Equation Problem Over Central Extensions of Hyperbolic Groups

BY

HAO LIANG
B.S., Zhejiang University, 2007
M.S., University of Illinois at Chicago, 2009

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2013

Chicago, Illinois

Defense Committee:

Daniel Groves, Chair and Advisor
Marc Culler , Mathematics, Statistics, and Computer Science
Alexander Furman, Mathematics, Statistics, and Computer Science
Kevin Whyte, Mathematics, Statistics, and Computer Science
Benson Farb, University of Chicago

To my parents and Zhuoying.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my advisor, Daniel Groves, to whom I am greatly indebted for the knowledge, guidance and support he gave me. This thesis would not have been possible without his mathematical insights. I have always enjoyed our conversations and I am never more excited about doing math than when I'm leaving his office with a collection of new ideas to explore. His perpetual energy and passion for mathematics will continue to be a source of inspiration.

It was an honor to have Marc Culler, Benson Farb, Alex Furman, and Kevin Whyte serve as members of my defense committee. Especially, I want thank Benson Farb for helpful insights and his interest in this work.

I would like to thank my colleagues with whom I have shared so many enlightening and wonderful conversations. Especially, I would like to thank Michael Siler, for discussing math with me countless times and for being a good friend.

I would like to thank the faculties and staffs of University of Illinois at Chicago math department for creating a wonderful environment for graduate study.

At last, I would like to thank my undergraduate advisor Shiu-chun Wong, without whose guidance and encouragement I might not ever have entered mathematics.

L.H.

TABLE OF CONTENTS

SUMMARY

The Equation Problem in finitely presented groups asks if there exists an algorithm which determines in finite amount of time whether any given equation system has a solution or not. We show that the Equation Problem in central extensions of hyperbolic groups is solvable.

CHAPTER 1

INTRODUCTION

Decision problems in groups has been an important area of group theory since Max Dehn proposed the Word Problem, the Conjugacy Problem and the Group Isomorphism Problem in 1911. The Equation Problem is a vast generalization of the word problem and the conjugacy problem. Let G be a finitely presented group and let C be a generating set for G. Denote a set of variables by U. An *equation system* is a finite collection of equations $w_i = 1$ where $w_i \in (U \cup C)^*$. Let $\mathcal{E} = \{w_i = 1 \mid i = 1 \cdots n\}$ be an equation system in G. A *solution* of $\mathcal{E}$ in G is a map $f : U \to G$ such that the induced monoid homomorphism (sending each $c \in C$ to itself) $\bar{f} : (U \cup C)^* \to G$ maps w_i to 1 for $1 \leq i \leq n$. Let $\mathcal{C}$ be a class of finitely presented groups. The *Equation Problem* in $\mathcal{C}$ asks the following question: Is there an algorithm which takes as input a presentation of a group $G \in \mathcal{C}$ and a finite system of equations with constants in G and which decides whether there exists a solution or not? When the answer is positive, we say that the Equation Problem in $\mathcal{C}$ is solvable.

It is well known that there exists finitely presented groups with unsolvable Word Problem. Since the Equation problem is a generalization of the Word Problem. A direct consequence is the existence of groups with unsolvable equation problem. In fact there exists a free 3-step nilpotent group of rank 2 with unsolvable equations problem ((18), see also (15)). Therefore the Equation Problem is strictly harder than the word problem and the conjugacy problem since these two problems are solvable in finitely generated nilpotent groups (See (16, Chapter 4)).

The most famous breakthrough in solving equations over groups is the solution of the Equation Problem in free groups by Makanin (9). In (3) Dahmani and Guirardel and independently in (8) Lohrey and Senizergues give an algorithm for solving equations and inequations with rational constraints (See Def 4) in virtually free groups. One of the most successful methods of solving the Equation Problem for groups is to reduce it to the Equation Problem over a (virtually) free group. Diekert and Muscholl (4) reduce the Equation Problem in right-angled Artin groups to free groups. Rips and Sela (14) reduce the Equation Problem in torsion free hyperbolic groups to the Equation Problem in free groups. Dahmani and Guirardel (3) reduce the problem in hyperbolic groups (possibly with torsion) to solving equations with rational constraints over virtually free groups.

Besides being a natural algorithmic problem in groups, the equation problem has the following interpretation in terms of homomorphisms between groups: Let K, G be finitely presented groups and $\langle x_1, \cdots, x_n \mid r_1, \cdots, r_i \rangle$ be a presentation of K. Suppose one's favorite elements in K are $w_1, \cdots, w_l$. Here w_i are words in x_i. Let $c_1, \cdots, c_l$ be elements of G. Here is a natural question one might want to ask: Is there a homomorphism from K to G sending w_i to c_i? The question is equivalent to asking whether the equation system $E = \{r_i = 1, w_j = c_j \mid 1 \leq i \leq m; 1 \leq j \leq l\}$ has a solution in G. Under this interpretation x_i become variables and note that r_i are words in x_i. Hence a positive solution to the Equation Problem for G gives a way to determine algorithmically whether particular kinds of homomorphisms to G exist.

A geodesic triangle in a metric space is said to be *δ-slim* if each of its sides is contained in the δ-neighbourhood of the union of the other two sides. A geodesic space X is said to be *hyperbolic* there exists some $\delta>0$ if every geodesic triangle in X is δ-slim. A finitely generated group is *hyperbolic* if its acts properly and cocompactly on a hyperbolic space.

Hyperbolic groups are one of the central classes of objects in geometric group theory. The study of hyperbolic groups has been very fruitful since Gromov introduced them in 1987. In particular, hyperbolic groups have very well-controlled algorithmic properties. All the decision problems mentioned above are solvable for hyperbolic groups.

In this thesis, we consider the Equation Problem in central extensions of hyperbolic groups. We prove the following theorem.

Theorem 1. *The Equation Problem is solvable in central extensions of hyperbolic groups.*

A source of interesting examples of central extensions of hyperbolic groups is 3-manifold theory. A Seifert fibered space is a 3-manifold together with a "nice" decomposition as a disjoint union of circles. Most "small" 3-manifolds are Seifert fibered spaces, and they account for all compact oriented manifolds in 6 of the 8 Thurston geometries of the geometrization conjecture (proved by Perelmann. See (10)). One of the most important algebraic invariants of 3-manifold is the fundamental group. The fundamental groups of a large and interesting class of Seifert fibered spaces are central extensions of hyperbolic groups. All these Seifert fibered spaces are aspherical and the fundamental group is a complete topological invariant. Hence information about maps between fundamental groups of these spaces gives essentially all information up to homotopy about maps between these spaces. As pointed out above the Equation Problem is

an important tool for studying maps between groups. We believe there will be applications of Theorem 1 that lead to new understanding of maps between Seifert fibered spaces.

The main tools we use are the following: (1) Canonical representatives constructed by Rips and Sela (See (14)), which allow them to solve equation systems over torsion free hyperbolic groups; (Dahmani and Guirardel ((3)) solve equations over hyperbolic groups with torsion based on Rips and Selas work.) (2) The theory of equations over virtually free group by Dahmani and Guirardel ((3)) and (3) the work of Neumann and Reeves on the automaticity of central extensions of hyperbolic groups ((12)).

The organization of this thesis is as follow. In Chapter 2 we recall important definitions and key results from (3) and (12), which are the main tools we use in this paper, and describe the idea of the proof of Theorem 1. In Chapter 3, we construct the finite state automata that we use in the proof of Theorem 1. In Chapter 4, we prove Theorem 1.

CHAPTER 2

BACKGROUND AND THE IDEA OF THE PROOF OF THEOREM 1

In the chapter we recall important definitions and key results from (3) and (12) and explain the idea of the proof of Theorem 1.

2.1 Equation Problem in hyperbolic groups

Definition 1. *Let $\delta>0$. A geodesic triangle in a metric space is said to be* δ-slim *if each of its sides is contained in the δ-neighbourhood of the union of the other two sides. A geodesic space X is said to be* hyperbolic *there exists some $\delta>0$ if every triangle in X is δ-slim. A finitely generated group is* hyperbolic *if its Cayley graph is hyperbolic.*

Let Γ be a hyperbolic group, X be a finite symmetric generating set of Γ, K_Γ be the Cayley graph of Γ with respect to X and δ be a hyperbolic constant for K_Γ.

Definition 2. *The* Rips complex *of K_Γ, denoted by $R_{50\delta}(K_\Gamma)$, is the simplicial complex whose set of vertices is Γ and whose simplices are subsets of Γ of diameter at most 50δ in K_Γ.*

Denote the 1-skeleton of the first barycentric subdivision of $R_{50\delta}(K_\Gamma)$ by $\mathcal{K}$.

The point of considering $\mathcal{K}$ is to associate a canonical center to every subset of Γ of diameter at most 50δ in K_Γ.

The action of Γ on K_Γ extends to an action on $\mathcal{K}$. The quotient $\mathcal{K}/\Gamma$ is a finite graph and can be given the structure of a finite graph of finite groups (vertices and edges are decorated

by stabilizers of their preimages in $\mathcal{K}$). Hence $\pi_1(\mathcal{K}/\Gamma)$ is virtually free. A finite presentation of $\pi_1(\mathcal{K}/\Gamma)$ can be computed.

As in (3), let V be the set of paths v in $\mathcal{K}$ which start at the identity and end at a vertex of K_Γ up to homotopy relative to endpoints. Let π denote the natural homomorphism from V to Γ sending each path to its endpoint. We give V a group structure by defining vv' to be the homotopy class of the concatenation $v \cdot (\pi(v)v')$ (where $\pi(v)v'$ is the translate of v' by $\pi(v) \in \Gamma$).

Dahmani and Guirardel prove the following (3, Lemma 9.9)

Lemma 1. *The group V is virtually free. More precisely, it is isomorphic to the fundamental group of the finite graph of finite groups $\mathcal{K}/\Gamma$. In particular, a presentation of V is computable from a presentation of Γ.*

We need a slightly stronger statement about V.

Lemma 2. *A finite presentation $\langle Y|R\rangle$ of V is computable. Moreover one can compute each $y \in Y$ as an explicit path in $\mathcal{K}$.*

Note that a finite presentation of V is computable by Lemma 1. The point of Lemma 2 is that one can compute each $y \in Y$ as an explicit path in $\mathcal{K}$.

Proof. First we note that any finite neighborhood of $\mathcal{K}$ can be constructed since the word problem of Γ is solvable. Let $\theta : T \to \mathcal{K}$ be the universal cover of $\mathcal{K}$. By (3, proof of Lemma 9.9) we have:

1. V acts on T by isometries;

2. θ is π-equivariant;

3. T/V (given a graph of group structure as in (17, page 54)) is isomorphic to $\mathcal{K}/\Gamma$ as graph of groups. In particular they are isomorphic as graphs.

Starting with a vertex $t_0 \in T$ which is mapped to $1_\Gamma \in \mathcal{K}$ by θ, one can construct any finite neighborhood of t_0 in T and compute the map u in that neighborhood. (This is because one can construct any finite neighborhood of $1_\Gamma \in \mathcal{K}$ and one can construct any finite ball of the universal cover of a locally finite graph.)

Since the quotient map from $\mathcal{K}$ to $\mathcal{K}/\Gamma$ can be computed in any finite neighborhood of 1_Γ, one can compute the quotient map from T to T/V explicitly in any finite neighborhood of t_0.

Given any $v \in V$ explicitly as a path in $\mathcal{K}$ and any point t in T in a explicitly constructed finite neighborhood of t_0, one can compute $v \cdot t$ explicitly. (Here we assume that the explicitly constructed finite neighborhood of t_0 also contains $v \cdot t$.)

One can compute elements of the vertex groups explicitly as paths in $\mathcal{K}$: vertex groups are stabilizers of vertices of T. One can find those vertices explicitly. For any given element of V, one can check whether it fixes any given vertex. Hence one can compute all elements in the stabilizer of a given vertex by checking each element of V according to their lengths (in $\mathcal{K}$). One knows when to stop checking because one knows the size of each stabilizer.

