 1 + \max\{N_k(u) \mid k \in \{0, \ldots, n-1\},\ u \in R(G_k)\}.$$

**Definition 3.4.1.** For any $P \in \mathbb{N}$ and $k \leq n$ define a function $\varphi_{(k,P)} : X_k^* \to X_{k-1}^*$ by $\varphi_{(k,P)}(w) = w$ for $g \in X_{k-1}^*$ and

$$\varphi_{(k,P)}(t_{u,i}) = u^{P^i}$$

and define $\Phi_{(n,P)} : X_n^* \to X_0^*$ by the composition

$$\Phi_{(n,P)} = \varphi_{(1,P^{N^{n-1}})}\varphi_{(2,P^{N^{n-2}})} \cdots \varphi_{(n-1,P^N)}\varphi_{(n,P)}.$$

□

Obverse that $\varphi_{(k,P)}$ is a homomorphism since, for every $i, j$,

$$[u, \varphi_{(k,P)}(t_{u,i})] = [u, u^{P^i}] = 1 = [u^{P^i}, u^{P^j}] = [\varphi_{(k,P)}(t_{u,i}), \varphi_{(k,P)}(t_{u,j})].$$

Consequently, $\varphi_{(k,P)}$ and $\Phi_{(n,P)}$ induce homomorphisms $\varphi_{(k,P)} : G_k \to G_{k-1}$ and $\Phi_{(n,P)} : G_n \to F$. We will use $\Phi_{(n,P)}$ to reduce the word problem in $G_n$ to the word problem in $F$.

**Theorem 3.4.2.** *Let $G_n$ be obtained from $F$ by a finite sequence of free finite rank extensions of centralizers as in (3.3) and let $w$ be a word over $X_n^{\pm}$. Then for any $P > 10L|w|$,*

$$\Phi_{(n,P)}(w) = 1 \text{ in } F \iff w = 1 \text{ in } G_n.$$

*Proof.* Since $\Phi_{(n,P)}$ is a homomorphism, if $w = 1$ in $G_n$ then $\Phi_{(n,P)}(w) = 1$ in $F$. It remains to show that for any $P > 10L|w|$,

$$w \neq 1 \text{ in } G_n \implies \Phi_{(n,P)}(w) \neq 1 \text{ in } F.$$

We proceed by induction on $n$. Letting $\Phi_{(0,P)} : F \to F$ be the identity map, there is nothing to prove in the base case $n = 0$. Assume the theorem holds up to $n-1$ and let $w \neq 1$ in $G_n$ and $P > 10L|w|$. By Lemma 3.3.1, $w$ has a normal form

$$\mathrm{NF}(w) = g_1 u_1^{c_1} \tau_1^{\alpha_1} g_2 \dots g_m u_m^{c_m} \tau_m^{\alpha_m} g_{m+1}$$

with $|\mathrm{NF}(w)| \leq 10L|w|$.

If no letter $t_{u,i}$ appears in $\mathrm{NF}(w)$, then $w \in X_{n-1}^*$ and $\Phi_{(n,P)}(w) = \Phi_{(n-1,P^N)}(w)$. Since

$$P^N > 10L|w| \geq |\mathrm{NF}(w)|$$

the induction assumption applies hence $\Phi_{(n,P)}(w) = \Phi_{(n-1),P^N)}(w) \neq 1$ in $F$. Otherwise, at least one $t_{u,i}$ appears with a non-zero power so we may assume that $m \geq 1$ and $\alpha_1 \neq 0$.

We claim that $\varphi_{(n,P)}(u_i^{c_i}\tau_i^{\alpha_i})$ is a non-zero power of $u_i$ of sign $\sigma(\alpha_i)$, for all $i$. We simplify notation by setting $u = u_i$, $a = \alpha_i$, and $d = N_{n-1}(u)$. We have that

$$\varphi_{(n,P)}(\tau_i^{\alpha_i}) = \varphi_{(n,P)}(t_{u,1}^{a_1} \cdots t_{u,d}^{a_d}) = u^{a_d P^d + a_{d-1} P^{d-1} + \ldots + a_1 P}.$$

We will give a lower bound of the magnitude of the exponent of $u$. Since, for all $s$,

$$|a_s| \leq |\mathrm{NF}(w)| \leq 10L|w| \leq P - 1,$$

we have that

$$\sum_{s=1}^{d-1} |a_s| P^s \leq \sum_{s=1}^{d-1} (P-1)P^s = P^d - P.$$

Consequently $|a_d P^d| - |a_{d-1}P^{d-1} + \ldots + a_1 P| \geq P$, and so

$$a_d P^d + a_{d-1} P^{d-1} + \ldots + a_1 P = C_i$$

where $|C_i| \geq P$ and $\mathrm{sgn}(C_i) = \mathrm{sgn}(a_d) = \sigma(a)$. Then

$$\varphi_{(n,P)}(u_i^{c_i}\tau_i^{\alpha_i}) = u^{C_i + c_i}$$

with $C_i + c_i \neq 0$ (since $|c_i| \leq |\mathrm{NF}(w)| < P$) and $\mathrm{sgn}(C_i + c_i) = \sigma(\alpha_i)$, which proves the claim.

Since $\varphi_{(n,P)}$ is the identity on $G_{n-1}$, we have, using property (IV) of normal forms,

$$\varphi_{(n,P)}(w) = \varphi_{(n,P)}(\mathrm{NF}(w)) = g_1 \circ u_1^{C_1+c_1} \circ g_2 \circ \cdots \circ g_m \circ u_m^{C_m+c_m} \circ g_{m+1}.$$

In particular, the above has Lyndon length

$$l(\varphi_{(n,P)}(\mathrm{NF}(w))) \geq l(u_1^{C_1+c_1}) > 0$$

hence $\varphi_{(n,P)}(w) \neq 1$ in $G_{n-1}$.

Now $\varphi_{(n,P)}(\mathrm{NF}(w))$ is a word over $X_{n-1}^*$ and we will show that $|\varphi_{(n,P)}(\mathrm{NF}(w))| < P^N$. In the worst case, $w = t_{u,i}t_{u,i}\ldots t_{u,i}$ where $|u| = L$ and $i = N-1$. Note that $w$ is already a normal form. Then

$$|\varphi_{(n,P)}(\mathrm{NF}(w))| = |u^{P^{N-1}|w|}| = |w|P^{N-1}L < P^N,$$

as required.

We may now apply the induction hypothesis to $\varphi_{(n,P)}(\mathrm{NF}(w))$ to obtain

$$\Phi_{(n,P)}(w) = \Phi_{(n-1,P^N)}(\varphi_{(n,P)}(\mathrm{NF}(w))) \neq 1$$

in the free group $F$. □

We can use Theorem 3.4.2 to solve the word problem in $G_n$ by setting $P = 10L|w| + 1$ and checking whether or not $\Phi_{(n,P)}(w)$ is trivial in $F$. Notice that the length of $\Phi_{(n,P)}(w)$ is bounded above by $P^{N^n}$.

We use this reduction to solve the compressed word problem in $G_n$.

**Theorem 3.4.3.** *Let $G_n$ be a group obtained from a free group by a finite sequence of free finite rank extensions of centralizers as in (3.3). There is an algorithm that decides the compressed word problem for $G_n$ in polynomial time.*

*Proof.* First, let us see that for any word $w$ and any $q \in \mathbb{Z}$ we can write a straight-line program $W^q$ of size $2|w| + \log_2 |q|$ producing $w^q$. We set the root production to be $W^q \to W^{q/2}W^{q/2}$, where the non-terminal $W^{q/2}$ produces $w^{q/2}$, and we continue by induction (making the appropriate adjustments when $q$ is odd). We create at most $\log_2 |q|$ non-terminals of the form $W^p$. We can obtain the program $W^1$, which produces $w$ and has size $2|w|$, by successively dividing $w$ in half. Similarly, we can obtain $W^{-1}$.

Now let $\mathbb{A}$ be a compressed word over $X_n^{\pm}$. For each $u \in \cup_{i=1}^{n} R(G_i)$ and $q \in \mathbb{Z}$, we can construct, by the remarks above, an SLP with root $U^q$ producing $u^q$ and having size $2|u| + \log_2 |q|$.

Let $P = P_n = 10L|w_{\mathbb{A}}| + 1$ and $P_k = P^{N^{n-k}}$. We build an SLP $\mathbb{A}_n$ by replacing every production of $\mathbb{A}$ of the form

$$A \to t_{u,i}^{\epsilon},$$

where $t_{u,i} \in T_n$ and $\epsilon = \pm 1$, by

$$A \to U^{\epsilon P^i}.$$

Notice that $w_{\mathbb{A}_n} = \varphi_{(n,P_n)}(w_{\mathbb{A}})$ in $G_{n-1}$. Repeat this process for $\mathbb{A}_n$, replacing $A \to t_{u,i}^{\epsilon}$, where $t_{u,i} \in T_{n-1}$, by $A \to U^{\epsilon P_{n-1}^i}$, to produce $\mathbb{A}_{n-1}$. Continue inductively until we obtain $\mathbb{A}_1$, which is an SLP producing $\Phi_{(n,P)}(w_{\mathbb{A}})$. By Theorem 3.4.2, $w_{\mathbb{A}_1} = 1$ in

$F$ if and only if $w_{\mathbb{A}} = 1$ in $G_n$ so we now apply Lohrey's algorithm (Proposition 3.1.4) to decide whether or not $w_{\mathbb{A}_1} = 1$ in $F$.

We need to show that the size of $\mathbb{A}_1$ is polynomial in the size of $\mathbb{A}$. For each program $\mathbb{A}_k$, we need, for each $u \in R(G_k)$, programs $U^{\pm P_k^1}, U^{\pm P_k^2}, \ldots, U^{\pm P_k^{N_k(u)}}$. Recalling that $N = 1 + \max\{N_k(u) \mid k \in \{0, \ldots, n-1\},\ u \in R(G_k)\}$, each new $U^{P_k^i}$ adds less than

$$2|u| + \log_2 |P_k^i| \leq 2L + \log_2(P_k^N)$$

new non-terminals to $\mathbb{A}_k$. Letting $M = \max_k\{|R(G_k)|\}$, the program $\mathbb{A}_k$ introduces less than

$$4LMN + 2N^2 M \log_2(P_k)$$

new non-terminals. In total, over all $n$ levels, the number of new non-terminals is bounded by

$$4LMNn + 2N^2 M \sum_{i=0}^{n-1} \log_2(P_{n-i}).$$

Noting that $L, M, N$, and $n$ are constants (i.e. they depend on $G_n$, not on $w$) and that $P_{n-i} = P^{N^i}$, we have that the number of new non-terminals is in

$$\begin{aligned} O\left(\sum_{i=0}^{n-1} \log(P_{n-i})\right) &= O\left(\sum_{i=0}^{n-1} N^i \log(P)\right) = O(\log(P)) \\ &= O\left(\log(10L \cdot 2^{|\mathbb{A}|} + 1)\right) = O(|\mathbb{A}|). \end{aligned}$$

Therefore $|\mathbb{A}_1| \in O(|\mathbb{A}|)$ and since Lohrey's algorithm runs in polynomial time in $|\mathbb{A}_1|$ we have a polynomial time algorithm for the compressed word problem in $G_n$. □

**Theorem 3.4.4.** *Let $G$ be a limit group. The compressed word problem for $G$ is decidable in polynomial time.*

*Proof.* Let $G$ be generated by $X$. By Proposition 3.2.2, we can effectively construct an embedding $\phi : G \to F^{\mathbb{Z}[t]}$. Since $G$ is finitely generated, $G^\phi$ is a subgroup of some group $G_n$ as described in (3.3). In the construction of $\phi$, the group $G_n$ is also constructed (see [KM98a]).

Now let $\mathbb{A}$ be an SLP over $X^{\pm}$. For each $y \in X^{\pm}$ introduce a non-terminal $Y^\phi$ that produces $y^\phi$. Note that $\max_{y \in X^{\pm}}\{|y^\phi|\}$ depends only on $G$ and $\phi$, so is constant with respect to the input $\mathbb{A}$. Replace each production of the form $A \to y$ by $A \to Y^\phi$ to form an SLP $\mathbb{A}'$. Then $w_{\mathbb{A}'} = \phi(w_{\mathbb{A}})$, so it suffices to solve the compressed word problem in $G_n$, which we have done in Theorem 3.4.3 in polynomial time. □

## 3.5 Word problem in the automorphism group of a limit group

In this section we prove that the word problem in the automorphism group of any limit group is decidable in polynomial time. In any group $G$, a polynomial time solution to the *compressed word problem* in $G$ yields a polynomial time solution to the *word problem* in any finitely generated subgroup of $\mathrm{Aut}(G)$.

**Proposition 3.5.1** ([Sch08],[LS07])**.** *Let $G$ be a finitely generated group and $H$ a finitely generated subgroup of* $\mathrm{Aut}(G)$*. Then the word problem in $H$ reduces in logarithmic space to the compressed word problem in $G$.*

Let us review briefly how this reduction works, following [Sch08]. First, one needs the generators of $H$ to be described by their action on generators of $G$. That is, if $G = \langle g_1, \ldots, g_n \rangle$ then each $\phi_i \in H$ must be described by

$$\phi_i(g_j) = w_{ij}(g_1, \ldots, g_n), \tag{3.8}$$

where $w_{ij}(g_1, \ldots, g_n)$ is a word over the alphabet $\{g_1 \ldots, g_n\}^{\pm 1}$. Now suppose $H = \langle \phi_1, \ldots, \phi_k \rangle$ and we want to decide whether or not a word $\phi_{i_1} \ldots \phi_{i_m}$ represents the trivial element of $H$. Build a set of non-terminals $\{A_{j,p}, \overline{A_{j,p}}\}$, where $j \in \{1, \ldots, n\}$ and $p \in \{1, \ldots, m\}$, with productions

$$\begin{aligned} A_{j,0} &\to g_j, \\ \overline{A_{j,0}} &\to g_j^{-1}, \\ A_{j,p} &\to w_{i_p j}(A_{1,p-1}, \ldots, A_{n,p-1}),\ p \geq 1, \\ \overline{A_{j,p}} &\to (w_{i_p j}(A_{1,p-1}, \ldots, A_{n,p-1}))^{-1},\ p \geq 1, \end{aligned}$$

where $w_{i_p j}(A_{1,p-1}, \ldots, A_{n,p-1})$ is the word $w_{i_p j}$ with every instance of $g_i$ replaced by $A_{i,p-1}$ and every instance of $g_i^{-1}$ replaced by $\overline{A_{i,p-1}}$. One may check that

$$w_{A_{j,m}} = \phi_{i_1} \ldots \phi_{i_m}(g_j).$$

Then the word problem in $H$ reduces to checking that $w_{A_{j,m}} = g_j$ for all $j$, i.e. it reduces to $n$ instances of the compressed word problem in $G$. Note that the total number of non-terminal symbols is linear in the length $m$ of the input.