One can also compute all the γ_y (as in (17)) explicitly because given any two vertices of T in the same V-orbit , one can find an explicit element of V that takes one to the other.

Since the presentation of V given by $\pi_1(T/V)$ has elements of the vertex groups of $(G, T/V)$ and γ_y's as generators, the proof is complete. □

We now recall how Dahmani and Guirardel reduce an equation system in Γ to finitely many equation systems in V.

By introducing new variables, one can find an equivalent triangular equation system for any equation of length greater than three. (The picture behind this is that one can cut a polygon into triangles.) For equation of length two, say $x^2 = 1$, one can replace it by the triangular equation with $x^2 1 = 1$. Therefore it suffice to consider only triangular equation systems.

Denote a set of variables (unknowns) by U and a finite set of words in X by C. Let $\mathcal{F} = \{\gamma_{i,1}\gamma_{i,2}\gamma_{i,3} = 1, i = 1, \cdots, n\}$ be a triangular equation system over Γ, where $\gamma_{i,j} \in U \cup C$.

Let $\mu_0 = 8$ and $\lambda_0 = 400\delta m_0$, where m_0 is a bound on the cardinality of balls of radius 50δ in K_Γ. Consider $(\lambda_1, \mu_1) = (\lambda_0, \mu_0 + 2 + 2/\lambda_0)$, so that any concatenation of a (λ_0, μ_0)-quasi-geodesic with a path of length 1 at each extremity is a (λ_1, μ_1)-quasi-geodesic.

Definition 3. *$\mathcal{QG}(V) \subset V$ is the set of elements such that the corresponding reduced path in $\mathcal{K}$ is (λ_1, μ_1)-quasi-geodesic.*

Denote by $V_{\leq l}$ the set of elements of V whose corresponding reduced path in $\mathcal{K}$ has length at most l.

Dahmani and Guirardel use Rips and Sela's canonical representatives (14) to prove the following key proposition (3, Proposition 9.10), which allows them to reduce any equation system in Γ to finitely many equation systems in V.

Proposition 1 (Dahmani-Guirardel)**.** *Then there exists a computable constant κ_1 (depending on Γ and $\mathcal{F}$) such that for any solution $(g_u) \in \Gamma^U$ we have the following:*

For each $u \in U \cup \bar{U}$, there exists $\tilde{g}_u \in \mathcal{QG}(V)$ with $\tilde{g}_{\bar{u}} = (\tilde{g}_u)^{-1}$ and $\pi(\tilde{g}_u) = g_u$. For each $\gamma_{i,1}\gamma_{i,2}\gamma_{i,3} = 1$ in $\mathcal{F}$ and for each $j \in \{1, 2, 3 \ mod \ 3\}$, there exists $l_{i,j} \in \mathcal{QG}(V)$ and $c_{i,j} \in V_{\leq \kappa_1}$ such that:

1. $\tilde{g}_{\gamma_{i,j}} = l_{i,j}c_{i,j}(l_{i,j+1})^{-1}$ *in* V;
2. $\pi(c_{i,1}c_{i,2}c_{i,3}) = 1$ *in* Γ.

Conversely, given any family of elements of V: $(\tilde{g}_u)_{u\in U\cup\bar{U}}$; $(l_{i,j})_{1\leq i\leq n, 1\leq j\leq 3}$ and $(c_{i,j})_{1\leq i\leq n, 1\leq j\leq 3}$ satisfying $\tilde{g}_{\bar{u}} = (\tilde{g}_u)^{-1}$, (1) and (2), respectively, the family $g_u = \pi(\tilde{g}_u)$ is a solution of $\mathcal{F}$.

The $\tilde{g}_u$'s are called *Canonical Representatives*.

For each tuple $\bar{c}$ of $c_{i,j} \in V_{\leq \kappa_1}$ satisfying (2), define an equation system $\mathcal{F}(\bar{c})$ in V as follows: Let $\{v_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq 3\}$ be a set of variables such that $v_{i,j}$ and $v_{i',j'}$ are the same variable if and only if $\gamma_{i,j}$ and $\gamma_{i',j'}$ are the same. Let $\{p_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq 3\}$ be a set of distinct variables. We define

$$\mathcal{F}(\bar{c}) = \begin{cases} p_{i,1}c_{i,1}(p_{i,2})^{-1} = v_{i,1} \\ p_{i,2}c_{i,2}(p_{i,3})^{-1} = v_{i,2} \qquad 1 \leq i \leq n; 1 \leq j \leq 3; \\ p_{i,3}c_{i,3}(p_{i,1})^{-1} = v_{i,3} \end{cases}$$

We call $\mathcal{F}(\bar{c})$ *tripod equation system* associated with $\bar{c}$.

Suppose that $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ is a solution of $\mathcal{F}(\bar{c})$ in V. Let $\tilde{v}_{i,j} = \pi(\bar{v}_{i,j})$. Then since $c_{i,j}$ satisfy Condition (2) in Proposition 1 we have that

$$\tilde{v}_{i,1}\tilde{v}_{i,2}\tilde{v}_{i,3} = 1, \quad i = 1, \cdots, n.$$

With these equations we are almost ready to say that $\{\tilde{v}_{i,j}\}$ is a solution of $\mathcal{F}$. The one extra thing we need is that $\tilde{v}_{i,j}$ should equal $\gamma_{i,j}$ whenever $\gamma_{i,j}$ is a constant in Γ. This is ensured by using Equation system with rational constraints, which is defined below.

Definition 4. *A* rational subset *of a finitely presented group G is the image of a regular language of some generating set under the canonical projection.*

Let C be a generating set for G. Denote a set of variables by U. An equation system with rational constraints *is an a finite collection of equations $w_i = 1$ where $w_i \in (U \cup C)^*$ with finite set of pairs (u, R_u), where $u \in U$ and R_u is a rational subset of G.*

Let $\mathcal{E} = \{w_i = 1 \mid i = 1 \cdots n\} \cup \{(u, R_u) \mid u \in U)\}$ be an equation system with rational constraints in G. A solution *of $\mathcal{E}$ in G is a map $f : U \to G$ such that $f(u) \in R_u$ and the induced monoid homomorphism (sending each $c \in C$ to itself) $\bar{f} : (U \cup C)^* \to G$ maps w_i to* 1 *for $1 \leq i \leq n$.*

Convention 2. *We will use the notation $u \in R_u$ instead of (u, R_u) when we write rational constraints in equation systems.*

We add rational constraints to the tripod equations system $\mathcal{F}(\bar{c})$ as follow: If $\gamma_{i,j}$ is a constant in Γ, let $L_{\gamma_{i,j}}$ be the rational subset (of V) $\{\tilde{g} \in \mathcal{QG}(V) \mid \pi(\tilde{g}) = \gamma_{i,j}\}$. Otherwise let $L_{\gamma_{i,j}} = V$. We define:

$$\mathcal{F}_R(\bar{c}) = \begin{cases} p_{i,1}c_{i,1}(p_{i,2})^{-1} = v_{i,1} \\ p_{i,2}c_{i,2}(p_{i,3})^{-1} = v_{i,2} \\ p_{i,3}c_{i,3}(p_{i,1})^{-1} = v_{i,3} \\ v_{i,j} \in L_{\gamma_{i,j}} \end{cases} \quad 1 \leq i \leq n; 1 \leq j \leq 3;$$

Suppose $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ to denote a solution of $\mathcal{F}_R(\bar{c})$ in V. When $\gamma_{i,j}$ is a constant, the rational constraint $v_{i,j} \in L_{\gamma_{i,j}}$ implies that $\tilde{v}_{i,j} = \pi(\bar{v}_{i,j}) = \gamma$. Therefore $\{\tilde{v}_{i,j}\}$ is a solution of $\mathcal{F}$.

On the other hand, by Proposition 1 if $\mathcal{F}$ has a solution in Γ then $\mathcal{F}_R(\bar{c})$ has a solution in V for some tuple $\bar{c}$ of $c_{i,j} \in V_{\leq \kappa_1}$ satisfying (2) in Proposition 1. All such tuples $\bar{c}$ can be computed since each $c_{i,j}$ has bounded length. Note that the length bound κ_1 on $c_{i,j}$ given by Proposition 1 is determined by Γ and $\mathcal{F}$. Hence the set of tuples $\bar{c}$ of $c_{i,j} \in V_{\leq \kappa_1}$ satisfying (2) in Proposition 1 is determined by Γ and $\mathcal{F}$. Since there are finitely many $\bar{c}$, any equation system in any hyperbolic group can be reduced to finitely many equation systems $\mathcal{F}_R(\bar{c})$ in some virtually free group, which are solvable by the next theorem (3, Theorem 3):

Theorem 3 (Dahmani-Guirardel)**.** *There exists an algorithm which takes as input a presentation of a virtually free group G, and a system of equations with constants in G, together with a set of rational constraints, and which decides if there exists a solution or not.*

Rational constraints play a very important role in our proof of Theorem 1 as we explain in the next section.

2.2 Idea of the proof of Theorem 1

Let E be a central extension of a hyperbolic group by a finitely generated abelian group. Given a finite presentation of E, by (2, Proposition 1.1) one can compute the finite presentations of all terms in a short exact sequence

$$1 \to A \to E \to \Gamma \to 1$$

where Γ is a hyperbolic group and A is a finitely generated abelian group. Denote the inclusion from A to E by i and the projection from E to Γ by p.

Let $\mathcal{E} = \{e_{i,1}e_{i,2}e_{i,3} = 1, i = 1, \cdots, n\}$ be a triangular equation system in E. Denote by $\mathcal{F}$ the equation system $p(\mathcal{E}) = \{p(e_{i,1})p(e_{i,2})p(e_{i,3}) = 1, i = 1, \cdots, n\}$ in Γ, where $p(e_{i,j}) = e_{i,j}$ if $e_{i,j}$ is a variable. Here is an attempt to check whether $\mathcal{E}$ has a solution in E:

Use the algorithm in Theorem 3 to solve all the tripod equation systems with rational constraints $\mathcal{F}_R(\bar{c})$ associated to $\mathcal{F}$ and Γ.

If none of the $\mathcal{F}_R(\bar{c})$ has a solution, then $\mathcal{F}$ has no solution in Γ and hence $\mathcal{E}$ has no solution in E.

Suppose some $\mathcal{F}_R(\bar{c})$ has a solution. Let $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ be a solution. Then $\{\pi(\bar{v}_{i,j})\}$ is a solution of $\mathcal{F}$ in Γ. Let $s : \Gamma \to E$ be a section. In general, $\{s(\pi(\bar{v}_{i,j}))\}$ is not a solution of $\mathcal{E}$. But we

know that $s(\pi(\bar{v}_{i,1}))s(\pi(\bar{v}_{i,2}))s(\pi(\bar{v}_{i,3})) \in A$ for all $1 \leq i \leq n$. We set up the following equation system in A:

$$\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j}) = \{w_{i,1}w_{i,2}w_{i,3} = -s(\pi(\bar{v}_{i,1}))s(\pi(\bar{v}_{i,2}))s(\pi(\bar{v}_{i,3})) \mid 1 \leq i \leq n\},$$

where $w_{i,j}$ and $w_{i',j'}$ represent the same variable if $e_{i,j}$ and $e_{i',j'}$ are the same variable in $\mathcal{E}$ and $w_{i,j} = e_{i,j} - s(p(\bar{v}_{i,j}))$ is a constant in A when $e_{i,j}$ is a constant in E. Suppose $\{\bar{w}_{i,j}\}$ is a solution of $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$. It is easy to check that $\{\bar{e}_{i,j} = s(\pi(\bar{v}_{i,j}))\bar{w}_{i,j}\}$ is a solution of $\mathcal{E}$. Linear algebra can be used to solve $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$ since A is finitely generated and abelian. We check all $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$ to see if they have a solution in A. If at least one does, than $\mathcal{E}$ has a solution.

We point out that if $\mathcal{E}$ has a solution, then the process above will detect it. (To see this, suppose $\mathcal{E}$ has a solution $\{\bar{e}_{i,j}\}$, then $\{p(\bar{e}_{i,j})\}$ is a solution of $\mathcal{F}$. Hence there is some $\bar{c}$ such that $\mathcal{F}(\bar{c})$ has a solution $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ with $\pi(\bar{v}_{i,j}) = p(\bar{e}_{i,j})$. It is easy to check that $\{\bar{w}_{i,j} = \bar{e}_{i,j} - s(p(\bar{v}_{i,j}))\}$ is a solution of $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$.) Hence if the above process terminates before any solution is found, then $\mathcal{E}$ has no solution in E.

There is a obvious problem about solving $\mathcal{E}$ this way: $\mathcal{F} = p(\mathcal{E})$ can have infinitely many solutions in Γ even if $\mathcal{E}$ has no solution. In this case at least of the tripod equation system with rational constraints $\mathcal{F}_R(\bar{c})$ has infinitely many solutions. So there are infinitely many $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$ to check. But none of them has a solution and so the process of checking will never terminate. Here is an explicit example of this phenomenon:

Example 1. *Let S be the genus two surface and T^1S be the unit tangent bundle of S. The following short exact sequence defines $\pi_1(T^1S)$ as a central extension of $\pi_1(S)$, which is hyperbolic.*

$$1 \to \mathbb{Z} \to < a, b, c, d, z \mid [a, b][c, d] = z^{-2}, z \text{ central} > \to < a, b, c, d \mid [a, b][c, d] = 1 > \to 1$$

Let x be a variable. The equation $[a, b][x, d] = 1$ has no solution in $\pi_1(T^1S)$ but its projection in $\pi_1(S)$ has infinitely many solutions: $x = cd^n$ for all $n \in \mathbb{Z}$. To see this, first solve $[a, b][x, d] = 1$ in $\pi_1(S)$, where we have $[a, b][x, d] = [a, b][c, d]$. By simply algebraic manipulation, we got $x^{-1}cd = dx^{-1}c$. But in $\pi_1(S)$, the only elements that commute with d are of the form d^n for $n \in \mathbb{Z}$. Hence we have that $x = cd^n$ for all $n \in \mathbb{Z}$ are the only solutions. Now any solution of $[a, b][x, d] = 1$ in $\pi_1(T^1S)$ must project down to a solution of its projection in $\pi_1(S)$. Hence if there is a solution, then it has the form $x = cd^n z^m$. Plug it into x, we have $[a, b][c, d] = 1$, which does not hold in $\pi_1(T^1(S))$. Therefore $[a, b][x, d] = 1$ has no solution in $\pi_1(T^1(S))$.

To deal with the above problem, we use rational constraints.

For each $\mathcal{F}_R(\bar{c})$ we will have finitely many ways to add more rational constraints to it. We denote the resulting equation systems with rational constraints by $\mathcal{F}_R^k(\bar{c})$. We will prove the following:

1. If $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ is solution of $\mathcal{F}_R(\bar{c})$ then it is a solution of $\mathcal{F}_R^k(\bar{c})$ for some k.

2. If $\{\bar{v}_{i,j}, \bar{p}_{i,j}\}$ and $\{\bar{v}'_{i,j}, \bar{p}'_{i,j}\}$ are solutions of $\mathcal{F}_R^k(\bar{c})$, then we have

$$s(\pi(\bar{v}_{i,1}))s(\pi(\bar{v}_{i,2}))s(\pi(\bar{v}_{i,3})) = s(\pi(\bar{v}'_{i,1}))s(\pi(\bar{v}'_{i,2}))s(\pi(\bar{v}'_{i,3}))$$

and one can compute this value from the rational constraints in $\mathcal{F}_R^k(\bar{c})$. We denote the above value by $s(\bar{c}, k)$.

Now instead of solving possibly infinitely many equation systems $\mathcal{W}(\bar{c}, \bar{v}_{i,j}, \bar{p}_{i,j})$, we only need to solve, for each $\bar{c}$ and k, the corresponding pair of equation systems $\mathcal{F}_R^k(\bar{c})$ and

$$\mathcal{W}^k(\bar{c}) = \{w_{i,1}w_{i,2}w_{i,3} = -s(\bar{c}, k) \mid 1 \leq i \leq n\}.$$

By (1), (2) we have that $\mathcal{E}$ has a solution in E if and only if $\mathcal{F}_R^k(\bar{c})$ has a solution in V and $\mathcal{W}^k(\bar{c})$ has a solution in A for some $\bar{c}$ and k.

Since there are finitely many tuples $\bar{c}$ and for each $\bar{c}$ there are finitely many k, there are finitely many pairs of $\mathcal{F}_R^k(\bar{c})$ and $\mathcal{W}^k(\bar{c})$. So any equation system in E can be reduced to finitely many equation systems with rational constraints in V and finitely many equation systems in A. Therefore we know that the Equation Problem in central extensions of hyperbolic groups is solvable.

To define the rational constraints in $\mathcal{F}_R^k(\bar{c})$ we need tools from (12), which we recall in the next section.

2.3 Central extensions of hyperbolic groups

In this section, we recall some definitions and facts from (12). We include the proofs of some of these facts since they are not in (12).

Recall that K_Γ is the Cayley graph of Γ with respect to X. Denote by L the language (over X) of all (λ, ν)-quasi-geodesic words in K_Γ. Everything in this section works for any fixed λ and ν, but in the next chapter we will fix a specific pair (λ, ν). Note that L is regular (See (6)). Let N a finite-state automaton accepting L. Then L is an asynchronous biautomatic structure of Γ (See (5) and (11)).

Definition 5 (L-rational)**.** *Let $\pi : X^* \to \Gamma$ be the canonical projection. A subset T of Γ is called* L-rational *if the language $\{w \in L \mid \pi(w) \in T\}$ is regular.*

Let $s : \Gamma \to E$ be a section and $\sigma_s : \Gamma \times \Gamma \to A$ be the cocycle defined by s.

Definition 6. *The cocycle σ_s is* L-regular *if*

1. *The sets $\sigma_s(g, \Gamma)$ and $\sigma_s(\Gamma, g)$ are finite for each $g \in \Gamma$.*
2. *For each $h \in \Gamma$ and $a \in A$ the subset $\{g \in \Gamma \mid \sigma_s(g, h) = a\}$ is an L-rational subset of Γ.*

Theorem 4 (Neumann-Reeves)**.** *For any central extensions of hyperbolic groups E defined by $1 \to A \to E \to \Gamma \to 1$, there exists a section $\rho : \Gamma \to E$ such that σ_ρ is L-regular, where L is any biautomatic structure of Γ.*

In (12) the above theorem is proved for a specific biautomatic structure of L. (In (12), L is the language of maximising words. See (12, Lemma 2.1) for more detail. But then the above theorem follows easily by applying (11, Proposition 1.1).

Remark 1. *Note that given a presentation of E, the L-rational structure of $\{g \in \Gamma \mid \sigma_\rho(g,h) = a\}$ can be computed (i.e. a finite state automaton which accepts all L-words representing elements of $\{g \in \Gamma \mid \sigma_\rho(g,h) = a\}$ can be constructed explicitly). One can see this by examining the proof of the above theorem from (12) and using the fact that any finite balls of the Cayley graphs of E and Γ can be constructed.*

Let $\rho : \Gamma \to E$ be a section such that σ_ρ is L-regular. Hence we know that $\{g \in \Gamma \mid \sigma_\rho(g,x) = a\}$ is L-rational for $x \in X$ and $a \in A$. We also need the fact that $\{g \in \Gamma \mid \sigma_\rho(x,g) = a\}$ is L-rational for $x \in X$ and $a \in A$. Since (12) doesn't include a proof, we give a proof.

Lemma 3. *$\{g \in \Gamma \mid \sigma_\rho(x,g) = a\}$ is L-rational for $x \in X$ and $a \in A$.*

Proof. Consider the finite subset $D = \{\rho(x)i(-\sigma_\rho(g,x)) \mid g \in \Gamma, x \in X\}^{\pm 1}$ of E as in (11, Proposition 2.2). If $w = x_1 \cdots x_n \in X^*$ then there exists $w' \in D^*$ whose initial segments have values $\rho(x_1), \rho(x_1x_2), \cdots, \rho(x_1 \cdots x_n)$. Let L' be the language $L' = \{w' \mid w \in L\}$. Then by (11, Proposition 2.2) L' is a regular language. Let Z be a generating set for A. It is easy to see that $D \cup i(Z)$ is a generating set of E. Let K_E be the Cayley graph of E with respect to $D \cup i(Z)$.

For $x \in X$ and $a \in A$ consider the set $F = \{(w_1, w_2) \in L' \times L' \mid \rho(x)w_1 = w_2 i(a)\}$. Since L is a biautomatic structure on Γ, we can apply (11, Proposition 2.2) and see that there exist K such that w_1 and w_2 K-fellow-travel in K_E if $(w_1, w_2) \in F$. Hence F is the language of a two-tape finite state automata. Therefore $F_1 = \{w_1 \in L' \mid \exists w_2 \in L', \rho(x)w_1 = w_2 i(a)\}$, which is the projection of F to the first factor, is regular. Let $F_1' = \{v \in L \mid \sigma_\rho(x,v) = a\}$. One can use the finite-state automaton accepting F_1 to read words in L and F_1' is the language

accepted by it. Therefore F_1' is regular, which is equivalent to $\{g \in \Gamma \mid \sigma_\rho(x, g) = a\}$ being L-rational. □

Convention 5 (s-coordinates)**.** *For any section $s : \Gamma \to E$ and any $g \in \Gamma$, $a \in A$, we denote by $(g, a)_s$ the element $s(g)i(a)$ in E and call (g, a) the* s-coordinates *of $s(g)i(a)$. For simplicity we omit the subscript when the section under consideration is clear.*

We will use a symmetric section to lift the solutions of $\mathcal{E}$ in Γ to E. The symmetric section q associated to ρ lands in an extension of E, which we now define.

Since A is finitely generated and abelian, it is isomorphic to $\mathbb{Z}^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$. We identify A with $\mathbb{Z}^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$ by fixing an isomorphism between them. Let $A' = \mathbb{Z}^n \oplus \mathbb{Z}_{2d_1} \oplus \cdots \oplus \mathbb{Z}_{2d_m}$.

Let ι_1 be the injective homomorphism from A to A' defined by

$$\iota_1(a_1, \cdots, a_n, b_1, \cdots, b_m) = (2a_1, \cdots, 2a_n, 2b_1, \cdots, 2b_m).$$

This map determines a pushout extension $1 \to A' \to E' \to \Gamma \to 1$ in the following sense: Let $E' = \Gamma \times A'$ be the direct product of Γ and A' as sets. The map from A' to E' is the inclusion from A' to $\{1\} \times A'$ and the map from E' to Γ is the projection of E' to the first factor. Make E' into a group by defining

$$(g_1, a_1)(g_2, a_2) = (g_1 g_2, a_1 + a_2 + \iota_1(\sigma_\rho(g_1, g_2))).$$

Let ι_2 denote the natural inclusion from E to E', which maps (g, a) to $(g, \iota_1(a))_\rho$. Let ρ' be the section from Γ to E' defined by $\rho' = \iota_2\rho$. Hence an element (g, a') in E' has ρ'-coordinates (g, a') and we have $\sigma_{\rho'}(g, h) = \iota_1(\sigma_\rho(g, h))$ for any $g, h \in \Gamma$.

Convention 6. *Let ι_3 be the map (not a homomorphism) from A to A' defined by*

$$\iota_3(a_1, \cdots, a_n, b_1, \cdots, b_m) = (a_1, \cdots, a_n, b_1, \cdots, b_m).$$

To simplify notation, in the rest of the paper, if $\sigma_\rho(-,-)$ appears in the second component of the ρ'-coordinates of an element in E', it represents the element $\iota_3(\sigma_\rho(-,-))$ in A'.

Definition 7. *The* symmetric section $q : \Gamma \to E'$ *is defined by:*

$$q(g) = (g, -\sigma_\rho(g, g^{-1}))$$

in ρ'-coordinate of E'.