Our goal then is to prove that for any limit group $G$, we can find a presentation for the automorphism group $\mathrm{Aut}(G)$.

**Theorem 3.5.2.** *Let $G = \langle X \mid R \rangle$ be a limit group. Then $\mathrm{Aut}(G)$ is finitely generated and one can construct a generating set in the form (3.8).*

*Proof.* First, consider the case when $G$ is a freely indecomposable limit group. The structure of the automorphism group of any such $G$ has been described in [BKM07] using an Abelian JSJ-decomposition of $G$. It follows from the results in §5 of that

paper that $\mathrm{Aut}(G)$ is finitely generated and the automorphisms can be described as in (3.8). Note that constructing an Abelian JSJ-decomposition of a limit group is effective (Theorem 13.1 of [KM05a]).

Now consider the case that $G$ has a free decomposition. Then $G$ has a *Grushko decomposition* as a free product

$$G = G_1 * \cdots * G_k * F_r, \tag{3.9}$$

where each $G_i$ is a freely indecomposable non-cyclic group and $F_r$ is a free group of rank $r$. This decomposition is unique in the sense that any other such decomposition has the same $k$ and $r$ and its freely indecompasable non-free factors are conjugate in $G$ to the factors $G_1, \ldots, G_k$. For limit groups, an algorithm for computing a Grushko decomposition is given in [KM05a].

The automorphism group of any free product of the form (3.9) has been described by Fouxe-Rabinovitch and Gilbert [Gil87] in terms of the automorphisms of its factors. $\mathrm{Aut}(G)$ is generated by the following automorphisms.

(i) *Permutation automorphisms.* For each pair of isomorphic factors $G_i \simeq G_j$, fix an automorhism $\phi_{ij}$. Choose $\phi_{ij}$ such that the collection is compatible, that is if $G_i \simeq G_j$ and $G_j \simeq G_k$ then $\phi_{ik} = \phi_{jk}\phi_{ij}$.

(ii) *Factor automorphisms.* Each automorphism of $G_i$ and of $F_r$ induces an automorphism of $G$ by acting as the identity on all other factors. Any product of such automorphisms is called a factor automorphism.

(iii) *Whitehead automorphisms.* Let $S$ be a basis of $F_r$. An automorhpism of $G$ is a Whitehead automorphism if there is an element $x$ in some $G_i$ or in $S$ such that

each factor $G_j$ is either conjugated by $x$ of fixed pointwise, and each $s \in S$ is sent to one of $s, sx, x^{-1}s, x^{-1}sx$.

It follows from Theorem 4.13 of [BKM07] that we can construct a compatible set of permutation automorphisms.

Since any subgroup of a limit group is again a limit group, each $G_i$ is a freely indecomposable limit group so we can construct a finite generating set for $\mathrm{Aut}(G_i)$ by the remarks above. The automorphism group of a free group $F(x_1, \ldots, x_r)$ is finitely generated by the Nielsen automorphisms,

$$\alpha_i(x_k) = \begin{cases} x_k^{-1} & k = i \\ x_k & k \neq i \end{cases}, \ i \in \{1, \ldots, r\}$$

$$\beta_{ij}(x_k) = \begin{cases} x_k x_j & k = i \\ x_k & k \neq i \end{cases}, \ i, j \in \{1, \ldots, r\}, i \neq j.$$

Consequently, the factor automorphisms are finitely generated.

Since each $G_i$ is finitely generated, as is $F_r$, the set of Whitehead automorphisms is finitely generated. Hence $\mathrm{Aut}(G)$ is finitely generated, and it is clear that all generators may be described as in (3.8). □

Combining Theorem 3.4.4, Proposition 3.5.1, and Theorem 3.5.2 we obtain our main result.

**Theorem 3.5.3.** *Let $G$ be a limit group. The word problem for $\mathrm{Aut}(G)$ is decidable in polynomial time.*

# CHAPTER 4
# Embedding limit hyperbolic groups into extensions of centralizers

Recall that in Chapter 3 we made use of an effective embedding of limit groups into groups obtained from a free group by iterated extensions of centralizers. Kharlampovich and Myasnikov have proved that, if $\Gamma$ is any toral relatively hyperbolic group and $G$ any finitely generated fully residually $\Gamma$ group, then there exists an embedding of $G$ into a group obtained from $\Gamma$ by iterated extensions of centralizers [KM09]. The construction, however, is not effective. In this chapter we give an algorithm that, for the case when $\Gamma$ is torsion-free hyperbolic, produces finitely many homomorphisms from $G$ into groups obtained from $\Gamma$ by iterated extensions of centralizers, one of which is an embedding.

## 4.1 $\Gamma$-limit groups

Since (relatively) hyperbolic groups are a generalization of free groups, it is natural to study elementary theory, algebraic geometry, and $\Gamma$-limit groups for any relatively hyperbolic group $\Gamma$. There is considerable ongoing work in this area, and we review a few results in this section. Many of the results concern the case when $\Gamma$ is torsion-free hyperbolic or toral relatively hyperbolic. As mentioned earlier, toral relatively hyperbolic groups are equationally Noetherian [Gro05]. We have the following characterization of $\Gamma$-limit groups.

**Proposition 4.1.1.** *Let $\Gamma$ be a toral relatively hyperbolic group and $G$ a finitely generated $\Gamma$-group. Then the following statements are equivalent.*

1. *$G$ is fully residually $\Gamma$.*
2. *$G$ is a $\Gamma$-limit group.*
3. *$\mathrm{Th}_\exists(G) = \mathrm{Th}_\exists(\Gamma)$ in the language of group theory with constants from $\Gamma$.*
4. *There exists a system of equations $S$ (possibly with coefficients) over $\Gamma$ such that $V(S)$ is irreducible and $G \simeq \Gamma_{R(S)}$.*
5. *$G$ is isomorphic to a subgroup of the Lyndon completion $\Gamma^{\mathbb{Z}[t]}$ of $\Gamma$.*

*Proof.* The equivalence (1) $\iff$ (2) is Theorem 5.10 of [Gro05], (3) $\iff$ (5) is Theorem C of [KM09], (3) $\iff$ (4) is Theorem D3 of [BMR99] together with the fact that toral relatively hyperbolic groups are equationally Noetherian, and (1) $\iff$ (4) was proved in Proposition 2.5.10. □

In fact, items (1), (2), and (4) are equivalent when $\Gamma$ is any equationally Noetherian group, see Theorem A of [KM09].

### 4.2 Notation

Throughout this chapter we fix $\Gamma = \langle A|\mathcal{R}\rangle$ a finitely presented torsion-free hyperbolic group, $F$ the free group on $A$, and $\pi : F \to \Gamma$ the canonical epimorphism.

The map $\pi$ induces an epimorphism $F[X] \to \Gamma[X]$, also denoted $\pi$, by fixing each $x \in X$. For a system of equations $S$ over $F$, we will often consider the system $S^\pi$ over $\Gamma$, which we may also denote simply by $S$. We will make other simplifications in notation when the context is clear. For example, the radical of $S^\pi$ over $\Gamma$ may be denoted $R_\Gamma(S^\pi)$, $R_\Gamma(S)$, or $R(S^\pi)$. Likewise, the coordinate group $\Gamma_{R_\Gamma(S^\pi)}$ may be denoted simply $\Gamma_{R(S)}$. Notice that the relators $\mathcal{R}$ of $\Gamma$ are in the radical $R_\Gamma(S)$ for

*every* system of equations $S$, hence

$$F_{R_\Gamma(S)} = \Gamma_{R(S)}.$$

In denoting a coordinate group $\Gamma_{R(S)} = \Gamma[X]/R(S)$ we always assume that $X$ is precisely the set of variables appearing in $S$.

### 4.3 Effective description of all homomorphisms to $\Gamma$

A major accomplishment in the theory of equations over free groups was the construction of *Hom-diagrams* (also called *Makanin-Razborov diagrams*). Such a diagram encodes the set of all (usually infinitely many) solutions to a given system of equations $S(X, A)$ over a free group $F$, or equivalently, the set of homomorphisms from a given group (or $F$-group) to $F$. We give a more precise description of Hom-diagrams in §4.3.2.

In this section, we describe an algorithm that take as input a system of equations $S(Z, A) = 1$ produces a diagram $\mathcal{T}$ that encodes the set $\mathrm{Hom}_\Gamma(\Gamma_{R(S)}, \Gamma)$. When $S$ is a system without coefficients, we interpret the input as the group presentation $G = \langle Z \,|\, S\rangle$ and the diagram $\mathcal{T}$ encodes instead the set $\mathrm{Hom}(G, \Gamma)$. Though our diagram $\mathcal{T}$ will encode $\mathrm{Hom}_\Gamma(\Gamma_{R(S)}, \Gamma)$, it is not a Makanin-Razborov diagram in the usual sense. We will comment on this at the end of the section.

There are two ingredients in this construction: first, the reduction of the system $S$ over $\Gamma$ to finitely many systems of equations over free groups, and second, the construction of Hom-diagrams for systems of equations over free groups. For the main result of this chapter, Theorem 4.4.17, we will need only the reduction to

systems of equations over free groups. However, we feel that the description of the diagram $\mathcal{T}$ is of sufficient interest to warrant the small detour.

**Notation 4.3.1.** We use the symbol $^-$ to denote both canonical epimorphisms $F(Z,A) \to \Gamma_{R(S)}$ and $F(Z) \to G$. For a homomorphism $\phi : F(Z,A) \to K$ (or $\phi : F(Z) \to K$) we define $\overline{\phi} : \Gamma_{R(S)} \to K$ (or $\overline{\phi} : G \to K$) by

$$\overline{\phi}\big(\overline{w}\big) = \phi(w),$$

where any preimage of $\overline{w}$ may be used. We will always ensure that $\overline{\phi}$ is a well-defined homomorphism.

### 4.3.1 Reduction to systems of equations over free groups

In [RS95], the problem of deciding whether or not a system of equations $S$ over a torsion-free hyperbolic group $\Gamma$ has a solution was solved by constructing *canonical representatives* for certain elements of $\Gamma$. This construction reduced the problem to deciding the existence of solutions in finitely many systems of equations over free groups, which had been previously solved. The reduction may also be used to find all solutions to $S$ over $\Gamma$, as described below.

**Lemma 4.3.2.** *Let $\Gamma = \langle A|\mathcal{R}\rangle$ be a torsion-free $\delta$-hyperbolic group and $\pi : F(A) \to \Gamma$ the canonical epimorphism. There is an algorithm that, given a system $S(Z,A) = 1$ of equations over $\Gamma$, produces finitely many systems of equations*

$$S_1(X_1,A) = 1, \ldots, S_n(X_n,A) = 1 \tag{4.1}$$

*over $F$ and homomorphisms $\rho_i : F(Z,A) \to F_{R(S_i)}$ for $i = 1,\ldots,n$ such that*

*(i) for every $F$-homomorphism $\phi : F_{R(S_i)} \to F$, the map $\overline{\rho_i \phi \pi} : \Gamma_{R(S)} \to \Gamma$ is a $\Gamma$-homomorphism, and*

*(ii) for every $\Gamma$-homomorphism $\psi : \Gamma_{R(S)} \to \Gamma$ there is an integer $i$ and an $F$-homomorphism $\phi : F_{R(S_i)} \to F(A)$ such that $\overline{\rho_i \phi \pi} = \psi$.*

*Further, if $S(Z) = 1$ is a system without coefficients, the above holds with $G = \langle Z \mid S \rangle$ in place of $\Gamma_{R(S)}$ and 'homomorphism' in place of '$\Gamma$-homomorphism'.*

*Proof.* The result is an easy corollary of Theorem 4.5 of [RS95], but we will provide a few details.

We may assume that the system $S(Z, A)$, in variables $z_1, \ldots, z_l$, consists of $m$ constant equations and $q - m$ triangular equations, i.e.

$$S(Z, A) = \begin{cases} z_{\sigma(j,1)} z_{\sigma(j,2)} z_{\sigma(j,3)} = 1 & j = 1, \ldots, q - m \\ z_s = a_s & s = l - m + 1, \ldots, l \end{cases}$$

where $\sigma(j, k) \in \{1, \ldots, l\}$ and $a_i \in \Gamma$. An algorithm is described in [RS95] which, for every $m \in \mathbb{N}$, assigns to each element $g \in \Gamma$ a word $\theta_m(g) \in F$ satisfying

$$\theta_m(g) = g \text{ in } \Gamma$$

called its *canonical representative*. In general, $\theta_m(g)$ does not satisfy any "canonical" properties. Useful properties are only satisfied for certain $m$ and certain finite subsets of $\Gamma$, as follows.