Lemma 4. *q is symmetric, i.e., $q(g)q(g^{-1}) = 1$.*

Proof. In ρ'-coordinates of E' we have

$$\begin{aligned} q(g)q(g^{-1}) &= (g, -\sigma_\rho(g, g^{-1}))(g^{-1}, -\sigma_\rho(g^{-1}, g)) \\ &= (1, -\sigma_\rho(g, g^{-1}) - \sigma_\rho(g^{-1}, g) + 2\sigma_\rho(g, g^{-1})) \\ &= (1, \sigma_\rho(g, g^{-1}) - \sigma_\rho(g^{-1}, g)) \end{aligned}$$

One the other hand, in ρ-coordinate of E we have

$$(g,0)(g^{-1},-\sigma_\rho(g,g^{-1})) = (1,-\sigma_\rho(g,g^{-1})+\sigma_\rho(g,g^{-1})) = (1,0).$$

Hence $(g^{-1},-\sigma_\rho(g,g^{-1}))$ is the inverse of $(g,0)$. So we have

$$(1,0) = (g^{-1},-\sigma_\rho(g,g^{-1}))(g,0) = (1,-\sigma_\rho(g,g^{-1})+\sigma_\rho(g^{-1},g)).$$

Therefore we have $-\sigma_\rho(g,g^{-1})+\sigma_\rho(g^{-1},g) = 0$. So we know

$$q(g)q(g^{-1}) = (1,\sigma_\rho(g,g^{-1})-\sigma_\rho(g^{-1},g)) = (1,0).$$

□

Let σ_q be the cocycle corresponding to q.

Lemma 5. *σ_q is L-regular.*

Proof. Let $x \in X$ and $g \in \Gamma$. In the ρ'-coordinate we have

$$\begin{aligned} q(g)q(x) &= (g,-\sigma_\rho(g,g^{-1}))(x,-\sigma_\rho(x,x^{-1})) \\ &= (gx,-\sigma_\rho(g,g^{-1})-\sigma_\rho(x,x^{-1})+2\sigma_\rho(g,x)) \end{aligned}$$

On the other hand, we have $q(gx) = (gx, -\sigma_\rho(gx, (gx)^{-1}))$. Therefore we have

$$\begin{aligned}
\sigma_q(g,x) &= \sigma_\rho(gx,(gx)^{-1}) - \sigma_\rho(g,g^{-1}) - \sigma_\rho(x,x^{-1}) + 2\sigma_\rho(g,x) \\
&= \sigma_\rho(g,g^{-1}) - \sigma_\rho(g,x) - \sigma_\rho(x^{-1},g^{-1}) + \sigma_\rho(x,x^{-1}) \\
&\quad -\sigma_\rho(g,g^{-1}) - \sigma_\rho(x,x^{-1}) + 2\sigma_\rho(g,x) \\
&= \sigma_\rho(g,x) - \sigma_\rho(x^{-1},g^{-1}).
\end{aligned}$$

From the above equation we know that $\sigma_q(\Gamma, x)$ is finite since both $\sigma_\rho(\Gamma, x)$ and $\sigma_\rho(x^{-1}, \Gamma)$ are finite. Similarly, one can show that $\sigma_q(x, \Gamma)$ is finite. Let $a \in A'$. From the above computation we have

$$\begin{aligned}
&\{g \in \Gamma \mid \sigma_q(g,x) = a\} \\
= &\bigcup_{a_1 - a_2 = a} (\{g \in \Gamma \mid \sigma_\rho(g,x) = a_1\} \cap \{g \in \Gamma \mid \sigma_\rho(x^{-1},g^{-1}) = a_2\})
\end{aligned}$$

Since σ_ρ is L-regular, the left side of the above equation is a finite union and $\{g \in \Gamma \mid \sigma_\rho(g,x) = a_1\}$ is an L-rational set. By Lemma 3.1 and the fact that the reverse of a regular language is a regular language, $\{g \in \Gamma \mid \sigma_\rho(x^{-1}, g^{-1}) = a_2\}$ is a L-rational set. Therefore $\{g \in \Gamma \mid \sigma_q(g,x) = a\}$ is L-rational; so σ_q is regular. □

Lemma 6. *$\{g \in \Gamma \mid \sigma_q(x,g) = a\}$ is L-rational for $x \in X$ and $a \in A'$.*

Proof. Reverse the roles of g and x in the proof of the last lemma. □

CHAPTER 3

FUTURE PREDICTING AUTOMATA AND PARITY PREDICTING AUTOMATA

In this chapter we define the Future Predicting Automata and Parity Predicting Automata. They allow us to define the rational constraints we put on the variables of the tripod equation systems in V.

3.1 Lifting rational constraints to V

Both Future Predicting Automata and Parity Predicting Automata define rational subsets of Γ. We explain how to lift these rational subsets to V first. This allows us to determine and fix the constants λ and ν which define L.

Recall that Y is a finite generating set of V. We define a morphism ϕ from Y^* to X^* to lift rational constraints to V.

By Lemma 2 we know each $y \in Y$ as explicit path in $\mathcal{K}$. For each $y \in Y$ we choose and fix a K_Γ-geodesic word w_y representing $\pi(y)$. Let $\phi : Y^* \to X^*$ be the monoid homomorphism induced by the map from Y to X^* sending y to w_y. For any regular language $K \subset X^*$, it is a standard fact that $\phi^{-1}(K) = \{w \in Y^* | \phi(w) \in K\}$ is a regular language over Y. (See (7) Theorem 4.2.4 for a proof.) Let $\mathcal{QG}(V)$ be as in Definition 3.

Lemma 7. *There exist λ, ν depending only on Γ such that the following is true: For any $v \in \mathcal{QG}(V)$, there exists $w \in Y^*$ representing v such that $\phi(w)$ represents a (λ, ν)-quasi-geodesics in K_Γ.*

Proof. For any adjacent vertices $s, t \in \mathcal{K}$, let $[s, t]$ denote the unique edge between them. If $s = t$, let $[s, t]$ be s considered as a constant path.

Suppose the length of v (considered as a path in $\mathcal{K}$) is n. Let $s_0, \cdots, s_n$ be the vertices along v. By the construction of $\mathcal{K}$, there are two types of vertices in $\mathcal{K}$: vertices of K_Γ and barycenters. If s_i is a barycenter of some simplex of $R_{50\delta}(K_\Gamma)$, let s_i' be a vertex of this simplex. If s_i is a vertex of K_Γ, let $s_i' = s_i$. Then $s_0', \cdots, s_n'$ determine a path v' in $\mathcal{K}$. Here the path between s_{i-1}' and s_i' consists of the edges $[s_{i-1}', s_{i-1}]$, $[s_{i-1}, s_i]$ and $[s_i, s_i']$ and we denote this path by $[s_{i-1}', s_i']$. Note that v' equals v in V.

Since s_i' is a vertex in K_Γ, it also represent an element of Γ. Let $v_i = (s_{i-1}')^{-1}[s_{i-1}', s_i']$. Then v_i are element of V and $v = v' = v_1 \cdots v_n$.

For each v_i, pick a Y-geodesic word w_i representing v_i. Let $w = w_1 \cdots w_n$. Then w is a Y-word representing v. Since there are finitely many elements of V of length less than four, there is an upper bound K_1 on the length of w_i. Here K_1 depends only on Γ. Hence w has length at most nK_1.

There is an upper bound K_2 depending only on Γ on the length of $\phi(y)$ for all $y \in Y$ since Y is finite. Let n' be the length of $\phi(w)$. Then we have

$$n' \leq nK_1K_2$$

Let d be the distance in $\mathcal{K}$ between the end points of v. Let d_X be the distance in K_Γ between the end points of v.

Since $\mathcal{K}$ is quasi-isometric to K_Γ, we have

$$\frac{1}{K_0}d - C \leq d_X$$

for some K_0 and C depending only on Γ.

We know that v is a (λ_1, ν_1)-quasi-geodesic in $\mathcal{K}$ since $v \in \mathcal{QG}(V)$, hence we have

$$\frac{1}{\lambda_1}n - \nu_1 \leq d.$$

From the three equations above, we have

$$\frac{1}{K_0 K_1 K_2 \lambda_1}n' - \nu_1 - C \leq d_X.$$

Let $\lambda = K_0 K_1 K_2 \lambda_1$ and $\nu = \nu_1 + C$. Then the above equation implies that $\phi(w)$ is a (λ, ν)-quasi-geodesics in K_Γ. Note that (λ, ν) depends only on Γ. □

3.2 Future Predicting Automata

We are now ready to define the Future Predicting Automata. We will first define the Future Predicting Automaton, which accepts exactly the language L. The Future Predicting Automaton has many accepting states. The languages defined by each of these accepting states

give a partition of L and these subsets of L will be used to define the rational constraints we need in the next chapter.

For the rest of the paper, we use L to denote the regular language of words over X representing (λ, ν)-quasi-geodesic in K_Γ , where λ and ν are given by Lemma 7.

By Lemma 5 $\{g \in \Gamma \mid \sigma_q(g, x) = a\}$ is L-rational for $x \in X$, $a \in A'$ and

$$A_x = \{\sigma_q(g, x) \in A' \mid g \in \Gamma\}.$$

is finite. For each $x \in X$, $a \in A_x$ we choose and fix a finite state automaton $M_{x,a}$ which accepts exactly the L-words representing elements in $\{g \in \Gamma \mid \sigma_q(g, x) = a\}$. Denote the set of states and the transition map of $M_{x,a}$ by $S_{x,a}$ and $F_{x,a}$, respectively.

Definition 8 (FPA)**.** *The* Future Predicting Automaton*, denoted by M, is defined as follows:*

States: $S = \prod_{x \in X, a \in A_x} S_{x,a}$.

Transition function: $F : S \times X \to S$ *is defined by*

$$F\Big((s_{x,a})_{x \in X, a \in A_x}, x'\Big) = \big(F_{x,a}(s_{x,a}, x')\big)_{x \in X, a \in A_x}.$$

Initial state: $(I_{x,a})_{x \in X, a \in A_x}$*, where* $I_{x,a}$ *is the initial state of* $M_{x,a}$.

Accepting state: The set of accepting states T *consists of states* $(s_{x,a})_{x \in X, a \in A_x} \in S$ *satisfying: for all* $x' \in X$ *there exists a unique* $a' \in A_{x'}$ *such that* $s_{x',a'}$ *is an accepting state of* $M_{x',a'}$.

Remark 2. *Note that M has finitely many states since X, A_x and $S_{x,a}$ are finite for all $x \in X$, $a \in A_x$.*

Lemma 8. *The language accepted by the Future Predicting Automaton is L.*

Proof. Suppose w is accepted by M. Then w ends up in a state in T. By the definition of T, for any $x \in X$, there exists a unique $a \in A_x$, such that $s_{x,a}$ is an accepting state of $M_{x,a}$. This together with the definition of M implies that w is accepted by $M_{x,a}$. Then by the definition of $M_{x,a}$, we know that w is an L-word representing an element in $\{g \in \Gamma \mid \sigma_q(g,x) = a\}$. In particular, w is in L.

Now suppose w is in L. Use M to read w. Suppose it ends at the state $(s_{x,a})_{x\in X, a\in A_x}$. Note that $s_{x,a}$ is an accepting state of $M_{x,a}$ if and only if we have $\sigma_q(w,x) = a$, where w is interpreted as the element of Γ it represents. Hence for each $x' \in X$, there is a unique $a' \in A_{x'}$ such that $s_{x',a'}$ is an accepting state of $M_{x',a'}$. Therefore $(s_{x,a})_{x\in X, a\in A_x}$ is in T. So w is accepted by M. □

Definition 9. *Let $\bar{s} = (s_{x,a}) \in T$. The* Future Predicting Automaton *associated with $\bar{s}$, denoted by $M(\bar{s})$, is the finite state automaton having the same states, transition function and initial state as the Future Predicting Automaton M, but $\bar{s}$ as the only accepting state.*

Let $L(\bar{s})$ be the regular language over X accepted by $M(\bar{s})$. The following fact is obvious from the definition and Lemma 8.