Let[1] $L = q \cdot 2^{5050(\delta+1)^6(2|A|)^{2\delta}}$. Suppose $\psi : Z \to \Gamma$ is a solution of $S(Z, A)$ and denote

$$\psi(z_{\sigma(j,k)}) = g_{\sigma(j,k)}.$$

Then there exist $h_k^{(j)}, c_k^{(j)} \in F(A)$ (for $j = 1, \ldots, q-m$ and $k = 1, 2, 3$) such that

(i) each $c_k^{(j)}$ has length less than[2] $L$ (as a word in $F$),

(ii) $c_1^{(j)} c_2^{(j)} c_3^{(j)} = 1$ in $\Gamma$,

(iii) there exists $m \leq L$ such that the canonical representatives satisfy the following equations in $F$:

$$\theta_m(g_{\sigma(j,1)}) = h_1^{(j)} c_1^{(j)} \left(h_2^{(j)}\right)^{-1} \tag{4.2}$$

$$\theta_m(g_{\sigma(j,2)}) = h_2^{(j)} c_2^{(j)} \left(h_3^{(j)}\right)^{-1} \tag{4.3}$$

$$\theta_m(g_{\sigma(j,3)}) = h_3^{(j)} c_3^{(j)} \left(h_1^{(j)}\right)^{-1}. \tag{4.4}$$

In particular, when $\sigma(j,k) = \sigma(j',k')$ (which corresponds to two occurrences in $S$ of the variable $z_{\sigma(j,k)}$) we have

$$h_k^{(j)} c_k^{(j)} \left(h_{k+1}^{(j)}\right)^{-1} = h_{k'}^{(j')} c_{k'}^{(j')} \left(h_{k'+1}^{(j')}\right)^{-1}. \tag{4.5}$$

---

[1] The constant of hyperbolicity $\delta$ may be computed from a presentation using the results of [EH01].

[2] The bound of $L$ here, and below, is extremely loose. Somewhat tighter, and more intuitive, bounds are given in [RS95].

Consequently, we construct the systems $S(X_i, A)$ as follows. For every positive integer $m \leq L$ and every choice of $3(q-m)$ elements $c_1^{(j)}, c_2^{(j)}, c_3^{(j)} \in F$ $(j = 1, \ldots, q-m)$ satisfying (i) and (ii)[3] we build a system $S(X_i, A)$ consisting of the equations

$$x_k^{(j)} c_k^{(j)} \left(x_{k+1}^{(j)}\right)^{-1} = x_{k'}^{(j')} c_{k'}^{(j')} \left(x_{k'+1}^{(j')}\right)^{-1} \tag{4.6}$$

$$x_k^{(j)} c_k^{(j)} \left(x_{k+1}^{(j)}\right)^{-1} = \theta_m(a_s) \tag{4.7}$$

where an equation of type (4.6) is included whenever $\sigma(j,k) = \sigma(j',k')$ and an equation of type (4.7) is included whenever $\sigma(j,k) = s \in \{l-m+1, \ldots, l\}$. To define $\rho_i$, set

$$\rho_i(z_s) = \begin{cases} x_k^{(j)} c_k^{(j)} \left(x_{k+1}^{(j)}\right)^{-1}, & 1 \leq s \leq l-m \text{ and } s = \sigma(j,k) \\ \theta_m(a_s), & l-m+1 \leq s \leq l \end{cases}$$

where for $1 \leq s \leq l-m$ any $j, k$ with $\sigma(j,k) = s$ may be used.

If $\psi : F(Z) \to \Gamma$ is any solution to $S(Z, A) = 1$, there is a system $S(X_i, A)$ such that $\theta_m(g_{\sigma(j,k)})$ satisfy (4.2)-(4.4). Then the required solution $\phi$ is given by

$$\phi\big(x_j^{(k)}\big) = h_j^{(k)}.$$

Indeed, (iii) implies that $\phi$ is a solution to $S(X_i, A) = 1$. For $s = \sigma(j,k) \in \{1, \ldots, l-m\}$,

$$z_s^{\rho_i \phi} = h_k^{(j)} c_k^{(j)} \left(h_{k+1}^{(j)}\right)^{-1} = \theta_m(g_{\sigma(j,k)})$$

and similarly for $s \in \{l-m+1, \ldots, l\}$, hence $\psi = \rho_i \phi \pi$.

[3] The word problem in hyperbolic groups is decidable.

Conversely, for any solution $\phi\big(x_j^{(k)}\big) = h_j^{(k)}$ of $S(X_i) = 1$ one sees that by (4.6),

$$z_{\sigma(j,1)} z_{\sigma(j,2)} z_{\sigma(j,3)} \overset{\rho_i\phi}{\longmapsto} h_1^{(j)} c_1^{(j)} c_2^{(j)} c_3^{(j)} \big(h_1^{(j)}\big)^{-1}$$

which maps to 1 under $\pi$ by (ii), hence $\rho_i\phi\pi$ induces a homomorphism. □

### 4.3.2 Encoding solutions with the tree $\mathcal{T}$

An algorithm is described in §5.6 of [KM05b] which constructs, for a given system of equations $S(X, A)$ over the free group $F$, a diagram encoding the set of solutions of $S$. The diagram consists of a directed finite rooted tree $T$ with the following properties. Let $G = F_{R(S)}$.

(i) Each vertex $v$ of $T$ is labelled by a pair $(G_v, Q_v)$ where $G_v$ is an $F$-quotient of $G$ and $Q_v$ a finitely generated subgroup of $\mathrm{Aut}_F(G_v)$. The root $v_0$ is labelled by $(G, 1)$ and every leaf is labelled by $(F(Y) * F, 1)$ where $Y$ is some finite set (called *free variables*). Each $G_v$, except possibly $G_{v_0}$, is fully residually $F$.

(ii) Every (directed) edge $v \to v'$ is labelled by a proper surjective $F$-homomorphism $\pi(v, v') : G_v \to G_{v'}$.

(iii) For every $\phi \in \mathrm{Hom}_F(G, F)$ there is a path $p = v_0 v_1 \dots v_k$ where $v_k$ is a leaf labelled by $(F(Y) * F, 1)$, elements $\sigma_i \in Q_{v_i}$, and a $F$-homomorphism $\phi_0 : F(Y) * F \to F$ such that

$$\phi = \pi(v_0, v_1)\sigma_1\pi(v_1, v_2)\sigma_2 \cdots \pi(v_{k-2}, v_{k-1})\sigma_{k-1}\pi(v_{k-1}, v_k)\phi_0. \tag{4.8}$$

The algorithm gives for each $G_v$ a finite presentation $\langle A_v|\mathcal{R}_v\rangle$, and for each $Q_v$ a finite list of generators in the form of functions $A_v \to (A_v \cup A_v^{-1})^*$. Note that the choices for $\phi_0$ are exactly parametrized by the set of functions from $Y$ to $F$.

Let $S(Z, A) = 1$ be a system of equations over $\Gamma$. We will construct the diagram $\mathcal{T}$ to encode the set of solutions of $S(Z, A) = 1$. Apply Lemma 4.3.2 to construct the systems $S_1(X_1, A), \ldots, S_n(X_n, A)$. Create a root vertex $v_0$ labelled by $F(Z, A)$. For each of the systems $S_i(X_i, A)$, let $T_i$ be the tree constructed above. Build an edge from $v_0$ to the root of $T_i$ labelled by the homomorphism $\rho_i\pi_{S_i}$, where $\pi_{S_i} : F(X_i, A) \to F_{R(S_i)}$ is the canonical projection. For each leaf $v$ of $T_i$, labelled by $F(Y) * F$, build a new vertex $w$ labelled by $F(Y) * \Gamma$ and an edge $v \to w$ labelled by the homomorphism $\pi_Y : F(Y) * F \to F(Y) * \Gamma$ which is induced from $\pi : F \to \Gamma$ by acting as the identity on $F(Y)$.

Define a *branch* $b$ of $\mathcal{T}$ to be a path $b = v_0v_1 \ldots v_k$ from the root $v_0$ to a leaf $v_k$. Let $v_1$ be labelled by $F_{R(S_i)}$ and $v_k$ by $F(Y) * \Gamma$. We associate to $b$ the set $\Phi_b$ consisting of all homomorphisms $F(Z) \to \Gamma$ of the form

$$\rho_i\pi_{S_i}\pi(v_1, v_2)\sigma_2 \cdots \pi(v_{k-2}, v_{k-1})\sigma_{k-1}\pi(v_{k-1}, v_k)\pi_Y\phi \tag{4.9}$$

where $\sigma_j \in Q_{v_j}$ and $\phi \in \mathrm{Hom}_\Gamma(F(Y) * \Gamma, \Gamma)$. Since $\mathrm{Hom}_\Gamma(F(Y) * \Gamma, \Gamma)$ is in bijective correspondence with the set of functions $\Gamma^Y$, all elements of $\Phi_b$ can be effectively constructed. We have thus obtained the following theorem.

**Theorem 4.3.3.** *There is an algorithm that, given a system $S(Z, A) = 1$ of equations over $\Gamma$, produces a diagram encoding its set of solutions. Specifically,*

$$\mathrm{Hom}(\Gamma_{R(S)}, \Gamma) = \{\overline{\phi} \mid \phi \in \Phi_b,\ b \text{ is a branch of } \mathcal{T}\}$$

*where $\mathcal{T}$ is the diagram described above. When the system is coefficient-free, then the diagram encodes* $\mathrm{Hom}(G, \Gamma)$ *where* $G = \langle Z \mid S \rangle$.

Let us remark here that in the diagram $\mathcal{T}$, the groups $G_v$ appearing at vertices are not quotients of coordinate group $\Gamma_{R(S)}$ and that one only obtains a homomorphism from $\Gamma_{R(S)}$ to $\Gamma$ by composing maps all the way down to the leaves of $\mathcal{T}$. D. Groves has shown, in [Gro05], that for any toral relatively hyperbolic group there exist Hom-diagrams with the property that every group $G_v$ is a quotient of $\Gamma_{R(S)}$ and that every edge map $\pi(v, v')$ is a proper surjective homomorphism. Our diagram $\mathcal{T}$ is not a Hom-diagram in this sense. The effective construction of these Hom-diagrams remains an interesting open problem (even for the case of torsion-free hyperbolic groups).

### 4.4 Embedding into extensions of centralizers

The proof given in [KM09] that $\Gamma$-limit groups embed into extensions of centralizers of $\Gamma$ involves two steps: first, any $\Gamma$-limit group is shown to embed into the coordinate groups of an *NTQ system* (see §4.4.1), and second, such groups are shown to embed into extensions of centralizers of $\Gamma$. The first step relies on the existence of so-called *shortening quotients* (see §5.3) for $\Gamma$-limit groups, which are the essential step in constructing Hom-diagrams over $\Gamma$. Shortening quotients were shown to exist in [Gro05], but their effective construction remains an open problem, and consequently the embedding of $\Gamma$-limit groups into extensions of centralizers of $\Gamma$ described in [KM09] is not effective.

However, in the case of free groups, the embedding of a limit group into the coordinate group of an NTQ system is effective [KM98b]. Our strategy is to reduce

to the free group case, construct embeddings into NTQ systems over free groups, and then 'convert' these into NTQ systems over $\Gamma$. First, we will need some background on quadratic equations and NTQ systems.

### 4.4.1 Quadratic equations and NTQ systems

An equation $s(X) \in G[X]$ over a group $G$ is said to be (strictly) *quadratic* if every variable appearing in $s$ appears at most (exactly) twice, and a system of equations $S(X) \subset G[X]$ is (strictly) quadratic if every variable that appears in $S$ appears at most (exactly) twice. Here we count both $x$ and $x^{-1}$ as an appearance of $x$. Constructing NTQ systems involves considerable analysis of quadratic equations, and is aided by considering certain standard forms.

**Definition 4.4.1.** A *standard quadratic equation* over a group $G$ is an equation of one of the following forms, where $c_i$ and $d$ are all nontrivial elements of $G$:

$$\prod_{i=1}^{n}[x_i, y_i] = 1, \quad n \geq 1; \tag{4.10}$$

$$\prod_{i=1}^{n}[x_i, y_i]\prod_{i=1}^{m} z_i^{-1}c_i z_i d = 1, \quad n, m \geq 0, n+m \geq 1; \tag{4.11}$$

$$\prod_{i=1}^{n} x_i^2 = 1, \quad n \geq 1; \tag{4.12}$$

$$\prod_{i=1}^{n} x_i^2 \prod_{i=1}^{m} z_i^{-1}c_i z_i d = 1, \quad n, m \geq 0, n+m \geq 1. \tag{4.13}$$

The left-hand sides of the above equations are the *standard quadratic words*. □

The following result allows us to assume that quadratic equations always appear in standard form.

**Lemma 4.4.2.** *Let $s(X) \in G[X]$ be a strictly quadratic word over a group $G$. Then there is a $G$-automorphism $\phi$ such that $s^\phi$ is a standard quadratic word over $G$.*

*Proof.* Follows easily from §I.7 of [LS77]. □

To each quadratic equation we associate a punctured surface. To (4.10) we associate the orientable surface of genus $n$ and zero punctures, to (4.11) the orientable surface of genus $n$ with $m+1$ punctures, to (4.12) the non-orientable surface of genus $n$, and to (4.13) the non-orientable surface of genus $n$ with $m+1$ punctures. For a standard quadratic equation $S$, denote by $\chi(S)$ the Euler characteristic of the corresponding surface.

Quadratic words of the form $[x, y]$, $x^2$, and $z^{-1}cz$ where $c \in G$, are called *atomic quadratic words* or simply *atoms*. An atom $[x, y]$ contributes $-2$ to the Euler characteristic of $S$ while $x^2$ and $z^{-1}cz$ (as well as $d$) each contribute $-1$. A standard quadratic equation $S = 1$ over $G$ has the form

$$r_1 r_2 \dots r_k d = 1,$$

where $r_i$ are atoms and $d \in G$. We classify solutions to quadratic equations based on the extent to which the images of the atoms commute, as follows.