Lemma 9. *$\{L(\bar{s}) \mid \bar{s} \in T\}$ is a finite partition of L.*

For any $\bar{s} \in T$, let $M_{\bar{s}}$ be the finite state automaton which has the same states, transition map and accepting states as M, but has $\bar{s}$ as the initial state. Note that $M_{\bar{s}}$ is different from $M(\bar{s})$.

Definition 10. *A word $v \in X^*$ is* compatible *with $\bar{s} \in T$ if v is accepted by $M_{\bar{s}}$.*

Note that v is compatible with $\bar{s}$ simply means that for any $w \in L(\bar{s})$, the word wv is in L (or equivalently accepted by M). The following fact is clear from Definition 10.

Lemma 10. *For any $\bar{s} \in T$, the language of all words compatible with $\bar{s}$ is regular.*

Convention 7. *We interpret any $w \in X^*$ as the element of Γ represented by the word w when any cocycle is applied to w.*

The next lemma is the key property of the Future Predicting Automata.

Proposition 2. *Suppose that $w_1, w_2 \in L(\bar{s})$. Then $\sigma_q(w_1, v) = \sigma_q(w_2, v)$ provided $v \in X^*$ is compatible with $\bar{s} \in T$.*

Proof. Let $v = x_1 x_2 \cdots x_l$. We argue by induction on l.

Suppose $l = 1$. Since $w_1, w_2 \in L(\bar{s})$, they both end at the same state of $M(\bar{s})$. Hence for $a \in A_{x_1}$, we have that w_1 and w_2, when read by $M_{x_1,a}$, end up in the same states. By the definition of FPA there exists a unique $a_1 \in A_{x_1}$ such that M_{x_1,a_1} accepts both w_1 and w_2. Therefore by the definition of M_{x_1,a_1}, we have $\sigma_q(w_1, x_1) = \sigma_q(w_2, x_1) = a_1$.

By the cocycle condition of σ_q, for $i = 1, 2$ we have

$$\sigma_q(w_i, x_1 x_2 \cdots x_l) = \sigma_q(w_i, x_1 x_2 \cdots x_{l-1}) + \sigma_q(w_i x_1 x_2 \cdots x_{l-1}, x_l) - \sigma_q(x_1 x_2 \cdots x_{l-1}, x_l)$$

By induction the first term does not depend on i. The third term clearly does not depend on i. Showing that the second term does not depend on i will complete the proof.

Since $\bar{s}$ and v are compatible, we have that $w_i v = w_i x_1 x_2 \cdots x_l$ is in L. Therefore we know that $w_i x_1 x_2 \cdots x_{l-1}$ is in L for $i = 1, 2$ since L is closed under taking subword. In fact both $w_1 x_1 x_2 \cdots x_{l-1}$ and $w_2 x_1 x_2 \cdots x_{l-1}$ end up in the same accepting state when read by M since that is true for w_1 and w_2. So there exists a unique $a_l \in A_{x_l}$ such that M_{x_l,a_l} accepts $w_i x_1 x_2 \cdots x_{l-1}$ for $i = 1, 2$. Hence $\sigma_q(w_i x_1 x_2 \cdots x_{l-1}, x_l) = a_l$, which does not depend on i. □

The above lemma explains the name "Future Predicting Automaton" since all we need to know to "predict" the value of $\sigma_q(w, v)$ is where w ends when read by the Future Predicting Automaton. By Proposition 2 the following definition makes sense.

Definition 11. *Let $\bar{s} \in T$ and $v \in X^*$. Suppose $\bar{s}$ and v are compatible. Define $\sigma_q(\bar{s}, v)$ to be $\sigma_q(w, v)$ for any $w \in L(\bar{s})$.*

3.3 Parity Predicting Automata

Recall that $q : \Gamma \to E'$ is the symmetric section (Definition 7). We are lifting solutions of equation system in Γ by q. We need to define appropriate rational constraints on variables of the Tripod Equation systems so that we can predict whether their lifts land in E or not. The Parity Predicting Automata define these rational constraints.

We first define the Left Future Predicting Automaton(LFPA) and the Right Future Predicting Automaton(RFPA), which we will use to define the Parity Predicting Automaton.

Let ρ be the section given by Theorem 4. Hence we know that $\{g \in \Gamma \mid \sigma_\rho(g, x) = a\}$ is L-rational for all $x \in X$ and $a \in A$ and $A_x^1 = \{\sigma_\rho(g, x) \mid g \in \Gamma\}$ is finite.

For each $x \in X$ and $a \in A^1_x$ choose and fix a finite state automaton $M^1_{x,a}$ which accepts exactly the L-words representing elements in $\{g \in \Gamma \mid \sigma_\rho(g,x) = a\}$. Denote by $S^1_{x,a}$ and $F^1_{x,a}$ the set of states and the transition function of $M^1_{x,a}$, respectively.

The following definition is almost the same as the definition of the Future Predicting Automaton M, except that we are now considering the section ρ instead of q.

Definition 12. *The* Left Future Predicting Automaton M_1 *over* X *is defined as follows:*

States: $S_1 = \prod_{x\in X, a\in A^1_x} S^1_{x,a}$

Transition function: $F_1 : S_1 \times X \to S_1$ *is defined by*

$$F_1\big((s^1_{x,a})_{x\in X,a\in A^1_x}, x'\big) = \big(F^1_{x,a}(s^1_{x,a}, x')\big)_{x\in X,a\in A^1_x}.$$

.

Initial state: $(I^1_{x,a})_{x\in X,a\in A^1_x}$, *where* $I^1_{x,a}$ *is the initial states of* $M^1_{x,a}$.

Accepting states: The set of accepting states T_1 *consists of states* $(s^1_{x,a})_{x\in X,a\in A^1_x}$ *satisfying: for all* $x' \in X$ *there exists a unique* $a' \in A^1_{x'}$ *such that* $s^1_{x',a'}$ *is the accepting state of* $M^1_{x',a'}$.

One can prove the following lemma the same way as we prove Lemma 8

Lemma 11. *The language accepted by* M_1 *is* L.

Definition 13. *Suppose* $\bar{s}_1 = (s^1_{x,a})_{x\in X,a\in A^1_x}$ *is an accepting state of* M_1. *For any* $x' \in X$, *define* $\sigma_\rho(\bar{s}_1, x') = a'$, *where* a' *is the unique element of* $A^1_{x'}$ *such that* $s^1_{x',a'}$ *is the accepting state of* $M^1_{x',a'}$.

The next lemma follows directly from the above definition and the definition of $M^1_{x,a}$.

Lemma 12. *Suppose $w \in X^*$ ends up in the state $\bar{s}_1 \in T_1$ when read by M_1. Then $\sigma_\rho(w, x) = \sigma_\rho(\bar{s}_1, x)$*

By Lemma 3 the set of all the L-words representing elements in $\{g \in \Gamma \mid \sigma_\rho(x, g) = a\}$ is a regular language. Hence its reverse is also a regular language. Let $M^2_{x,a}$ be the finite state automaton accepting the reverse language. Let $S^2_{x,a}$ and $F^2_{x,a}$ be the set of states and the transition function of $M^2_{x,a}$, respectively. Let $A^2_x = \{\sigma_\rho(x, g) \mid g \in \Gamma\}$. Note that A^2_x is finite by Theorem 4.

Definition 14. *The* Right Future Predicting Automaton M_2 *over X is defined as follows:*

States: $S_2 = \prod_{x\in X, a\in A^2_x} S^2_{x,a}$.

Transition function: $F_2 : S_2 \times X \to S_2$ *is defined as follow:*

$$F_2\big((s^2_{x,a})_{x\in X,a\in A^2_x}, x'\big) = \big(F^2_{x,a}(s^2_{x,a}, (x')^{-1})\big)_{x\in X,a\in A^2_x}.$$

Initial state: $(I^2_{x,a})_{x\in X,a\in A^2_x}$, *where $I^2_{x,a}$ is the initial states of $M^2_{x,a}$.*

Accepting states: The set of accepting states T_2 consists of states $(s^2_{x,a})_{x\in X,a\in A^2_x}$ satisfying that for all $x' \in X$ there exists a unique $a' \in A^2_{x'}$ such that $s^2_{x',a'}$ is the accepting state of $M^2_{x',a'}$.

One can prove the following lemma the same way as we prove Lemma 8

Lemma 13. *The language accepted by M_2 is*

$$L^{-1} = \{w^{-1} = w_n^{-1} \cdots w_1^{-1} \mid w = w_1 \cdots w_n \in L\}.$$

Definition 15. *Suppose* $\bar{s}_2 = (s^2_{x,a})_{x\in X, a\in A^2_x}$ *is an accepting state of* M_2*. Define* $\sigma_\rho(x', \bar{s}_2) = a'$*, where* a' *is the unique element of* $A^1_{x'}$ *such that* $s^1_{x',a'}$ *is the accepting state of* $M^1_{x',a'}$*.*

The next lemma follows directly from the above definition and the definition of $M^2_{x,a}$.

Lemma 14. *Suppose* $w \in X^*$ *ends up in the state* $\bar{s}_2 \in T_2$ *when read by* M_2*. Then* $\sigma_\rho(x, w^{-1}) = \sigma_\rho(x, \bar{s}_2)$

We now define a homomorphism Pa, which makes what we mean by "parity" precise. Denote the natural project from $\mathbb{Z}$ to $\mathbb{Z}_2$ by P_2. Recall that the finite generated abelian group A central in E is identified with $\mathbb{Z}^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$. The homomorphism $Pa : A \to \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$ is defined by

$$Pa(a_1, \cdots, a_n, b_1, \cdots, b_m) = (P_2(a_1), \cdots, P_2(a_n), b_1, \cdots, b_m).$$

The *parity* of an element $a \in A$ is define to be $Pa(a)$.

Let $a \in A$. Recall that ι_3 and ι_1 are defined in Convention 6 and the paragraph before it, respectively. In general $\iota_3(a)$ does not lie in $\iota_1(A)$. However once we know the parity of a, we can use it to "move" $\iota_3(a)$ to something in $\iota_1(A)$. We now make this precise: Define the map (not a homomorphism) $\iota_4 : \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m} \to A' = \mathbb{Z}^n \oplus \mathbb{Z}_{2d_1} \oplus \cdots \oplus \mathbb{Z}_{2d_m}$ by

$$(a_1, \cdots, a_n, b_1, \cdots, b_m) = (a_1, \cdots, a_n, b_1, \cdots, b_m)$$

Then the following fact is clear.

Lemma 15. *For any $a \in A$, we have $\iota_3(a) + \iota_4(Pa(a)) \in \iota_1(A)$.*

Now we define the Parity Predicting Automaton.

Definition 16 (PPA)**.** *The* Parity Predicting Automaton*, denoted by D, is defined as follows:*

States: $S_D = S_1 \times S_2 \times (\mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}) \cup \{\emptyset\}$.

Transition functions: $F_D : S_D \times X \to S_D$ *is defined as follows:*

If $\bar{s}_1 \in T_1$ *and* $\bar{s}_2 \in T_2$*, then we define*

$$\begin{aligned} & F_D\Big((\bar{s}_1, \bar{s}_2, b), x\Big) \\ = \quad & \Big(F_1(\bar{s}_1, x), F_2(\bar{s}_2, x), b'\Big), \end{aligned}$$

where

$$b' = b + Pa\Big(\sigma_\rho\big(x, x^{-1}\big) - \sigma_\rho\big(\bar{s}_1, x\big) - \sigma_\rho\big(x^{-1}, \bar{s}_2\big)\Big).$$

Otherwise we define

$$F_D\Big(\big(\bar{s}_1, \bar{s}_2, b\big), x\Big) = \emptyset.$$

For all $x \in X$, we define

$$F_D(\emptyset, x) = \emptyset.$$

The initial state: $(I_1, I_2, 0)$*. Here I_1 and I_2 are the initial states of M_1 and M_2 respectively.*

The accepting states: All states $(\bar{s}_1, \bar{s}_2, b)$ *so that* $\bar{s}_1 \in T_1$ *and* $\bar{s}_2 \in T_2$.