**Definition 4.4.3.** Let $S = 1$ be a standard quadratic equation written in the atomic form $r_1 r_2 \dots r_k d = 1$ with $k \geq 2$. A solution $\phi : G_{R(S)} \to G$ of $S = 1$ is called

(i) *degenerate*, if $r_i^\phi = 1$ for some $i$, and *non-degenerate* otherwise;

(ii) *commutative*, if $[r_i^\phi, r_{i+1}^\phi] = 1$ for all $i = 1, \dots, k-1$, and *non-commutative* otherwise;

(iii) in *general position*, if $[r_i^\phi, r_{i+1}^\phi] \neq 1$ for all $i = 1, \dots, k-1$,.

□

When the group $G$ is commutation transitive, a commutative solution satisfies $[r_i^\phi, r_j^\phi] = 1$ for all $i, j$. We will only be interested in the case when $G$ is toral relatively hyperbolic, hence commutation transitive (recall §2.3). In this case, solutions also have the following important property.

**Lemma 4.4.4.** *Let $S \in G[X]$ be a non-degenerate standard quadratic equation over a toral relatively hyperbolic group $G$ such that $S$ has at least two atoms. Then either*

*(1) $S$ has a solution in general position, or*

*(2) every solution of $S$ is commutative.*

*Further, there is an algorithm that distinguishes the cases.*

*Proof.* The dichotomy is true for all CSA groups, by Proposition 3 of [KM98a]. For the algorithm, let $S$ has the atomic form $r_1 r_2 \dots r_k d$ with variables $x_1, \dots, x_n$. Consider the sentences

$$\mathcal{S}_i : \exists x_1 \dots \exists x_n \ (S = 1) \wedge ([r_i, r_{i+1}] \neq 1)$$

for $i = 1, \dots, k-1$. Then all solutions of $S = 1$ are commutative if and only if none of the sentences $\mathcal{S}_i$ is true in $G$. Since every parabolic subgroup of $G$ is a free abelian group, and such groups have decidable existential theory. Then it follows from [Dah09] that $G$ has decidable existential theory, hence we can decide whether or not each $\mathcal{S}_i$ is true in $G$. □

Now we define NTQ systems. Let $G$ be a group generated by $A$ and let $S(X, A)$ be a system of equations and suppose $S$ can be partitioned into subsystems

$$\begin{aligned} S_1(X_1, X_2, \ldots, X_n, A) &= 1, \\ S_2(X_2, \ldots, X_n, A) &= 1, \\ &\ldots \\ S_n(X_n, A) &= 1 \end{aligned}$$

where $\{X_1, X_2, \ldots, X_n\}$ is a partition of $X$. Define groups $G_i$ for $i = 1, \ldots, n+1$ by

$$\begin{aligned} G_{n+1} &= G \\ G_i &= G_{R(S_i, \ldots, S_n)}. \end{aligned}$$

We interpret $S_i$ as a subset of $G_{i-1} * F(X_i)$, i.e. letters from $X_i$ are considered variables and letters from $X_{i+1} \cup \ldots \cup X_n \cup A$ are considered as constants from $G_i$. A system $S(X, A) = 1$ is called *triangular quasi-quadratic* (TQ) if it can be partitioned as above such that for each $i$ one of the following holds:

(I) $S_i$ is quadratic in variables $X_i$;

(II) $S_i = \{[x, y] = 1,\ [x, u] = 1 \mid x,\ y \in X_i,\ u \in U_i\}$ where $U_i$ is a finite subset of $G_{i+1}$ such that $\langle U_i \rangle = C_{G_{i+1}}(g)$ for some $g \in G_{i+1}$;

(III) $S_i = \{[x, y] = 1 \mid x,\ y \in X_i\}$;

(IV) $S_i$ is empty.

The system is called *non-degenerate triangular quasi-quadratic* (NTQ) is for every $i$ the system $S_i(X_i, \ldots, X_n, A)$ has a solution in the coordinate group $G_{R(S_{i+1}, \ldots, S_n)}$.

**Definition 4.4.5.** A group $H$ is called a *G-NTQ group* if there is a NTQ system $S$ over $G$ such that $H \simeq G_{R(S)}$. $\square$

For any quadratic system $S$ over $G$ one can, by eliminating linear variables, find a strictly quadratic system $S'$ over $G$ such that every variable occurs in exactly one equation and $G_S \simeq G_{S'}$. Consequently, if $H$ is an NTQ group with $H \simeq G_{R(S)}$ then we may assume that every system $S_i$ of $S$ that has the form (I) consists of a single quadratic equation in standard form.

In order to study NTQ groups by induction on the height $n$ of the NTQ system, we will need the following lemma.

**Lemma 4.4.6.** *Let $S(X, A)$ and $T(Y, A)$ be systems of equations over a group $G$ with $X \cap Y = \emptyset$ and let $G_1 = G[X]/R_G(S)$. Then*

$$G_{R(S \cup T)} \simeq G_1[Y]/R_{G_1}(T).$$

*Proof.* Let $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_m\}$, $u = u(x_1, \ldots, x_n, y_1, \ldots, y_m) \in G[X \cup Y]$. We will show that the natural map, which sends $u$ to the element represented by $u$ in $G_1[Y]/R_{G_1}(T)$, is an isomorphism.

To see that the map is well-defined, suppose $u \in R_G(S \cup T)$. It suffices to show that $u \in R_{G_1}(T)$. Let $\varphi : Y \to G_1$ be any solution of $T$ over $G_1$ and denote $y_j^{\varphi} = w_j(x_1, \ldots, x_n)$. We need to show that $u^{\varphi} = 1$ in $G_1$, i.e. $u^{\varphi} \in R_G(S)$. Let $\psi : X \to G$ be any solution of $S$ over $G$, and denote $x_i^{\psi} = g_i$. Consider the map $\alpha : X \cup Y \to G$ defined by

$$\begin{aligned} x_i &\to g_i, \\ y_j &\to w_j(g_1, \ldots, g_n), \end{aligned}$$

for $i = 1, \ldots, n$ and $j = 1, \ldots, m$. The map $\alpha$ is a solution to $S \cup T$. Indeed, if $s \in S$ then $s^\alpha = s^\psi$, and $\psi$ is a solution to $S$ so $s^\psi = 1$. If $t \in T$ then

$$t^\alpha = t(w_1(g_1, \ldots, g_n), \ldots, w_m(g_1, \ldots, g_n)) = (t^\varphi)^\psi .$$

Since $\varphi$ is a solution to $T$ over $G_1$, we have that $t^\varphi \in R_G(S)$ and since $\psi$ is a solution to $S$ over $G$ we have that $(t^\varphi)^\psi = 1$ in $G$, proving that $\alpha$ is a solution to $S \cup T$. Since $u \in R_G(S \cup T)$, $u^\alpha = 1$ hence

$$1 = u^\alpha = (u^\varphi)^\psi$$

so $u^\varphi \in R_G(S)$ as required.

The fact that the natural map is surjective is trivial, so it remains to prove injectivity. Let $u \in G[X \cup Y]$ with $u \notin R_G(S \cup T)$. We must show that $u \notin R_{G_1}(T)$. Since $u \notin R_G(S \cup T)$, there exists a solution $\alpha : X \cup Y \to G$ of $S \cup T$ such that $u^\alpha \neq 1$. The restriction $\alpha|_Y$ of $\alpha$ to $Y$ is a solution to $T$ over $G_1$. Indeed, if $t \in T$ then variables of $X$ do not occur in $t$, so

$$t^{\alpha|_Y} = t^\alpha = 1$$

in $G$, hence $t^{\alpha|_Y} = 1$ in $G_1$ as well. Since $\alpha|_X$ is a solution to $S$ over $G$ and

$$\left(u^{\alpha|_Y}\right)^{\alpha|_X} = u^\alpha \neq 1$$

we conclude that $u^{\alpha|_Y}$ is non-trivial in $G_1$ hence $u$ is not in $R_{G_1}(T)$, as required. $\square$

It follows from the lemma that for every $i = 1, \ldots, n$,

$$G_i \simeq G_{i+1}[X_i]/R_{G_{i+1}}(S_i). \tag{4.14}$$

Note that this isomorphism holds for any system of equations that can be partitioned in triangular form, not just for NTQ systems. It is essential to observe that when $R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i)$, $G_i$ admits the presentation

$$G_i = \langle G_{i+1},\ X_i \,|\, S_i \rangle.$$

In this case, $G_i$ has a graph of groups decomposition of one of the following four types, according to the form of $S_i$:

(I) as a graph of groups with vertices $v_1$, $v_2$ where $G_{v_1} = G_{i-1}$ and $G_{v_2}$ is a QH-subgroup;

(II) as a graph of groups with vertices $v_1$, $v_2$ where $G_{v_1} = G_{i-1}$, $G_{v_2}$ is a free abelian group of rank $m$ and the edge groups generate a maximal abelian subgroup of $G_{v_1}$ ('rank $m$ extension of centralizer');

(III) as a free product with a finite rank free abelian group;

(IV) as a free product with a finitely generated free group.

A frequently used method of proving that $R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i)$ is the following well-known fact.

**Lemma 4.4.7.** *Let $S(X)$ be a system of equations over a group $G$. If $G_S$ is residually $G$, then $R_G(S) = \mathrm{ncl}_G(S)$. In particular,*

$$G_{R(S)} = G_S.$$

*Proof.* It is always the case that $\mathrm{ncl}_G(S) \subset R_G(S)$, so assume for contradiction that there exists $w \in R_G(S) \backslash \mathrm{ncl}_G(S)$. Then $w \neq 1$ in $G_S$, so there exists a homomorphism $\phi : G_S \to G$ such that $w^\phi \neq 1$. But $\phi$ is a solution to $S$ and $w \in R_G(S)$ so $w^\phi = 1$. $\square$

For NTQ systems over toral relatively hyperbolic groups, [KM09] has shown that the condition $R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i)$ holds except in some exceptional cases. We recall the relevant definitions from [KM09].

**Definition 4.4.8.** A standard quadratic equation $S = 1$ over a group $G$ is said to be *regular* if either $\chi(S) \leq -2$ and $S$ has a non-commutative solution over $G$, or $S = 1$ is an equation of the form $[x, y]d = 1$ or $[x_1, y_1][x_2, y_2] = 1$. An NTQ system is called *regular* if every quadratic equation appearing in case (I) is regular. □

**Proposition 4.4.9** ([KM09])**.** *Let $G$ be a toral relatively hyperbolic group and $S = S_1 \cup \ldots \cup S_n$ a regular NTQ system over $G$. Then for all $i = 1, \ldots, n$,*

$$R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i).$$

The condition $R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i)$ allows us to use the graph of groups decomposition of $G_i$ to derive properties of NTQ groups inductively. In particular, we have the following.

**Lemma 4.4.10.** *Let $\Gamma = \langle A|\mathcal{R}\rangle$ be a toral relatively hyperbolic group and $G$ a $\Gamma$-NTQ group such that $R_{G_{i+1}}(S_i) = \mathrm{ncl}_{G_{i+1}}(S_i)$ for all $i = 1, \ldots, n$. Then $G$ is toral relatively hyperbolic and fully residually $\Gamma$.*

*Proof.* The second statement is proved in [KM09]. For the first, we proceed by induction on the height of the NTQ system. The base $\Gamma$ is toral relatively hyperbolic. Now assume that $G_{n-1}$ is toral relatively hyperoblic. We will show that $G_n$ is toral relatively hyperbolic by applying Theorem 0.1 of [Dah03] ('Combination theorerm') to the four possible decompositions of $G_i$ described above.

Cases (IV) and (III) follow from Theorem 0.1 parts (3) and (2), respectively, by amalgamating over the trivial subgroup. Note that to use Theorem 0.1 (2) we need the fact that if $G$ is hyperbolic relative to the collection of subgroups $\mathcal{H}$ then it is also hyperbolic relative to $\mathcal{H} \cup \{1\}$. Case (II) follows from Theorem 0.1 (2) by amalgamating over $P = \langle U_i \rangle$, which is maximal abelian in $G_{i-1}$.

For case (I), consider first the case when the surface corresponding to the quadratic equation has punctures. In this case we form $G_i$ by amalgamating $G_{i-1}$ with a free group over a $\mathbb{Z}$ subgroup, followed HNN-extensions over $\mathbb{Z}$ subgroups. It follows from the results of [Osi06b] that these $\mathbb{Z}$ subgroups are maximal parabolic subgroups, hence we may apply Theorem 0.1 (3), (3'). □

**Remark 4.4.11.** From the Combination Theorem it follows that $G$ has finitely many maximal non-cyclic abelian subgroups up to conjugation, and we can construct, by induction, the list of them along with a finite generating set for each. In the base group $\Gamma$ this is possible using the results of [Dah08].

NTQ groups over free groups played a central role in the solution to Tarski's problems by Kharlampovich-Miasnikov and Sela. In Sela's work, they are called *$\omega$-residually free towers* [Sel01].

### 4.4.2 Embedding into extensions of centralizers

Let $G = \langle Z \mid S \rangle$ be a finitely presented fully residually $\Gamma$ group. We consider $S$ as a (coefficient-free) system of equations over $\Gamma$. The results of this section also hold in the category of $\Gamma$-groups, i.e. when $G = \langle Z, A \mid S(Z, A),\ \mathcal{R} \rangle$ is fully residually $\Gamma$. Recall that $\Gamma$ is presented by $\langle A | \mathcal{R} \rangle$.

For a system of equations over free groups, Kharlampovich and Miasnikov proved that every solution factors through one of finitely many NTQ groups, which can be effectively constructed.

**Proposition 4.4.12.** *[KM98b] There is an algorithm that, given a system of equations $T(X, A) = 1$ over a free group, produces finitely many $F$-NTQ systems*

$$T_1(X_1, A) = 1, T_2(X_2, A) = 1, \ldots, T_n(X_n, A) = 1$$

*and homomorphisms*

$$\mu_i : F(X) \to F_{R(T_i)}$$

*such that for every homomorphism $\psi : F_{R(T)} \to F$ there is an integer $i$ and a homomorphism $\phi : F_{R(T_i)} \to F$ such that*

$$\psi = \mu_i \phi.$$

Given this result, we may assume that the systems $S_1(X_1, A), \ldots, S_n(X_n, A)$ constructed in Lemma 4.3.2 are in fact NTQ systems. For each of these systems $S_i$ we consider the system $S_i^\pi$ over $\Gamma$. In the following lemma, we construct homomorphisms from $G$ to the coordinate groups $\Gamma_{R(S_i)}$, one of which must be an embedding. However, the systems $S_i^\pi$ need not be NTQ systems over $\Gamma$. Properties (I), (III), and (IV) of NTQ systems as well as non-degeneracy, but property (II) need not hold since $U_i^\pi$ might not generate a complete centralizer.

**Lemma 4.4.13.** *There is an algorithm that, given a finitely presented group $G = \langle Z \,|\, S \rangle$, produces*

*(i) finitely many $F$-NTQ systems $S_1(X_1, A), \ldots, S_m(X_m, A)$, and*

*(ii) homomorphisms* $\alpha_i : G \to \Gamma_{R(S_i)}$

*such that*

*(1) if* $G$ *is fully residually* $\Gamma$*, then there exists* $i \in \{1, \ldots, m\}$ *such that* $\alpha_i$ *is injective, and*

*(2) if* $G$ *is residually* $\Gamma$*, then for every* $g \in G$ *there exists* $i \in \{1, \ldots, m\}$ *such that* $g^{\alpha_i} \neq 1$.

*Proof.* Refer to Figure 4–1 for a diagram of the maps constructed in this proof. Construct the $F$-NTQ systems $S_1(X_1, A), \ldots, S_n(X_n, A)$ and the homomorphisms

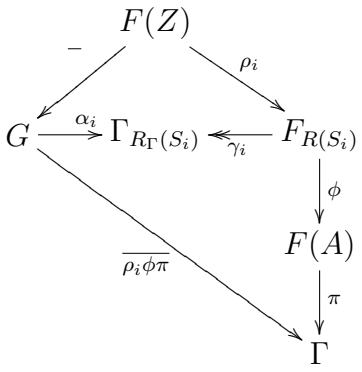


Figure 4–1: Commutative diagram for Lemma 4.4.13.

$\rho_i : F(Z) \to F_{R(S_i)}$ from Lemma 4.3.2. Let $\gamma_i : F_{R(S_i)} \to \Gamma_{R(S_i)}$ be the canonical epimorphism and set $\alpha_i = \overline{\rho_i \gamma_i}$. That is, for any $\overline{u} \in G$,

$$\overline{u}^{\alpha_i} = u^{\rho_i \gamma_i}.$$

Since $\rho_i$ is given as a word mapping, so is $\alpha_i$.

To check that $\alpha_i$ is well-defined, let $u \in F(Z)$ with $\overline{u} = 1$ (in $G$). Since $u \in \mathrm{ncl}_{F(Z)}(S)$, there exist $s_j \in S$ and $w_j \in F(Z)$ such that $u = \prod_{j=1}^{n} s_j^{w_j}$ hence

$$u^{\rho_i\gamma_i} = \prod_{j=1}^{m} (s_j^{\rho_i\gamma_i})^{w_j^{\rho_i\gamma_i}}.$$

Recall from the description of canonical representatives in Lemma 4.3.2 that $s_j$ has the form $s_j = z_1 z_2 z_3$ and hence $s_j^{\rho_i}$ has the form

$$s_j^{\rho_i} = (x_1 c_1 x_2^{-1})(x_2 c_2 x_3^{-1})(x_3 c_3 x_1^{-1})$$

where $c_1 c_2 c_3 = 1$ in $\Gamma$ and $x_1, x_2, x_3 \in X_i$. Hence

$$s_j^{\rho_i} = (c_1 c_2 c_3)^{x_1}.$$

Since the relators of $\Gamma$ are elements of $R_\Gamma(S_i)$ we have that $s_j^{\rho_i\gamma_i} = 1$ in $\Gamma_{R(S_i)}$ hence $u^{\rho_i\gamma_i} = 1$ and $\alpha_i$ is well-defined.

Suppose now that $G$ is fully residually $\Gamma$. For each $i \in \{1, \ldots, n\}$ set

$$\Phi_i = \{\overline{\rho_i \phi \pi} \mid \phi \in \mathrm{Hom}(F_{R(S_i)}, F)\}.$$

From Lemma 4.3.2 we know that

$$\mathrm{Hom}(G, \Gamma) = \bigcup_{i=1}^{n} \Phi_i.$$

Since $G$ is fully residually $\Gamma$, there exists $i$ such that $\Phi_i$ is a discriminating family of homomorphisms. Indeed, if no $\Phi_i$ discriminates $G$, then for each $i$ there is a finite subset $W_i \leq G$ such that every $\phi \in \Phi_i$ is not injective on $W_i$. Then $\bigcup_{i=1}^{m} W_i$ is a finite subset that is not discriminated by $\bigcup_{i=1}^{m} \Phi_i$.

Let $i$ be such that $\Phi_i$ is a discriminating family and let $\overline{u}$ be any non-trivial element of $G$. Then there exists $\overline{\rho_i\phi\pi} \in \Phi_i$ with $u^{\rho_i\phi\pi} \neq 1$. The homomorphism $\phi\pi : F_{R(S_i)} \to \Gamma$ is a solution to $S_i$ over $\Gamma$. Since $(u^{\rho_i})^{\phi\pi} \neq 1$, $u^{\rho_i}$ is not in $R_\Gamma(S_i)$. Hence

$$\overline{u}^{\alpha_i} = (u^{\rho_i})^{\gamma_i} \neq 1$$

so $\alpha_i$ is injective.

Now suppose that $G$ is residually $\Gamma$ and let $\overline{u} \in G$. Since $\mathrm{Hom}(G, \Gamma) = \bigcup_{i=1}^{n} \Phi_i$, there exists $i$ and $\overline{\rho_i\phi\pi} \in \Phi_i$ such that $u^{\rho_i\phi\pi} \neq 1$. As above, this implies $\overline{u}^{\alpha_i} \neq 1$. □

**Remark 4.4.14.** Though at least one of the homomorphisms $\alpha_i$ must be injective, we are not aware of a method for determining which one (there may be several). We will comment on this further in Chapter 5.

Our objective now is to construct an effective embedding of each coordinate group $\Gamma_{R(S_i)}$ into a group obtained from $\Gamma$ by a series of extensions of centralizers. We will need the following lemma in order to argue by induction.

**Lemma 4.4.15.** *Let $H \leq G$ be any torsion-free groups and let $S$ be a system of equations over $H$ such that $S$ has one of the NTQ forms (I)–(IV). Then the canonical homomorphism $H_S \to G_S$ is an embedding.*

*Proof.* The case when $S$ is a standard quadratic equation is Proposition 2 of [KM98a], the case when $S$ is an extension of a centralizer follows immediately from the theory of normal forms for HNN-extensions, and the cases of a free product with a free group or free abelian group are obvious. □

**Lemma 4.4.16.** *Let $\Gamma = \langle A|\mathcal{R}\rangle$ a finitely presented torsion-free hyperbolic group. There exists an algorithm that, given an NTQ system $S(X, A)$ over the free group $F$, constructs a group $H$ obtained from $\Gamma$ by a series of extensions of centralizers and an embedding*

$$\beta : \Gamma_{R(S)} \hookrightarrow H.$$

*Further, both groups $\Gamma_{R(S)}$ and $H$ are toral relatively hyperbolic and a generating set for any maximal abelian subgroup can be effectively constructed.*

*Proof.* Let $S(X, A)$ be partitioned as an NTQ system as $S_1, \ldots, S_n$. Consider $S$ as a system of equations over $\Gamma$, with $G_{n+1} = \Gamma$ and

$$G_i = G_{i+1}[X_i]/R_{G_{i+1}}(S_i).$$

Note that $\Gamma_{R(S)} = G_1$.

We proceed by induction on $n$. For the base case $n = 0$ there are no equations or variables in $S$ so $\Gamma_{R(S)} = \Gamma$ so we may take $H = \Gamma$ and $\beta$ the identity. Now assume the theorem holds up to $n-1$. That is, assume we have constructed a group $H'$ obtained by extensions of centralizers of $\Gamma$ and as an embedding $\beta' : G_2 \to H'$. We argue based of the form (I)–(IV) of the system of equations $S_1(X_1, A)$. In the following we will frequently use without mention Lemma 4.4.7 to obtain a presentation of $G_1$, and Lemma 4.4.10 and Remark 4.4.11 to show that $G_1$ is toral relatively hyperbolic with a finite collection of maximal abelian subgroups (up to conjugation), generating sets of which can be effectively constructed.

**Form (IV): Free product with a free group**. Suppose $S_1$ has the form (IV), that is, $S_1$ is empty. We will show that the group $\langle G_2, X_1 \,|\, -\rangle \simeq G_2 * F(X_1)$ embeds

in a group obtained from $G_2$ by extensions of centralizers . It will suffice to consider the case of two variables, $X_1 = \{x, y\}$. Let $u, v \in G_2$ such that $C(u) \cap C(v) = 1$, and consider the sequence of extensions of centralizers

$$\begin{aligned} G_2' &= \langle G_2, t \,|\, [C_{G_2}(u), t] \rangle, \\ G_2'' &= \langle G_2', s \,|\, [C_{G_2'}(v), s] \rangle, \\ G_2''' &= \langle G_2'', r \,|\, [C_{G_2''}(ust), r] \rangle. \end{aligned}$$

One checks that $C_{G_2'}(v) = C_{G_2}(v)$, that $t$ and $s$ generate a rank two free group in $G_2'''$, that $C_{G_2''}(ust) \cap G_2 = 1$, and that $C_{G_2''}(ust) \cap \langle t, s \rangle = 1$. Define $\phi : G_2 * F(x, y) \to G_2'''$ by $x^\phi = t^r$, $y^\phi = s^r$, and $g^\phi = g$ for $g \in G_2$. A non-trivial element $w \in G_2 * F(x, y)$ has reduced form

$$w = g_1 w_1(x, y) g_2 w_2(x, y) \dots g_m w_m(x, y) g_{m+1}$$

and is sent under $\phi$ to

$$w^\phi = g_1 r^{-1} w_1(t, s) r g_2 r^{-1} w_2(t, s) r \dots g_m r^{-1} w_m(t, s) r g_{m+1}.$$

This word has no reduction of the form $r g_i r^{-1} \to g_i$, since $C_{G_2''}(ust) \cap G_2 = 1$, and no reduction of the form $r^{-1} w_i(t, s) r \to w_i(t, s)$, since $C_{G_2''}(ust) \cap \langle t, s \rangle = 1$ and $\langle t, s \rangle$ is free of rank two. Hence $w^\phi$ is reduced and therefore non-trivial by Britton's Lemma, so $\phi$ is injective.

We conclude that $\langle G_2, X_1 \,|\, - \rangle$ is residually $G_2$, hence $G_1 = G_1 * F(x, y)$ and $G_1$ is toral relatively hyperbolic. By Lemma 4.4.15, $G_1$ embeds canonically in $H' * F(x, y)$. Repeating the construction above with $H'$ in place of $G_2$ we may construct

an embedding of $H' * F(x, y)$ into a group $H$ obtained by extensions of centralizers from $H'$.

**Form (III): Free product with a free abelian group**. Suppose $S_1$ has the form (III). First, suppose that $|X_1| = 2$, and so $\langle G_2, X_1 \,|\, S_1\rangle \simeq G_2 * \mathbb{Z}^2$. Lemma 16 of [KM98a] shows that $G_2 * \mathbb{Z}^2$ embeds in every non-trivial extension extension of a centralizer of $G_2$. Consequently, $G_2 * \mathbb{Z}^2$ is residually $G_2$ so $G_1 \simeq G_2 * \mathbb{Z}^2$ and is toral relatively hyperbolic.

From Lemma 4.4.15, $G_1$ embeds canonically in $H' * \mathbb{Z}^2$. Apply Lemma 16 of [KM98a] again to embed $H' * \mathbb{Z}^2$ in in an extension of centralizers $H$ of $H'$. It follows immediately from the proof that the embedding is effective, provided we can produce two non-commuting elements of $H'$. This is possible by Lemma 2.3.6 since $H'$ is toral relatively hyperbolic.

If $|X_1| > 2$, we partition $S_1$ into two subsystems

$$\begin{aligned} S_{1,a} &= \{[x_i, x_j] = 1, [x_i, u] = 1, \mid i, j \in \{3, \ldots, m\}, u \in U_{1,a}\} \\ S_{1,b} &= \{[x_1, x_2] = 1\} \end{aligned}$$

where $X_1 = \{x_1, \ldots, x_n\}$ and $U_{1,a} = \{x_1, x_2\}$. The system $S_{1,b}$ has the form (III) with two variables, which we have dealt with above, and $S_{1,a}$ is an extension of the centralizer $C_{G_{1,b}}(x_1) = \langle x_1, x_2\rangle$ in $G_{1,b} \simeq G_2 * \langle x_1, x_2\rangle$, which we deal with in form (II) below.

**Form (II): Extension of a centralizer**. Suppose $S_1$ has the form (II). If $U_1$ generates the trivial subgroup in $G_2$, which we may check since the word problem in $G_2$ is decidable, then we have the form (III) and we may argue as above.

Otherwise, let $U'$ be the centralizer of $U_1$ in $G_2$. In general, $\langle U_1 \rangle$ is a proper subgroup of $U'$. We must construct a generating set $u_1, \ldots, u_m$ for $U'$. By induction, $G_2$ has, up to conjugation, finitely many parabolic (i.e. abelian of rank at least two) subgroups $P_1, \ldots, P_l$ and we have constructed a generating set for each one. The centralizer $U'$ is a maximal abelian subgroup of $G_2$, hence is either conjugate to one of the $P_i$ or is cyclic.