The following fact is clear from the above definition.

Lemma 16. *The language accepted by* D *is* L.

Definition 17. *Let* $d \in \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$. *The* Parity Predicting Automaton *associated to* d*, denoted by* $D(d)$*, is the same as the Parity Predicting Automaton with the extra requirement that the third component of any accepting state is* d.

Let $L(d)$ denote the regular language defined by $D(d)$.

Lemma 17. $\{L(d) \mid d \in \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}\}$ *is a finite partition of* L.

The following lemma is the key property of the Parity Predicting Automata.

Lemma 18. *Let* $w \in L(d)$. *Then* $Pa\big(\sigma_\rho(w, w^{-1})\big) = d$.

Proof. We proceed by induction on the length of w. The base case is when w has length 0. In this case, w is the identity. Hence $\sigma_\rho(w, w^{-1}) = 0$. Since D's initial state has 0 as its last component, the lemma is true in this case.

Suppose the lemma is true for words of length less then l. Let $w = x_1 \cdots x_l$. By the cocycle condition of σ_ρ we have

$$\begin{aligned}
\sigma_\rho(w, w^{-1}) &= \sigma_\rho(x_1 \cdots x_l, x_l^{-1} \cdots x_1^{-1}) \\
&= \sigma_\rho(x_1 \cdots x_l, x_l^{-1}) + \sigma_\rho(x_1 \cdots x_{l-1}, x_{l-1}^{-1} \cdots x_1^{-1}) \\
&\quad -\sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1}) \\
&= \sigma_\rho(x_1 \cdots x_{l-1}, 1) - \sigma_\rho(x_1 \cdots x_{l-1}, x_l) + \sigma_\rho(x_l, x_l^{-1}) \\
&\quad +\sigma_\rho(x_1 \cdots x_{l-1}, x_{l-1}^{-1} \cdots x_1^{-1}) - \sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1}) \\
&= \sigma_\rho(x_1 \cdots x_{l-1}, x_{l-1}^{-1} \cdots x_1^{-1}) + \sigma_\rho(x_l, x_l^{-1}) \\
&\quad -\sigma_\rho(x_1 \cdots x_{l-1}, x_l) - \sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1})
\end{aligned}$$

Suppose $x_1 \cdots x_{l-1}$ ends at a state $(\bar{s}_1, \bar{s}_2, b_{l-1})$. Note that $\bar{s}_1 \in T_1$ and $\bar{s}_2 \in T_2$ (otherwise w wouldn't be accepted by D). By the induction hypothesis, $Pa\big(\sigma_\rho(x_1 \cdots x_{l-1}, x_{l-1}^{-1} \cdots x_1^{-1})\big) = b_{l-1}$. Then by the equation above we have

$$\begin{aligned}
& Pa\big(\sigma_\rho(w, w^{-1})\big) \\
= \; & Pa\big(\sigma_\rho(x_1 \cdots x_{l-1}, x_{l-1}^{-1} \cdots x_1^{-1})\big) + \\
& Pa\big(\sigma_\rho(x_l, x_l^{-1}) - \sigma_\rho(x_1 \cdots x_{l-1}, x_l) - \sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1})\big) \\
= \; & b_{l-1} + Pa\big(\sigma_\rho(x_l, x_l^{-1}) - \sigma_\rho(x_1 - \cdots x_{l-1}, x_l) - \sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1})\big).
\end{aligned}$$

On the other hand, by the definition of D, $x_1 \cdots x_l$ ends at the state $\Big(F_1\big(\bar{s}_1, x_l\big), F_2\big(\bar{s}_2, x_l^{-1}\big), b\Big)$, where

$$b = b_{l-1} + Pa\big(\sigma_\rho(x_l, x_l^{-1}) - \sigma_\rho(\bar{s}_1, x_l) - \sigma_\rho(x_l^{-1}, \bar{s}_2)\big)$$

Therefore it is enough to show that

$$\sigma_\rho(x_1 \cdots x_{l-1}, x_l) = \sigma_\rho(\bar{s}_1, x_l)$$

and

$$\sigma_\rho(x_l^{-1}, x_{l-1}^{-1} \cdots x_1^{-1}) = \sigma_\rho(x_l^{-1}, \bar{s}_2).$$

Since $x_1 \cdots x_{l-1}$ ends at $(\bar{s}_1, \bar{s}_2, b_{l-1})$, we know that $x_1 \cdots x_{l-1}$ ends at $\bar{s}_1$ when read by M_1 and it ends at $\bar{s}_2$ when read by M_2. Hence by Lemma 12 and Lemma 14, the above two equations follow and the proof of the lemma is completed. □

CHAPTER 4

PROOF OF THEOREM 1

Let U be a finite set of variables and $C \subset E$ be a finite set of constants in E. Recall from Chapter 2 that it is enough to consider triangular equation systems. Let $\mathcal{E} = \{e_{i,1}e_{i,2}e_{i,3} = 1, i = 1, \cdots, n\}$ be a triangular equation system where $e_{i,j} \in U \cup C$.

Now we construct equation systems $\mathcal{V}_t$ over V and $\mathcal{W}_t$ over A where t runs over some finite set Θ. The size of Θ depends on $\mathcal{E}$ and Γ. Then we show that $\mathcal{E}$ has a solution in E if and only if there is some $t \in \Theta$ such that $\mathcal{V}_t$ has a solution in V and $\mathcal{W}_t$ has a solution in A.

First we describe the finite set Θ over which the subscript t of $\mathcal{V}_t$ and $\mathcal{W}_t$ runs. The index set Θ consists of tuples $\big((c_{i,j}), (\bar{s}_{i,j}), (b_{i,j}), (d_{i,j})\big)_{1 \le i \le n, 1 \le j \le 3}$ satisfying the following 4 conditions:

Recall that $V_{\le l}$ is the set of elements of V whose corresponding reduced path in $\mathcal{K}$ has length at most l. Let κ_1 be as in Proposition 1. There exists κ_2 such that all elements of $V_{\le \kappa_1}$ are represented by some Y-words of word length as most κ_2. Recall that ϕ is the monoid homomorphism from Y^* to X^* defined in the Section 3.1.

Condition 1: For each $1 \le i \le n$, $1 \le j \le 3$, $c_{i,j}$ is a Y-word of word length at most κ_2 and for each i we have $\pi(c_{i,1}c_{i,2}c_{i,3}) = 1$ in Γ.

Condition 2: For $1 \le i \le n$, $1 \le j \le 3$, $\bar{s}_{i,j} \in T$ is an accepting state of the Further Predicting Automaton so that $\bar{s}_{i,j}$ and $\phi(c_{i,j})$ are compatible.

Recall that for any $\bar{s} \in T$, $M_{\bar{s}}$ is the finite state automaton which has the same states, transition map and accepting states as M, but has $\bar{s}$ as the initial state. Let $\bar{s}'_{i,j}$ be where $\phi(c_{i,j})$ ends when read by $M_{\bar{s}_{i,j}}$. Denote the language of words in X that are compatible with $\bar{s}'_{i,j}$ by $L(\bar{s}_{i,j}, c_{i,j})$. Let $A(\bar{s}_{i,j}, c_{i,j}) = \{\sigma_q(\bar{s}'_{i,j}, w) \mid w \in L(\bar{s}_{i,j}, c_{i,j})\}$.

Condition 3: For all $1 \leq i \leq n$, $1 \leq j \leq 3$, $b_{i,j} \in A(\bar{s}_{i,j}, c_{i,j})$.

Condition 4: For all $1 \leq i \leq n$, $1 \leq j \leq 3$, $d_{i,j} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$.

Lemma 19. Θ *is finite.*

Proof. Since the lengths of $c_{i,j}$'s are bounded, there are finitely many tuples $(c_{i,j})$ satisfying Condition 1. We know that T is finite for it is the set of accepting states of a finite state automaton (FPA). Hence there are finitely many tuples $(\bar{s}_{i,j})$ satisfying Condition 2.

For each choice of $(c_{i,j})$ and $(\bar{s}_{i,j})$, note that $A(\bar{s}_{i,j}, c_{i,j}) = \{\sigma_q(u_{i,j}, w) \mid w \in L(\bar{s}_{i,j}, c_{i,j})\}$ for any $u_{i,j} \in L(\bar{s}'_{i,j})$. Hence $A(\bar{s}_{i,j}, c_{i,j})$ is finite by Lemma 5. Therefore there are finitely many choices for $(b_{i,j})$. At last, possibilities of $(d_{i,j})$ are bounded since $\mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$ is finite. □

For each $t = \big((c_{i,j}), (\bar{s}_{i,j}), (b_{i,j}), (\bar{d}_{i,j})\big)_{1 \leq i \leq n, 1 \leq j \leq 3}$ we have the following setups:

Let $L(\bar{s}_{i,j}) \subset X^*$ be the regular language associated to $\bar{s}_{i,j}$.

Let $L(b_{i,j}) = \{w \in L(\bar{s}_{i,j}, c_{i,j}) \mid \sigma_q(\bar{s}'_{i,j}, w) = b_{i,j}\}$.

Lemma 20. $L(b_{i,j})$ *is regular.*

Proof. Pick and fix $u_{i,j} \in L(\bar{s}'_{i,j})$. Note that $L(b_{i,j}) = \{w \in L \mid \sigma_q(u_{i,j}, w) = b_{i,j}\} \cap L(\bar{s}_{i,j}, c_{i,j})$. By Lemma 5 $\{w \in L \mid \sigma_q(u_{i,j}, w) = b_{i,j}\}$ is regular and $L(\bar{s}_{i,j}, c_{i,j})$ is regular by Lemma 10. Hence $L(b_{i,j})$ is a regular language. □

Let $L(d_{i,j}) \subset X^*$ be the regular language associated to $d_{i,j}$.

If $e_{i,j}$ is a constant in E, let $L(e_{i,j})$ denote the regular language of all L-representatives of $p(e_{i,j})$; otherwise, let $L(e_{i,j}) = L$.

Convention 8. *For any regular language K, we use $\phi^{-1}(K)$ to denote the rational subset of V defined by $\phi^{-1}(K) \subset Y^*$.*

We now define $\mathcal{V}_t$ as follows:

Let $\{v_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq 3\}$ be a set of variables such that $v_{i,j}$ and $v_{i',j'}$ are the same variable if and only if $e_{i,j}$ and $e_{i',j'}$ are the same. Let $P = \{p_{i,j} | 1 \leq i \leq n, 1 \leq j \leq 3\}$ be another set of distinct variables.

$$\mathcal{V}_t = \begin{cases} p_{i,1}c_{i,1}(p_{i,2})^{-1} = v_{i,1} & \\ p_{i,2}c_{i,2}(p_{i,3})^{-1} = v_{i,2} & \\ p_{i,3}c_{i,3}(p_{i,1})^{-1} = v_{i,3} & \\ \quad p_{i,j} \in \phi^{-1}(L(\bar{s}_{i,j})) & 1 \leq i \leq n; 1 \leq j \leq 3; 3+1=1 \\ p_{i,j+1}^{-1} \in \phi^{-1}(L(b_{i,j})) & \\ \quad v_{i,j} \in \phi^{-1}(L(d_{i,j})) & \\ \quad v_{i,j} \in \phi^{-1}(L(e_{i,j})) & \end{cases}$$

Let $a_{i,j} = \sigma_q(\bar{s}_{i,j}, \phi(c_{i,j}))$. Recall that $\pi : V \to \Gamma$ sends each $v \in V$ (which is a path in $\mathcal{K}$) to its terminal point.