It follows from [Bum04] and the fact that conjugacy in the abelian groups $P_i$ is decidable (see also Theorem 5.6 of [Osi06b]), that for any element $g \in G_2$ and parabolic subgroup $P_i$ we can decide whether or not $g$ is conjugate to an element of $P_i$, and if so find a conjugating element. Applying this to any non-trivial element $g$ of $U_1$, we either identify $U'$ as a conjugate of one of the $P_i$ and construct a generating set by conjugating the generating set of $P_i$, or we determine that $U'$ is in fact cyclic and we find a generator using Lemma 2.3.6.

Now consider the system of equations

$$S_1' = \{[x, u_i], [x, y] \mid x, y \in X_1,\ i \in \{1, \ldots, m\}\}$$

over $G_2$. Since $G_2$ is commutation-transitive, we know that if $\phi : X_1 \to G_2$ is any solution to the system $S_1$ then $[x^\phi, u_i] = 1$ for all $x \in X_1$ and $i = 1, \ldots, m$. Consequently, $[x, u_i] \in R_{G_2}(S_1)$ for all $x \in X_1$ and $i = 1, \ldots, m$ so $S_1' \subset R_{G_2}(S_1)$. The group $\langle G_2, X \mid S_1' \rangle$ is an extension of a centralizer of $G_2$, so by Proposition 3.2.1 is residually $G_2$. Then by Lemma 4.4.7,

$$R_{G_2}(S_1) = R_{G_1}(S_1') = \mathrm{ncl}_{G_2}(S_1')$$

hence $G_1 = \langle G_2,\ X_1 \,|\, S_1' \rangle$ and is toral relatively hyperbolic.

We need to show that $G_1$ embeds in an extension of centralizer of $H'$. By induction, we may construct a finite generating set $v_1, \ldots, v_l$ for the maximal abelian subgroup of $H'$ that contains $U'$. Consider the system of equations

$$T = \{[x, v_i], [x, y] \mid x, y \in X_1,\ i \in \{1, \ldots, l\}\}.$$

and the group $H = \langle H', X_1 \,|\, T \rangle$, which is an extension of centralizer of $H'$.

Define the map $\beta : G_1 \to H$ by $x^\beta = x$ for $x \in X_1$ and $g^\beta = g^{\beta'}$ for $g \in G_2$. One easily checks that $\beta$ is a (well-defined) homomorphism. To show that $\beta$ is injective, let $w \in G_1$ be non-trivial. Since $G_1$ is residually $G_2$, there is a function $\phi : X_1 \to G_2$ which is a solution to $S_1'$ and such that $w^\phi$ is a non-trivial element of $G_2$. We claim that $\phi\beta' : X_1 \to H'$ is a solution to $T$. For $x, y \in X_1$ we have

$$[x^{\phi\beta'}, y^{\phi\beta'}] = [x^\phi, y^\phi]^{\beta'} = 1^{\beta'} = 1.$$

For $x \in X$ and any $u_i$ we have that

$$[x^{\phi\beta'}, u_i^{\beta'}] = [x^\phi, u_i]^{\beta'} = 1^{\beta'} = 1$$

so by commutation-transitivity $[x^{\phi\beta'}, v_j] = 1$ for all $j$. Hence $\phi\beta'$ is a solution as required, and induces a homomorphism $\phi\beta' : G_1 \to H'$. The image of $w^\beta$ under this homomorphism is

$$(w^\beta)^{\phi\beta'} = w^{\phi\beta'}$$

and is non-trivial since $w^\phi \neq 1$ and $\beta'$ is injective. Consequently, $w^\beta \neq 1$ in $H$ as required.

**Form (I): Quadratic equation**. Suppose that $S_1$ is a quadratic equation. Then $S_1$ has one of the standard forms (4.10)–(4.13). The words $c_i$ and $d$ in the standard form are non-trivial in $F_{R(S_2 \cup \ldots \cup S_n)}$, but may be trivial in $G_2$. We can check which are trivial by solving the word problem in $G_2$. Form an equation $S_{1,a}$ by

(i) erasing from $S_1$ each atom $c_i^{z_i}$ such that $c_i = 1$ in $G_2$, and

(ii) if $d = 1$ in $G_2$, by erasing $d$ and replacing the rightmost atom of the form $c_i^{z_i}$ by $c_i$.

Let $Z$ be the set of variables of $X_1$ not appearing in $S_{1,a}$ (i.e. the $z_i$ from the erased atoms, as well as the rightmost $z_i$ if $d = 1$). Partition $X$ into $X \setminus Z$ and $Z$. The system of equations $S_1(X_1, A)$ is equivalent over $G_2$ to the union of the systems $S_{1,b} = \emptyset$ in variables $Z$ and $S_{1,a}$ in variables $X_1 \setminus Z$, so we replace $S_1(X_1, A)$ with these two systems and apply case (IV) to $S_{1,b}$.

The equation $S_{1,a}$ is a quadratic equation in standard form over $G_2$. To simplify notation, we rename $S_{1,a}$ to $S_1$ and $X_1 \setminus Z$ to $X_1$. We study cases based on the Euler characteristic $\chi(S_1)$ of the surface associated with $S_1$.

**Case $\chi(\mathbf{S_1}) \leq -\mathbf{2}$.** Assume that $\chi(S_1) \leq -2$. First, check using Lemma 4.4.4 whether or not $S_1$ has a solution in general position over $G_2$. If so, then $S_1$ is regular. Whenever $S_1$ is regular and $G_2$ is toral relatively hyperbolic, Theorem 4.1 of [KM09] proves that the group $\langle G_2, X_1 \,|\, S_1 \rangle$ embeds into a group $H$ obtained from $G_2$ by a series of extensions of centralizers. Consequently, this group is residually $G_2$ hence $G_1 = \langle G_2, X_1 \,|\, S_1 \rangle$ and $G_1$ is toral relatively hyperbolic. Embed $G_1$ canonically into $\langle H', X_1 \,|\, S_1 \rangle$, using Lemma 4.4.15.

The equation $S_1$ is regular over $H'$, and $H'$ is toral relatively hyperbolic, so again applying Theorem 4.1 of [KM09] we obtain that $\langle H', X_1 \,|\, S_1 \rangle$ embeds into a group obtained from $H'$ by a sequence of extensions of centralizers. It suffices to show that this embedding is effective. The reader may verify that in order to obtain an effective embedding from the proof given in [KM09], one must be able to solve the following three problems: (a) solve the word problem in $H'$, (b) decide whether or not an quadratic equation over $H'$ has a non-commutative solution, and (c) find such a solution. We can solve (a) by Lemma 2.3.6 since $H'$ is toral relatively hyperbolic, (b) by Lemma 4.4.4, and (c) by enumerating all possible solutions until we find a non-commutative one.

Now suppose that $S_1$ does not have a solution in general position over $G_2$. By Lemma 4.4.4, all solutions are commutative. We consider cases based on the from of $S_1$.

*Orientable forms.* Suppose $S_1$ contains a commutator. If $S_1 = [x_1, y_1][x_2, y_2]$, then $S_1$ is regular by definition and we may proceed as above. Otherwise, by Proposition 4.3 of [KM09], $S_1$ has a solution in general position in a group $K$ obtained from $G_2 * F$, where $F$ is a finite-rank free group, by a series of centralizer extensions. Since $K$ is discriminated by $G_2$ (see form (IV)), it follows that $S_1$ has a solution in general position in $G_2$, which contradicts the fact that all solutions are commutative.

*Genus zero forms.* Suppose that $S_1$ has the form

$$c_1^{z_1} \dots c_k^{z_k} d.$$

Although $\chi(S_1) \leq -2$ implies that $k \geq 3$, we will assume only $k \geq 2$. Since $G_2$ has the CSA property, we may apply Corollary 3 of [KM98a] to obtain that

$$R_{G_2}(S_1) = \mathrm{ncl}\left(\left\{ [a_i^{-1} z_i, C], [a_i^{-1} z_i, a_j^{-1} z_j] \mid i, j = 1 \ldots k \right\}\right)$$

where $C = C_{G_2}(c_1^{a_1}, \ldots, c_m^{a_m})$ and $z_j \to a_j$ is a solution to $S_1$. A solution must exist since $S_1$ has a solution over $F_{R(S_2 \cup \ldots \cup S_n)}$, and $G_2$ is a quotient of $F_{R(S_2 \cup \ldots \cup S_n)}$. We may find such a solution by enumerating all possible solutions.

Since $G_2$ is CSA, the group $C$ is precisely the maximal abelian subgroup which is the centralizer of $c_1^{a_1}$. By assumption, we may compute a generating set $\{u_1, \ldots, u_m\}$ for $C$. Then

$$G_1 \simeq \langle G_2, t_1, \ldots, t_k \,|\, [t_i, u_l],\ [t_i, t_j],\ 1 \leq i, j \leq k,\ 1 \leq l \leq m \rangle$$

via the isomorphism $t_i \to a_i^{-1} z_i$. Since this is an extension of a centralizer, we complete the argument by reasoning as in Case (II).

*Non-orientable forms.* Suppose that $S_1$ corresponds to a non-orientable surface. Suppose $S_1$ has the form

$$x_1^2 \cdots x_p^2$$

where, by assumption, $p \geq 4$. Then any two non-commuting elements $g, h \in G_2$ yield the non-commutative solution $x_1 \to g$, $x_2 \to g^{-1}$, $x_3 \to h$, $x_4 \to h^{-1}$, and $x_i \to 1$ for $i \geq 4$. This contradicts the assumption that all solutions of $S_1$ are commutative. Suppose $S_1$ has the form

$$x_1^2 \cdots x_p^2 d$$

with $d \neq 1$ and $p \geq 3$. For any commutative solution $x_i \to s_i$ and any $g \notin C_{G_2}(s_1)$, the function $x_1 \to g$, $x_2 \to g^{-1}$, $x_3 \to s_1 \cdots s_p$, and $x_i \to 1$ for $i > 3$ is a non-commutative solution, which is a contradiction.

Suppose $S_1$ has the form

$$x_1^2 \ldots x_p^2 c_1^{z_1} \cdots c_k^{z_k} d.$$

with $p \geq 2$. Though $\chi(S_1) \leq -2$ implies $k \neq 0$, the following argument applies for all $k \geq 0$. Construct any (commutative) solution $x_i \to s_i$, $z_j \to a_j$. From transitivity of commutation, it follows that

$$[c_i^{a_i}, c_j^{a_j}] = [c_i^{a_i}, s_1 \ldots s_p] = 1$$

for all $i, j = 1, \ldots, k$. Let $U = C_{G_2}(c_1^{a_1}, \ldots, c_k^{a_k}, s_1 \ldots s_p)$ and construct a generating set $\{u_1, \ldots, u_m\}$ for $U$. From the proof of Proposition 8 of [KM98a], which needs only the fact that $G_2$ is commutation-transitive and torsion-free, we see that $G_1$ is isomorphic to the group

$$\langle G_2, t_1, \ldots, t_{p+k-1} \mid [u_l, t_j],\ [t_i, t_j],\ 1 \leq i, j \leq p+k-1,\ 1 \leq l \leq m \rangle * \langle x_p \rangle$$

via the isomorphism $t_i \to a_i^{-1} z_i$ for $i = 1, \ldots, k$ and $t_i \to x_i$ for $i = k+1, \ldots, k+p-1$. This group is an extension of a centralizer followed by free product with $\mathbb{Z}$, so we proceed as in Case (II) and Case (IV).

Finally, suppose $S_1$ has the form

$$x_1^2 c_1^{z_1} \ldots c_k^{z_k} d.$$

It is shown in the proof of Proposition 8 of [KM98a] that there exists $s \in G_2$ such that every solution of $S_1$ sends $x_1$ to $s$. Consequently, $s^{-1}x_1$ is in the radical of $S_1$ over $G_2$, hence

$$G_1 \simeq G_2[z_1, \ldots, z_k]/R_{G_2}(c_1^{z_1} \ldots c_k^{z_k} d)$$

and we may argue as in the genus zero case above. Note that we may find $s$ by finding any solution.

**Case $\chi(\mathbf{S_1}) > -\mathbf{2}$.** Assume that $\chi(S_1) > -2$. We consider cases based on the form of $S_1$.

*Orientable forms.* There are two possible forms, $[x, y]d$ and $[x, y]$. The form $[x, y]d$ is a regular quadratic equation (by definition), and the argument for regular equations given at the beginning of the case $\chi(S_1) \leq -2$ applies. For the form $[x, y]$, we apply Case (III).

*Non-orientable forms.* The possible forms are $x^2$, $x^2d$, $x^2y^2$, $x^2y^2d$, and $x^2y^2z^2$. For the form $x^2$, $x \to 1$ is the unique solution since $G_2$ is torsion-free. Hence $x \in R_{G_2}(S_1)$ and $G_1 \simeq G_2$, so there is nothing further to prove.

For the form $x^2d$, find a solution $x \to a$. Note that $d = a^{-2}$. Suppose, for contradiction, that there exists a second solution $x \to b$. Then since $[a, a^{-2}] = 1$, $[b, b^{-2}] = 1$, and $a^{-2} = b^{-2}$ we conclude $[a, b] = 1$ by transitivity of commutation. Then

$$(ab^{-1})^2 = a^2b^{-2} = d^{-1}d = 1$$

which implies $a = b$ since $G_2$ is torsion-free. Consequently, $x \to a$ is the unique solution and $xa^{-1}$ is in the radical of $x^2d$ over $G_2$. Then $\langle G_2, x \,|\, xa^{-1}, x^2d\rangle \simeq G_2$ hence $R_{G_2}(\{x^2d\}) = \mathrm{ncl}_{G_2}(xa^{-1})$ and $G_1 \simeq G_2$.

For the form $x^2y^2$, the analysis is similar. First, check for the existence of a non-trivial solution using Proposition 2.5.9. If all solutions are trivial, then $G_1 \simeq G_2$. Otherwise, let $x \to a$, $y \to b$ be a non-trivial solution. Since $[a, a^2] = 1$ and $[b, b^{-2}] = 1$ we obtain $[a, b] = 1$ by transitivity of commutation. As above, $(ab)^2 = 1$ implies $ab = 1$ hence $xy$ is in the radical of $x^2y^2$. The group $\langle G_2, x, y \,|\, xy, x^2y^2 \rangle \simeq G_2 * \langle x \rangle$ is fully residually $G_2$ hence $R_{G_2}(x^2y^2) = \mathrm{ncl}_{G_2}(xy)$ so

$$G_1 \simeq G_2 * \mathbb{Z}$$

and we may argue as in Case (IV).

For the form $x^2y^2d$, first we determine whether or not all solutions are commutative, using Lemma 4.4.4. If all solutions are commutative, the proof given for the case $\chi(S_1) \leq -2$ and $S_1 = x_1^2 \dots x_p^2 c_1^{z_1} \dots c_k^{a_k} d$ with $p \geq 2$ applies, since there we allowed $k = 0$. Otherwise, find any (non-commutative) solution $x \to a$, $y \to b$. Consider the series of extensions of centralizers

$$\begin{aligned} G_2' &= \langle G_2, t \,|\, [C_{G_2}(ab), t] \rangle, \\ G_2'' &= \langle G_2', s \,|\, [C_{G_2'}(atat), s] \rangle, \\ G_2''' &= \langle G_2'', r \,|\, [C_{G_2''}(s^{-1}atst^{-1}b), r] \rangle, \end{aligned}$$

and the map $\psi : \langle G_2, x, y \,|\, x^2y^2d \rangle \to G_2'''$ given by

$$\begin{aligned} x &\to (at)^s r \\ y &\to r^{-1}t^{-1}b. \end{aligned}$$

Since $(x^2y^2d)^\psi = 1$, hence $\psi$ defines a homomorphism. Using normal forms for elements of HNN-extensions, we can show that $\psi$ is injective (see for example §5 of [KM98a]). Consequently, $\langle G_2, x, y \,|\, S_1 \rangle$ is residually $G_2$ hence $G_1 = \langle G_2, x, y \,|\, S_1 \rangle$. By Lemma 4.4.15, $G_1$ embeds canonically into $\langle H', x, y \,|\, S_1 \rangle$. We then apply the construction above to $\langle H', x, y \,|\, S_1 \rangle$ to embed this group into a group $H$ obtained from $H'$, hence from $\Gamma$, by extensions of centralizers.

For the form $x^2c^zd$, first we determine whether or not all solutions are commutative, using Lemma 4.4.4. Suppose all solutions are commutative. Find any (commutative) solution $x \to a$, $z \to b$. Let $x \to a_1$, $z \to b_1$ be any other solution. We have that $d = (a^2c^b)^{-1} = (a_1^2c^{b_1})^{-1}$ and $[c^b, d] = [c^{b_1}, d] = 1$ since both solutions are commutative. By transitivity of commutation, $[c^b, c^{b_1}] = 1$, and from the CSA property it follows that $[b_1b^{-1}, c] = 1$. This equation may be rewritten as $c^b = c^{b_1}$, and consequently $a_1^2 = a^2$. If $a = 1$, then $a_1 = 1$ since $G_2$ is torsion-free. If $a \neq 1$, then by transitivity of commutation $[a_1, a] = 1$ hence $(a_1a)^2 = 1$ so $a_1 = a$. In either case, $xa^{-1} \in R_{G_2}(S_1)$. Since

$$\langle G_2, x, z \,|\, xa^{-1},\ x^2c^zd \rangle \simeq \langle G_2, z \,|\, c^zda^2 \rangle$$

we may apply the argument for the case $S_1 = c^zd$, given below.

If not all solutions are commutative, find any (non-commutative) solution $x \to a$, $z \to b$. As was done in [KM98a], consider the sequence of extensions of centralizers

$$\begin{aligned} G_2' &= \langle G_2, t \,|\, [C_{G_2}(d), t] \rangle, \\ G_2'' &= \langle G_2', s \,|\, [C_{G_2'}(c^b), s] \rangle, \\ G_2''' &= \langle G_2'', r \,|\, [C_{G_2''}(c^{bt}), r] \rangle, \end{aligned}$$

and the map $\psi : \langle G_2, x, y \,|\, x^2 c^z d \rangle \to G_2'''$ given by

$$\begin{aligned} x &\to a^t \\ y &\to bstr. \end{aligned}$$

As in the previous case, $(x^2 c^z d)^\psi = 1$ and we may prove using normal forms that $\psi$ is injective and complete the argument as above.

For the form $x^2y^2z^2$, first we determine whether or not all solutions are commutative, using Lemma 4.4.4. Suppose all solutions are commutative. It follows from commutation-transitivity of $G_2$ that $[x, y], [x, z], [y, z] \in R_{G_2}(S_1)$, and then from the fact that $G_2$ is torsion-free that $xyz \in R_{G_2}(S_1)$. Let $S_1'$ be the system of equations $\{x^2y^2z^2, [x, y], [x, z], [y, z], xyz\}$. Then

$$\langle G_2, x, y, z \,|\, S_1' \rangle \simeq G_2 * \mathbb{Z}^2.$$

It follows from Case (III) that this group is fully residually $G_2$ and hence

$$\mathrm{ncl}_{G_2}(S_1') = R_{G_2}(S_1') = R_{G_2}(S_1).$$

Then $G_1 = G_2 * \mathbb{Z}^2$ and we may argue as in Case (III).

Now find any solution $x \to a$, $y \to b$, $z \to c$ of $S_1$ in general position. Consider the series of six extensions of centralizers

$$\begin{aligned}
G_2^{(1)} &= \langle G_2, s \,|\, [s, C_{G_2}(ab)] \rangle, \\
G_2^{(2)} &= \langle G_2^{(1)}, r \,|\, [r, C_{G_2^{(1)}}(s^{-1}bc)] \rangle, \\
G_2^{(3)} &= \langle G_2^{(2)}, v \,|\, [v, C_{G_2^{(2)}}(abrs^{-1}bc)] \rangle, \\
G_2^{(4)} &= \langle G_2^{(3)}, t \,|\, [t, C_{G_3}(vasvas)] \rangle, \\
G_2^{(5)} &= \langle G_2^{(4)}, u \,|\, [u, C_{G_2^{(4)}}(s^{-1}brs^{-1}br)] \rangle, \\
G_2^{(6)} &= \langle G_2^{(5)}, w \,|\, [w, C_{G_2^{(5)}}(r^{-1}cv^{-1}r^{-1}cv^{-1})] \rangle,
\end{aligned}$$

and the map $\psi : \langle G_2, x, y, z \,|\, x^2y^2z^2 \rangle \to G_2^{(6)}$ given by

$$\begin{aligned}
x &\to (vas)^t \\
y &\to (s^{-1}br)^u \\
z &\to (r^{-1}cv^{-1})^w.
\end{aligned}$$

As in the previous case, $(x^2y^2z^2)^\psi = 1$ and we may prove, with a lengthy argument using normal forms, that $\psi$ is injective and complete the argument as before.

*Genus zero forms.* The possible forms are $c^z d$ and $c_1^{z_1} c_2^{z_2} d$. The form $c_1^{z_1} c_2^{z_2} d$ was covered under genus zero forms for $\chi(S_1) \leq -2$, since the proof there needed only $k \geq 2$.

For the form $c^z d$, find a solution $z \to a$ and a generating set $\{u_1, \ldots, u_m\}$ for $C_{G_2}(c)$. We claim that $[za^{-1}, u_i]$ is in the radical of $c^z d$, for all $i$. Indeed, if $z \to b$ is

any solution to $c^z d = 1$ over $G_2$ then

$$[ba^{-1}, c] = ab^{-1}c^{-1}ba^{-1}c = ada^{-1}c = c^{-1}c = 1$$

and by transitivity of commutation we have $[ba^{-1}, u_i] = 1$, hence $[za^{-1}, u_i]$ is in the radical. Then

$$\langle G_2, z \mid [za^{-1}, u_i],\ i = 1, \ldots, m\rangle \simeq \langle G_2, t \mid [t, u_i],\ i = 1, \ldots, m\rangle$$

is an extension of the centralizer of $c$, hence is residually $G_2$. Consequently, $G_1$ is isomorphic to the extension of centralizer

$$G_1 \simeq \langle G_2, t \mid [t, u_i],\ i = 1, \ldots, m\rangle$$

and we may argue as in Case (II).

All possible forms of $S_1$ have been covered, so the proof is complete. □

The main result of this chapter now follows from Lemmas 4.4.13 and 4.4.16.

**Theorem 4.4.17.** *Let $\Gamma$ be any torsion-free hyperbolic group. There is an algorithm that, given a finitely presented group $G$ that is fully residually $\Gamma$, constructs*

*(1) finitely many groups $H_1, \ldots, H_n$, each given as a sequence of extensions of centralizers of $\Gamma$, and*

*(2) homomorphisms $\phi_i : G \to H_i$,*

*such that at least one of the $\phi_i$ is injective. This also holds for $G$ in the category of $\Gamma$-groups.*

Although the theorem does not produce a single map that is an embedding, we can produce a single embedding of any *residually*-$\Gamma$ group into a direct product

of groups obtained from $\Gamma$ by extensions of centralizers. Recall that every fully residually $\Gamma$ group is also residually $\Gamma$.

**Corollary 4.4.18.** *Let $\Gamma$ be a torsion-free hyperbolic group. Every finitely presented residually $\Gamma$ group $G = \langle Z \,|\, S \rangle$ embeds into a finite direct product $H_1 \times \ldots \times H_n$, where each $H_i$ is obtained from $\Gamma$ by a finite sequence of extensions of centralizers. Further, the embedding can be constructed effectively.*

*Proof.* Construct the groups and homomorphisms $\phi_i : G \to H_i$. Since $G$ is not assumed to be fully residually $\Gamma$, it may be that no $\phi_i$ is injective, but the construction may be carried out regardless. Let $\phi = \phi_1 \times \ldots \times \phi_n : G \to H_1 \times \ldots \times H_n$ and recall that $\phi_i = \alpha_i \beta_i$, where $\alpha_i : G \to \Gamma_{R(S_i)}$ is constructed in Lemma 4.4.13 and $\beta_i : \Gamma_{R(S_i)} \to H_i$ is constructed in Lemma 4.4.16. Let $g$ be any non-trivial element of $G$. By Lemma 4.4.13, there exists $i$ such that $g^{\alpha_i} \neq 1$, hence $g^{\alpha_i \beta_i} \neq 1$ and therefore $\phi$ is injective. □

We are also able to solve the word problem in any finitely presented residually $\Gamma$ group in polynomial time.

**Corollary 4.4.19.** *Let $\Gamma$ be a torsion-free hyperbolic group and $G = \langle Z \,|\, S \rangle$ any finitely presented group that is known to be residually $\Gamma$. There is an algorithm that, given a word $w$ over the alphabet $Z^{\pm}$, decides whether or not $w = 1$ in $G$ in time polynomial in $|w|$.*

*Proof.* We compute in advance the embedding $\phi : G \to H_1 \times \ldots \times H_n$ from Corollary 4.4.18. Given the input word $w$, we need only compute $w^{\phi}$ and solve the word problem in $H_1 \times \ldots \times H_n$. There is a fixed constant $L$ such that $|\pi_{H_i}(w^{\phi})| \leq L|w|$,

where $\pi_{H_i}$ is projection onto $H_i$, so we have a polynomial reduction to $n$ word problems in the groups $H_1, \ldots, H_n$. It then suffices to show that each $H_i$ has a polynomial time word problem.

Let $H_i$ be formed by a sequence of $m$ extensions of centralizers and proceed by induction. If $m = 0$, then $H_i = \Gamma$ so the word problem in $H_i$ is decidable in polynomial time. Now assume that

$$H_i = \langle H_i', t \,|\, [t, C_{H_i'}(u)] \rangle \tag{4.15}$$

where $u \in H_i'$ and $H_i'$ is formed from $\Gamma$ by a sequence of $m-1$ extensions of centralizers and has a polynomial time word problem. Let $w$ be a word in $H_i$. It suffices to produce a reduced form for $w$ as an element of the HNN-extension (4.15): if any $t^{\pm 1}$ appears in the reduced form then $w \neq 1$, and if no $t^{\pm 1}$ appears then $w \in H_i'$ and we check whether or not $w = 1$ using the word problem algorithm for $H_i'$.

We produce a reduced form for $w$ by examining all subwords of the form $tvt^{-1}$ and $t^{-1}vt$ where no $t^{\pm 1}$ appears in $v$, and making reductions

$$tvt^{-1} \to v, \quad t^{-1}vt \to v$$

whenever $v \in C_{H_i'}(u)$. The element $v$ is in $C_{H_i'}(u)$ if and only if $[v, u] = 1$ in $H_i'$, which is an instance of the word problem in $H_i'$ and so may be checked in polynomial time. It is clear that we need only examine a polynomial number of subwords $tvt^{-1}$ and $t^{-1}vt$ before reaching a reduced form. $\square$

# CHAPTER 5
# Conclusions

In this concluding chapter we provide some commentary on our results and discuss some unsolved problems to which they relate.

## 5.1 Compressed word problem in $\Gamma$-limit groups

The principal results of this work are Theorem 3.4.4 and Theorem 4.4.17. Theorem 3.4.4 gave a polynomial time algorithm for the compressed word problem in limit groups, and prompts the following question.