Lemma 21. *Suppose $\{\tilde{v}_{i,j}, \tilde{p}_{i,j}\}$ is a solution of $\mathcal{V}_t$. The following are true:*

1. $\sigma_q\big(\pi(\tilde{p}_{i,j}), \pi(c_{i,j})\big) = a_{i,j}$;
2. $\sigma_q\big(\pi(\tilde{p}_{i,j}c_{i,j}), \pi((\tilde{p}_{i,j+1})^{-1})\big) = b_{i,j}$;
3. $Pa\Big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi((\tilde{v}_{i,j})^{-1})\big)\Big) = d_{i,j}$.
4. $\pi(\tilde{v}_{i,j}) = p(e_{i,j})$ *if* $e_{i,j}$ *is a constant.*

Proof. First note for $v_i \in V$ and $w_i \in Y^*$ represents v_i we have

$$\sigma_q\big(\pi(v_1), \pi(v_2)\big) = \sigma_q\big(\phi(w_1), \phi(w_2)\big).$$

Hence we can prove any statement about $\sigma_q\big(\pi(v_1), \pi(v_2)\big)$ by proving the same statement about $\sigma_q\big(\phi(w_1), \phi(w_2)\big)$

Since $\tilde{p}_{i,j} \in \phi^{-1}(L(\bar{s}_{i,j}))$, there exists $p'_{i,j} \in Y^*$ representing $\tilde{p}_{i,j}$ such that $\phi(p'_{i,j}) \in L(\bar{s}_{i,j})$. Hence by Lemma 2 and the definition of $a_{i,j}$, we have $\sigma_q\big(\phi(p'_{i,j}), \phi(c_{i,j})\big) = a_{i,j}$, which proves (1).

For (2), since $(\tilde{p}_{i,j+1})^{-1} \in \phi^{-1}(L(b_{i,j}))$, there exists $p'_{i,j+1} \in Y^*$ representing $\tilde{p}_{i,j+1}$ such that $\phi\big((p'_{i,j+1})^{-1}\big) \in L(b_{i,j})$. By the definition of $L(b_{i,j})$ we know that $\sigma_q\big(u_{i,j}, \phi((p'_{i,j+1})^{-1})\big) =$

$b_{i,j}$ and that $\phi\big((p'_{i,j+1})^{-1}\big)$ is compatible with $\bar{s}'_{i,j}$. We know that $\phi(p'_{i,j}c_{i,j}) \in L(\bar{s}'_{i,j})$ by the definition of $\bar{s}'_{i,j}$. We have $u_{i,j} \in L(\bar{s}'_{i,j})$. Hence by Proposition 2 we have

$$\sigma_q\big(\phi(p'_{i,j}c_{i,j}), \phi((p'_{i,j+1})^{-1})\big) = \sigma_q\big(u_{i,j}, \phi((p'_{i,j+1})^{-1})\big) = b_{i,j}$$

For (3), since $\tilde{v}_{i,j} \in \phi^{-1}(L(d_{i,j}))$, there exists $v'_{i,j} \in Y^*$ representing $\tilde{v}_{i,j}$ such that $\phi(v'_{i,j}) \in L(d_{i,j})$. Hence by Lemma 18 we have $Pa\Big(\sigma_\rho\big(\phi(v'_{i,j}), (\phi(v'_{i,j}))^{-1}\big)\Big) = d_{i,j}$.

(4) directly follows from the definition of $L(e_{i,j})$. □

We now define the equation system $\mathcal{W}_t$ in A correspond to $\mathcal{V}_t$.

Let $\{w_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq 3\}$ be a set of constants and variables satisfying the follows:

1. $w_{i,j} = w_{i',j'}$ if and only if $e_{i,j} = e_{i',j'}$.
2. If $e_{i,j}$ is a variable in $\mathcal{E}$, then $w_{i,j}$ is a variable in $\mathcal{W}_t$.
3. When $e_{i,j}$ is a constant in E, we define

$$w_{i,j} = \iota_1^{-1}\big(\iota_2(e_{i,j}) \cdot (qp(e_{i,j}))^{-1} \cdot \iota_4(d_{i,j})\big)$$

Note that in the last case $w_{i,j}$ may not be well defined since ι_1 is not surjective. If this happens, we define $\mathcal{W}_t$ to have no solution.

The equation system $\mathcal{W}_t$ over A is defined as follow:

$$\mathcal{W}_t = \Big\{ \ \textstyle\sum_{j=1}^{3} w_{i,j} = \iota_1^{-1}\Big(\sum_{j=1}^{3}(a_{i,j} + b_{i,j} + \iota_4(d_{i,j})) - \sigma_q\big(\pi(c_{i,1}), \pi(c_{i,2})\big)\Big); \ \ 1 \leq i \leq n$$

Note that the right hand sides of the equations above might not be well defined since ι_1 is not surjective. In that case, we define $\mathcal{W}_t$ to have no solution.

Theorem 9. *$\mathcal{E}$ has a solution in E if and only if $\mathcal{E}_t = \mathcal{V}_t \cup \mathcal{W}_t$ constructed above has a solution for some $t \in \Theta$.*

Proof. Suppose $\mathcal{E}_t$ has a solution for $t = \big((c_{i,j}), (\bar{s}_{i,j}), (b_{i,j}), (d_{i,j})\big)$, i.e. $\mathcal{V}_t$ has a solution in V and $\mathcal{W}_t$ has a solution in A. Let $\{\tilde{v}_{i,j}, \tilde{p}_{i,j}\}$ be a solution of $\mathcal{V}_t$ and $\{\tilde{w}_{i,j}\}$ be a solution of $\mathcal{W}_t$.

Recall that i is the inclusion from A' to E', ι_1 is embedding of A into A' and ι_2 is the embedding of E into E'. We will show that

$$\tilde{e}_{i,j} = q\big(\pi(\tilde{v}_{i,j})\big) i\big(\iota_1(\tilde{w}_{i,j}) - \iota_4(d_{i,j})\big)$$

is a solution of $\mathcal{E}$ in E'. Here we think of $\mathcal{E}$ as an equation system in E' by replacing all constants by their image under ι_2.

First note that $\tilde{e}_{i,j}$ has q-coordinates $\big(\pi(\tilde{v}_{i,j}), \iota_1(\tilde{w}_{i,j}) - \iota_4(d_{i,j})\big)$. By direct computation, we have:

$$\begin{aligned}
& \tilde{e}_{i,1}\tilde{e}_{i,2}\tilde{e}_{i,3} \\
= \;& \big(\pi(\tilde{v}_{i,1}), \iota_1(\tilde{w}_{i,1}) - \iota_4(d_{i,1})\big)\big(\pi(\tilde{v}_{i,2}), \iota_1(\tilde{w}_{i,2}) - \iota_4(d_{i,2})\big)\big(\pi(\tilde{v}_{i,3}), \iota_1(\tilde{w}_{i,3}) - \iota_4(d_{i,3})\big) \\
= \;& \big(\pi(\tilde{v}_{i,1})\pi(\tilde{v}_{i,2})\pi(\tilde{v}_{i,3}),\ \sigma_q(\pi(\tilde{v}_{i,1}), \pi(\tilde{v}_{i,2})) + \sigma_q(\pi(\tilde{v}_{i,1})\pi(\tilde{v}_{i,2}), \pi(\tilde{v}_{i,3})) + \sum_{j=1}^{3}(\iota_1(\tilde{w}_{i,j}) - \iota_4(d_{i,j}))\big) \qquad (1)
\end{aligned}$$

By the definition of $\mathcal{V}_t$ and the fact that $\{\tilde{v}_{i,j}\}$ is a solution of $\mathcal{V}_t$, we have $\pi(\tilde{v}_{i,1})\pi(\tilde{v}_{i,2})\pi(\tilde{v}_{i,3}) = 1$ in Γ .

Now we consider the second component of (1). The following claim reduces the first two terms into something we have control over.

Claim 1.

$$\begin{aligned} & \sigma_q(\pi(\tilde{v}_{i,1}), \pi(\tilde{v}_{i,2})) + \sigma_q(\pi(\tilde{v}_{i,1})\pi(\tilde{v}_{i,2}), \pi(\tilde{v}_{i,3})) \\ = \quad & \sigma_q(\pi(c_{i,1}), \pi(c_{i,2})) - \sum_{j=1}^{3} \sigma_q(\pi(\tilde{p}_{i,j}), \pi(c_{i,j})) - \sum_{j=1}^{3} \sigma_q(\pi(\tilde{p}_{i,j})\pi(c_{i,j}), \pi(\tilde{p}_{i,j+1})^{-1}) \end{aligned}$$

Proof. Since $\{\tilde{v}_{i,j}, \tilde{p}_{i,j}\}$ is a solution of $\mathcal{V}_t$. We have

$$\begin{cases} \tilde{p}_{i,1}c_{i,1}(\tilde{p}_{i,2})^{-1} = \tilde{v}_{i,1} \\ \tilde{p}_{i,2}c_{i,2}(\tilde{p}_{i,3})^{-1} = \tilde{v}_{i,2} \qquad 1 \leq i \leq n \\ \tilde{p}_{i,3}c_{i,3}(\tilde{p}_{i,1})^{-1} = \tilde{v}_{i,3} \end{cases}$$

Project these equations to Γ by π, we have

$$\begin{cases} \pi(\tilde{p}_{i,1})\pi(c_{i,1})(\pi(\tilde{p}_{i,2}))^{-1} = \pi(\tilde{v}_{i,1}) \\ \pi(\tilde{p}_{i,2})\pi(c_{i,2})(\pi(\tilde{p}_{i,3}))^{-1} = \pi(\tilde{v}_{i,2}) \qquad 1 \leq i \leq n \\ \pi(\tilde{p}_{i,3})\pi(c_{i,3})(\pi(\tilde{p}_{i,1}))^{-1} = \pi(\tilde{v}_{i,3}) \end{cases}$$

A direct computation using the cocycle condition of σ_q and the fact that q is symmetric gives the identity in the claim. □

By (1) and (2) of Lemma 21, we have

$$\sum_{j=1}^{3} \sigma_q(\pi(\tilde{p}_{i,j}), \pi(c_{i,j})) = \sum_{j=1}^{3} a_{i,j}$$

and

$$\sum_{j=1}^{3} \sigma_q(\pi(\tilde{p}_{i,j})\pi(c_{i,j}), \pi(\tilde{p}_{i,j+1})^{-1}) = \sum_{j=1}^{3} b_{i,j}.$$

Now Claim 2 and the fact that $\{\tilde{w}_{i,j}\}$ is a solution of $\mathcal{W}_t$ tell us that the second component of (1) equals

$$\begin{aligned} & \sigma_q\big(\pi(c_{i,1}), \pi(c_{i,2})\big) - \sum_{j=1}^{3}(a_{i,j} + b_{i,j}) + \sum_{j=1}^{3} \iota_1(\tilde{w}_{i,j}) - \sum_{j=1}^{3} \iota_4(d_{i,j}) \\ = \quad & \sigma_q\big(\pi(c_{i,1}), \pi(c_{i,2})\big) - \sum_{j=1}^{3}(a_{i,j} + b_{i,j} + \iota_4(d_{i,j})) + \sum_{j=1}^{3} \iota_1(\tilde{w}_{i,j}) = 0 \quad (*) \end{aligned}$$

At this point, we have shown that $\tilde{e}_{i,1}\tilde{e}_{i,2}\tilde{e}_{i,3} = 1$ in E'.

Claim 2. *$\tilde{e}_{i,j} = q\big(\pi(\tilde{v}_{i,j})\big) i\big(\iota_1(\tilde{w}_{i,j}) - \iota_4(d_{i,j})\big)$ is in $\iota_2(E)$.*

Proof. We use the ρ'-coordinate for E'. Note that an element $(g, a)_{\rho'} \in E'$ is in $\iota_2(E)$ if and only if $a \in \iota_1(A)$. By the definition of the symmetric section q, we have

$$\tilde{e}_{i,j} = \Big(\pi(\tilde{v}_{i,j}), -\iota_3\big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi(\tilde{v}_{i,j}^{-1})\big)\big) + \iota_1(\tilde{w}_{i,j}) - \iota_4(d_{i,j})\Big)_{\rho'}.$$

Hence it is enough to show that $-\iota_3\big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi(\tilde{v}_{i,j}^{-1})\big)\big) - \iota_4(d_{i,j}) \in \iota_1(A)$. But this follows Lemma 15 since we know that

$$Pa\Big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), (\pi(\tilde{v}_{i,j}^{-1})\big)\Big) = d_{i,j}.$$

by (3) of Lemma 21. The proof of the claim is complete. □

Therefore we know that $\mathcal{E}$ has a solution in $\iota_2(E)$. Note that $\iota_2(E)$ is isomorphic to E. So $\mathcal{E}$ has a solution in E. We have completed the proof of the "if" part of the theorem at this point.

Now suppose $\mathcal{E}$ has a solution in E. Then $\mathcal{E}$ (with constants replaced by their images under ι_2) has a solution in $\iota_2(E) \subset E'$. Let $\{\tilde{e}_{i,j}\}$ be such a solution. We will show that one of the $\mathcal{E}_t$ we constructed also has a solution.

First note that $\{p(\tilde{e}_{i,j})\}$ is a solution of $\mathcal{E}$ (with the constants replaced by their p images) in Γ . Then by Proposition 1 for some $(c_{i,j})$ satisfying Condition 1, the tripod equation system

$$\mathcal{V}_t^1 = \begin{cases} p_{i,1}c_{i,1}(p_{i,2})^{-1} = v_{i,1} \\ p_{i,2}c_{i,2}(p_{i,3})^{-1} = v_{i,2} \qquad 1 \leq i \leq n \\ p_{i,3}c_{i,3}(p_{i,1})^{-1} = v_{i,3} \end{cases}$$

has a solution $\{\tilde{p}_{i,j}, \tilde{v}_{i,j}\}$ in V such that $\pi(\tilde{v}_{i,j}) = p(\tilde{e}_{i,j})$.

By Proposition 1 we know that $\tilde{p}_{i,j}, \tilde{v}_{i,j}$ are (λ_1, ν_1)-quasi geodesics in $\mathcal{K}$. Hence by Lemma 7 there exists $p'_{i,j}, v'_{i,j} \in Y^*$ representing $\tilde{p}_{i,j}, \tilde{v}_{i,j}$ such that $\phi(p'_{i,j})$, $\phi(v'_{i,j})$ are (λ, ν)-quasi geodesics in K_Γ and $p'_{i,j}$ is a subword of $v'_{i,j}$. Recall in the definition of the tripod equation system, $v_{i,j}$

and $v_{i',j'}$ are defined to be the same variable if $e_{i,j}$ and $e_{i',j'}$ are the same variable. However we don't require $v'_{i,j}$ and $v'_{i',j'}$ to be the same Y-word even if $v_{i,j}$ and $v_{i',j'}$ are the same variable (hence $\tilde{v}_{i,j} = \tilde{v}_{i',j'}$).

Use the Future Predicting Automaton M to read $\phi(p'_{i,j})$. Suppose it ends at the state $\bar{s}_{i,j}$. Note that $\bar{s}_{i,j}$ and $\phi(c_{i,j})$ are compatible since $\phi(v'_{i,j})$ is in L and $\phi(p'_{i,j})\phi(c_{i,j})$ is a subword of $\phi(v'_{i,j})$. Hence $(\bar{s}_{i,j})$ satisfy Condition 2. With the above choice of $c_{i,j}$ and $\bar{s}_{i,j}$, let $\bar{s}'_{i,j}$ be the state where $\phi(c_{i,j})$ ends when read by $M_{\bar{s}_{i,j}}$.

Note that $\phi(p'_{i,j}c_{i,j}) \in L(\bar{s}'_{i,j})$. Also $\phi(p'^{-1}_{i,j+1}) \in L(\bar{s}_{i,j}, c_{i,j})$ because $\phi(p'_{i,j}c_{i,j}p'^{-1}_{i,j+1})$ is in L. Let $b_{i,j} = \sigma_q\big(\pi(\tilde{p}_{i,j}c_{i,j}), \pi(\tilde{p}^{-1}_{i,j+1})\big)$. Then we have $b_{i,j} \in A(\bar{s}_{i,j}, c_{i,j}) = \{\sigma_q(\bar{s}'_{i,j}, w) \mid w \in L(\bar{s}_{i,j}, c_{i,j})\}$. Therefore $(b_{i,j})$ satisfy Condition 3.

Use the Parity Predicting Automaton D to read $\phi(v'_{i,j})$. Let $d_{i,j} \in \mathbb{Z}_2^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$ be the last component of the state where it ends.

The above choice of $\big((c_{i,j}), (\bar{s}_{i,j}), (b_{i,j}), (d_{i,j})\big)$ satisfies all conditions defining Θ. Let $t = \big((c_{i,j}), (\bar{s}_{i,j}), (b_{i,j}), (d_{i,j})\big)$.

Let $\mathcal{E}_t$ be the system of equations defined by the above t. Then it is clear from the construction of $\mathcal{E}_t$ that $\{\tilde{p}_{i,j}, \tilde{v}_{i,j}\}$ is a solution of it.

Let $\tilde{e}^2_{i,j} \in A' = \mathbb{Z}^n \oplus \mathbb{Z}_{2d_1} \oplus \cdots \oplus \mathbb{Z}_{2d_m}$ be the second component of the ρ'-coordinates of $\tilde{e}_{i,j}$. Since $\tilde{e}_{i,j}$ lies in $\iota_2(E)$, we know that $\tilde{e}^2_{i,j} \in \iota_1(A)$. By the above way of choosing $d_{i,j}$ and (3) of Lemma 21 we have

$$d_{i,j} = Pa\Big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi(\tilde{v}^{-1}_{i,j})\big)\Big).$$

Therefore by Lemma 15 we know that $\tilde{e}_{i,j}^2 + \iota_3\Big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi(\tilde{v}_{i,j}^{-1})\big)\Big) + \iota_4(d_{i,j}) \in A'$ lies in $\iota_1(A)$. Let $\tilde{w}_{i,j} \in A$ be the unique element such that

$$\iota_1(\tilde{w}_{i,j}) = \tilde{e}_{i,j}^2 + \iota_3\Big(\sigma_\rho\big(\pi(\tilde{v}_{i,j}), \pi(\tilde{v}_{i,j}^{-1})\big)\Big) + \iota_4(d_{i,j}).$$

Claim 3. *$\{\tilde{w}_{i,j}\}$ is a solution of $\mathcal{W}_t$.*

Proof. With all the notation above, we have

$$\tilde{e}_{i,j} = q\big(\pi(\tilde{v}_{i,j})\big)i\big(\iota_1(\tilde{w}_{i,j}) - d_{i,j}\big)$$

just as in the proof of the "if" part. But this time, we know that $\{\tilde{e}_{i,j}\}$ is a solution of E' instead of $\{\tilde{w}_{i,j}\}$ being a solution of $\mathcal{W}_t$ and everything else is the same. So we can go through the same calculation and when we reach $(*)$, we use the fact that $\tilde{e}_{i,1}\tilde{e}_{i,2}\tilde{e}_{i,3} = 1$ to conclude that $(*)$ holds. Therefore $\{\tilde{w}_{i,j}\}$ is a solution of $\mathcal{W}_t$ over A. □

The proof of Theorem 9 is complete. □

Theorem 1 follows from Theorem 9 since equation systems with rational constraints in virtually free groups are solvable by Theorem 3 and equation systems in finitely generated abelian groups can be solved by using linear algebra.

CITED LITERATURE

1. M. R. Bridson and A. Haefliger. *Metric spaces of non-positive curvature*, volume 319 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1999.

2. M. R. Bridson and L. Reeves. *On the algorithmic construction of classifying spaces and the isomorphism problem for biautomatic groups*, *Sci. China Math* 54 (2011), no. 8, 1533-1545.

3. F. Dahmani and V. Guirardel, *Foliations for solving equations in groups: free, virtually free and hyperbolic groups*, *Journal of Topology* 3 (2010), 343-404.

4. V. Diekert and A. Muscholl, *Solvability of equations in free partially commutative groups is decidable* In F. Orejas, P. G. Spirakis, and J. van Leeuwen, editors, Proc. 28th International Colloquium on Automata, Languages and Programming (ICALP'01), number 2076 in Lecture Notes in Computer Science, pages 543-554, Berlin Heidelberg, 2001. Springer-Verlag.

5. M. Gromov, Hyperbolic groups, *Essays in group theory*, *Math. Sci. Res. Inst. Publ.*, vol. 8, Springer, New York, (1987), 75-263.

6. D. F. Holt, S. Rees, *Regularity of quasigeodesics in a hyperbolic group. Internat. J. Algebra Comput.* 13 (2003), no. 5, 585-596.

7. M. V. Lawson, *Finite automata.* Chapman & Hall/CRC, Boca Raton, FL, 2004.

8. M. Lohrey and G. Senizergues, *Theories of HNN-extensions and amalgamated products Proceedings ICALP06, Part II, Lecture Notes in Computer Science* 4052 (Springer, Berlin, 2006) 504-515.

9. G. S. Makanin, *Equations in a free group*, *Izv. Akad. Nauk SSSR Ser. Mat.* 46 (1982) 1199-1273,1344.

10. J. Morgan and G. Tian, *Ricci flow and the Poincar conjecture.* Clay Mathematics Monographs, 3. American Mathematical Society, Providence, RI; Clay Mathematics Institute, Cambridge, MA, 2007.

11. W. D. Neumann and L. Reeves, *Regular cocycles and biautomatic structures*, *Internat. J. Algebra Comput.* 6 (1996), no. 3, 313-324.

12. W. D. Neumann and L. Reeves, *Central extensions of word hyperbolic groups*, *Ann. of Math.* (2) 145 (1997), no. 1, 183-192.

13. W. D. Neumann and M. Shapiro, *Equivalent automatic structures and their boundaries*, *Internat. J. Algebra Comput.* 2 (1992), no. 4, 443-469.

14. E. Rips and Z. Sela, *Canonical representatives and equations in hyperbolic groups*, *Invent. Math.* 120 (1998) 489-512.

15. V. A. Roman'kov. *Universal theory of nilpotent groups*, *Mat. Zametki.*, 635 (1979) 25(4):487-495.

16. D. Segal, *Polycyclic groups*. Cambridge Tracts in Mathematics, 82. Cambridge University Press, Cambridge, 1983.

17. J-P. Serre, *Trees*, Springer, Berlin (1980) Translated from the French by John Stillwell

18. J. K. Truss, *Equation-solving in free nilpotent groups of class 2 and 3*, *Bull. London Math. Soc.*, (1995) 27(1):39-45.

VITA

Education

Ph.D. (Expected) University of Illinois at Chicago, 2009-Present
M.S. University of Illinois at Chicago, 2007-2009
B.S. Zhejiang University, 2003-2007

Research Interests

geometric group theory and low-dimensional topology

Papers

Centralizer of finite subgroups of the mapping class group, arXiv:1202.5714, February 2012

Equations over central extensions of hyperbolic groups. In preparation.

Presentations

"Finite subgroups of Mod(S) and almost fixed points in $C(S)$", group theory seminar, University of Illinois at Urbana-Champaign, April 2012

"Equations over central extensions of hyperbolic groups", Geometry, Topology, Dynamics Seminar, University of Illinois at Chicago, September 2012

"Equations over central extensions of hyperbolic groups", Geometry and Topology Seminar, The Graduate Center, CUNY, October 2012

Awards

Deans Scholar Award, University of Illinois at Chicago, 2012-2013.

Conferences Attended

Geometric structures and representation varieties, 2012, University of Illinois at Urbana-Champaign
AMS sectional meeting, 2011, The University of NebraskaCLincoln
Geometric Group Theory and Logic, 2011, University of Illinois at Chicago
Approaches to Group Theory, 2010, Cornell University
More Examples of Groups, 2009, Ohio State University
RTG Workshop on Geometric Group Theory, 2009, University of Michigan

Teaching Experience

Teaching assistant, University of Illinois at Chicago, 2007-2011

- Calculus, Intermediate Algebra, Finite Math for Business Majors

Instructor, University of Illinois at Chicago, 2012

- Multivariable Calculus.