**Question 5.1.1.** *Let $\Gamma$ be a torsion-free hyperbolic group. Is there a polynomial time algorithm for the compressed word problem in $\Gamma$-limit groups? In particular, is there a polynomial time algorithm for the compressed word problem in $\Gamma$?*

The answer is currently unknown, but Theorem 4.4.17 may be part of the solution. Recall that to prove Theorem 3.4.4, we required the following three components.

(1) An algorithm that embeds any $F$-limit group into a group obtained from $F$ by extensions of centralizers.

(2) A 'big powers' property for extensions of centralizers of limit groups: if $G$ is a limit group and $H = \langle G, t \,|\, [C(g), t] \rangle$ then the set of homomorphisms $\{\phi_n : t \to g^n \mid n \in \mathbb{N}\}$ discriminates $H$ into $G$.[1] Further, for any given

[1] We did not mention this explicitly. It follows from the proof of Theorem 3.4.2, and is a well-known fact.

element of $h \in H$ the minimum $n$ such that $h^{\phi_n} \neq 1$ may be computed and is polynomial in $|h|$.

(3) A polynomial time algorithm for the compressed word problem in $F$.

For the case of a $\Gamma$-limit group $G$, Theorem 4.4.17 provides the algorithm for (1). The fact that the theorem does not produce a single embedding is not a limitation. Suppose we can solve the compressed word problem in each $H_i$ in polynomial time. Then we may compute in advance the maps $\alpha_i : G \to H_i$ and the groups $H_i$, independent of the compressed input word, and apply Corollary 4.4.19.

For item (2), Proposition 1.1 of [KM09] gives the required 'big powers' property. However, it remains unclear how to obtain a bound on the minimum required value of $n$. In the free group case, we used normal forms and a Lyndon length function on $F^{\mathbb{Z}[t]}$, ideas which were developed in [MRS05] using infinite words. Such ideas have yet to be developed for the Lyndon completion $\Gamma^{\mathbb{Z}[t]}$.

For hyperbolic groups, Item (3) remains an open problem.

## 5.2 Compressed word problem in $F^{\mathbb{Z}[t]}$

In Theorem 3.4.4, the limit group $G$ is not included as a part of the input (the algorithm is *non-uniform*). To produce a uniform algorithm would require that the embedding used in Proposition 3.2.2 be computable in polynomial time. The embedding uses Kharlampovich-Miasnikov's Elimination Process, the running time of which seems unlikely to be polynomial.

If we insist that the input group $G$ be given as a sequence of extensions of centralizers of $\Gamma$, the problem is approachable. This is essentially the same as asking to solve the compressed word problem in $F^{\mathbb{Z}[t]}$. Our method does not immediately

give a polynomial time algorithm to this problm: the degree of the polynomial in Theorem 3.4.4 depends on the number extensions of centralizers, the degree of each extension, and the word length of each element whose centralizer is extended, and so increases with a 'larger' input group $G$. However, the 'big powers' $P^i$ that we use in Theorem 3.4.2 are overestimates and needed only in the worst case of a word consisting entirely of a power of a single stable letter $t_{u,i}$. One can reduce the running time by selecting the powers more carefully, though whether this would be enough to obtain polynomial time (for the uniform algorithm) in unclear.

## 5.3 Comments on Chapter 4

In §4.3.2 we produced diagrams encoding the set of homomorphisms from a finitely presented group $G$ to $\Gamma$. As we noted there, these are not 'Hom-digarams' in the usual sense. Groves has proved that diagrams in which the vertex groups are proper quotients of $G$ do exists, but their effective construction remains an open problem.

In our main result, Theorem 4.4.17, we are not able to determine which of the homomorphisms $\phi_i$ is an embedding. It is possible that many of the homomorphisms are embeddings: this prevents us from simply enumerating elements $g$ of $G$ and computing their image under the $\phi_i$ until all but one of the $\phi_i$ fails to be injective. We could avoid this problem by grouping the images $G^\phi$ of $G$ into isomorphism classes, since the images $G^{\phi_i}$ for injective $\phi_i$ will form a single class. However, it is not clear how to solve this isomorphism problem (i.e. the isomorphism problem for finitely generated subgroups of groups obtained from $\Gamma$ by extensions of centralizers).

We saw in Corollary 4.4.19 that despite not knowing which of the homomorphisms $\phi_i$ is injective, we could still use a solution to the word problem in the groups $H_i$ to solve the word problem in $G$. The same holds for some other interesting algorithmic problems. The conjugacy problem in $G$ reduces to checking that conjugacy holds in $G^{\phi_i}$ for all $i$, and similarly for the membership problem. Though neither of these problems has been solved in subgroups of groups obtained from $\Gamma$ by extensions of centralizers, solutions are known for the case when $\Gamma$ is free.

REFERENCES


[Aea91] J. M. Alonso and et al. Notes on word hyperbolic groups. In *Group theory from a geometrical viewpoint (Trieste, 1990)*, pages 3–63. World Sci. Publ., River Edge, NJ, 1991. Edited by H. Short.

[Ali05] E. Alibegović. A combination theorem for relatively hyperbolic groups. *Bull. London Math. Soc.*, 37(3):459–466, 2005.

[BF09] M. Bestvina and M. Feighn. Notes on Sela's work: limit groups and Makanin-Razborov diagrams. In *Geometric and cohomological methods in group theory*, volume 358 of *London Math. Soc. Lecture Note Ser.*, pages 1–29. Cambridge Univ. Press, Cambridge, 2009.

[BKM07] I. Bumagin, O. Kharlampovich, and A. Miasnikov. The isomorphism problem for finitely generated fully residually free groups. *J. Pure Appl. Algebra*, 208(3):961–977, 2007.

[BMR99] G. Baumslag, A. Myasnikov, and V. Remeslennikov. Algebraic geometry over groups. I. Algebraic sets and ideal theory. *J. Algebra*, 219(1):16–79, 1999.

[BMR02] G. Baumslag, A. Myasnikov, and V. Remeslennikov. Discriminating completions of hyperbolic groups. *Geom. Dedicata*, 92:115–143, 2002. Dedicated to John Stallings on the occasion of his 65th birthday.

[Boo59] W. Boone. The word problem. *Ann. of Math. (2)*, 70:207–265, 1959.

[Bow99] B. Bowditch. Relatively hyperbolic groups. 1999. Preprint, University of Southampton.

[Bry77] R. M. Bryant. The verbal topology of a group. *J. Algebra*, 48(2):340–346, 1977.

[Bum04] I. Bumagin. The conjugacy problem for relatively hyperbolic groups. *Algebr. Geom. Topol.*, 4:1013–1040, 2004.

[CG05] C. Champetier and V. Guirardel. Limit groups as limits of free groups. *Israel J. Math.*, 146:1–75, 2005.

[Dah03] F. Dahmani. Combination of convergence groups. *Geom. Topol.*, 7:933–963 (electronic), 2003.

[Dah08] F. Dahmani. Finding relative hyperbolic structures. *Bull. Lond. Math. Soc.*, 40(3):395–404, 2008.

[Dah09] F. Dahmani. Existential questions in (relatively) hyperbolic groups. *Israel J. Math.*, 173:91–124, 2009.

[EH01] D. Epstein and D. Holt. Computation in word-hyperbolic groups. *Internat. J. Algebra Comput.*, 11(4):467–487, 2001.

[Far98] B. Farb. Relatively hyperbolic groups. *Geom. Funct. Anal.*, 8(5):810–840, 1998.

[Gil87] N. D. Gilbert. Presentations of the automorphism group of a free product. *Proc. London Math. Soc. (3)*, 54(1):115–140, 1987.

[GM08] D. Groves and J. F. Manning. Dehn filling in relatively hyperbolic groups. *Israel J. Math.*, 168:317–429, 2008.

[Gro87] M. Gromov. Hyperbolic groups. In *Essays in group theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 75–263. Springer, New York, 1987.

[Gro05] D. Groves. Limit groups for relatively hyperbolic groups. II. Makanin-Razborov diagrams. *Geom. Topol.*, 9:2319–2358, 2005.

[Gro09] D. Groves. Limit groups for relatively hyperbolic groups. I. The basic tools. *Algebr. Geom. Topol.*, 9(3):1423–1466, 2009.

[Gub86] V. S. Guba. Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems. *Mat. Zametki*, 40(3):321–324, 428, 1986.

[Hal59] M. Hall, Jr. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[HL08] N. Haubold and M. Lohrey. Compressed word problems in hnn-extensions and amalgamated products. 2008. Preprint. arXiv:0811.3303v1 [math.GR].

[HLM10] N. Haubold, M. Lohrey, and C. Mathissen. Compressed conjugacy and the word problem for outer automorphism groups of graph groups. 2010. Preprint. arXiv:1003.1233v1 [math.GR].

[KM98a] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz. *J. Algebra*, 200(2):472–516, 1998.

[KM98b] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. II. Systems in triangular quasi-quadratic form and description of residually free groups. *J. Algebra*, 200(2):517–570, 1998.

[KM99] O. Kharlampovich and A. Myasnikov. Description of fully residually free groups and irreducible affine varieties over a free group. In *Summer School in Group Theory in Banff, 1996*, volume 17 of *CRM Proc. Lecture Notes*, pages 71–80. Amer. Math. Soc., Providence, RI, 1999.

[KM05a] O. Kharlampovich and A. Myasnikov. Effective JSJ decompositions. In *Groups, languages, algorithms*, volume 378 of *Contemp. Math.*, pages 87–212. Amer. Math. Soc., Providence, RI, 2005.

[KM05b] O. Kharlampovich and A. Myasnikov. Implicit function theorem over free groups. *J. Algebra*, 290(1):1–203, 2005.

[KM06] O. Kharlampovich and A. Myasnikov. Elementary theory of free non-abelian groups. *J. Algebra*, 302(2):451–552, 2006.

[KM09] O. Kharlampovich and A. Myasnikov. Limits of relatively hyperbolic groups and Lyndon's completions. arXiv:0904.2423v3 [math.GR], 2009.

[KM10] O. Kharlampovich and A. Myasnikov. Equations and fully residually free groups. In *Combinatorial and geometric group theory*, Trends Math., pages 203–242. Birkhäuser/Springer Basel AG, Basel, 2010.

[KMSS03] I. Kapovich, A. Miasnikov, P. Schupp, and V. Shpilrain. Generic-case complexity, decision problems in group theory, and random walks. *J. Algebra*, 264(2):665–694, 2003.

[Loh04] M. Lohrey. Word problems on compressed words. In *Automata, languages and programming*, volume 3142 of *Lecture Notes in Comput. Sci.*, pages 906–918. Springer, Berlin, 2004.

[LS77] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. Springer, 1977.

[LS07] M. Lohrey and S. Schleimer. Efficient computation in groups via compression. In *Second International Symposium on Computer Science in Russia, CSR 2007, Ekaterinburg, Russia, September 3-7, 2007. Proceedings*, volume 4649 of *Lecture Notes in Computer Science*, pages 249–258. Springer Berlin / Heidelberg, 2007.

[Lyn60] R. Lyndon. Groups with parametric exponents. *Trans. Amer. Math. Soc.*, 96:518–533, 1960.

[Mac10] J. Macdonald. Compressed words and automorphisms in fully residually free groups. *Internat. J. Algebra Comput.*, 20(3):343–355, 2010.

[Mak84] G. S. Makanin. Decidability of the universal and positive theories of a free group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 48(4):735–749, 1984.

[MR96] A. Myasnikov and V. Remeslennikov. Exponential groups. II. Extensions of centralizers and tensor completion of CSA-groups. *Internat. J. Algebra Comput.*, 6(6):687–711, 1996.

[MRS05] A. Myasnikov, V. Remeslennikov, and D. Serbin. Regular free length functions on Lyndon's free $\mathbb{Z}[t]$-group $F^{\mathbb{Z}[t]}$. In *Groups, languages, algorithms*, volume 378 of *Contemp. Math.*, pages 37–77. Amer. Math. Soc., Providence, RI, 2005.

[Nie19] J. Nielsen. Uber die Isomorphismen unendlicher Gruppen ohne Relation. *Mathematische Annalen*, 79:269–272, 1919.

[Nov58] P. S. Novikov. On the algorithmic insolvability of the word problem in group theory. In *American Mathematical Society Translations, Ser 2, Vol. 9*, pages 1–122. American Mathematical Society, Providence, R. I., 1958.

[Osi06a] D. Osin. Elementary subgroups of relatively hyperbolic groups and bounded generation. *Internat. J. Algebra Comput.*, 16(1):99–118, 2006.

[Osi06b] D. Osin. Relatively hyperbolic groups: intrinsic geometry, algebraic properties, and algorithmic problems. *Mem. Amer. Math. Soc.*, 179(843):vi+100, 2006.

[Pla94] W. Plandowski. Testing equivalence of morphisms on context-free languages. In *Algorithms—ESA '94 (Utrecht)*, volume 855 of *Lecture Notes in Comput. Sci.*, pages 460–470. Springer, Berlin, 1994.

[Raz84] A. A. Razborov. Systems of equations in a free group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 48(4):779–832, 1984.

[RS95] E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Invent. Math.*, 120(3):489–512, 1995.

[RW10] C. Reinfeldt and R. Weidmann. Makanin-razborov diagrams for hyperbolic groups. Preprint, 2010.

[Sch08] S. Schleimer. Polynomial-time word problems. *Comment. Math. Helv.*, 83(4):741–765, 2008.

[Sel01] Z. Sela. Diophantine geometry over groups. I. Makanin-Razborov diagrams. *Publ. Math. Inst. Hautes Études Sci.*, (93):31–105, 2001.

[Sel06] Z. Sela. Diophantine geometry over groups. VI. The elementary theory of a free group. *Geom. Funct. Anal.*, 16(3):707–730, 2006.

[Sel09] Z. Sela. Diophantine geometry over groups. VII. The elementary theory of a hyperbolic group. *Proc. Lond. Math. Soc. (3)*, 99(1):217–273, 2009.